Proceedings

2000 IEEE International Symposium on Information Theory



Sorrento Palace Hotel
Conference Center
Sorrento, Italy

25–30 June, 2000

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited





Sponsored by
the IEEE Information Theory Society

20010618 105

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY *(Leave Blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
		Final

4. TITLE AND SUBTITLE
2000 IEEE Internatinal Symposium on Information Theory

5. FUNDING NUMBERS
G

6. AUTHORS
variou

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
IEEE
445 Hoes Lane, PO Box 1331
Piscataway, NJ 08855-1331

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Office of Naval Research
Ballston Centre Tower One
800 North Quincy Street
Arlington, VA 22217-5660

10. SPONSORING / MONITORING AGENCY REPORT NUMBER
N00014-98-1-0811

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

This is the program for the IEEE International Sympoaium on Information Theory that took place in Sorrento in June 2000.

14. SUBJECT TERMS
Information Theory

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	**Unclassified**	**Unclassified**	

Proceedings

2000 IEEE International Symposium on Information Theory

Sorrento Palace Hotel
Conference Center
Sorrento, Italy

25–30 June, 2000





Sponsored by
the Information Theory Society
of the Institute of Electrical and Electronics Engineers

Proceedings 2000 IEEE International Symposium on Information Theory

Copyright and Reprint Permission: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923. For copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Operations Center, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331. All rights reserved. Copyright ©2000 by The Istitute of Electrical and Electronics Engineers, Inc.

IEEE Catalog Number:	00CH37060
ISBN:	0-7803-5857-0 0-7803-5858-9 (Casebound Edition) 0-7803-5859-7 (Microfiche Edition)
Library of Congress:	72-179437

Additional copies of this publication are available from:

IEEE Operations Center
P.O. Box 1331
445 Hoes Lane
Piscataway, NJ 08855-1331 USA

1-800-678-IEEE
1-732-981-1393
1-732-981-9667 (Fax)
833-233 (Telex)
email: customer.service@ieee.org

Organizing Committee

General Co-Chairmen
Ezio Biglieri
Sergio Verdú

Program Co-Chairmen
Anthony Ephremides
Thomas Ericson

Tutorials
Ken Vastola

Finance
Giorgio Taricco

Publications
Emanuele Viterbo

Publicity
Giuseppe Caire
Walter Balzano

Secretariat
Stilema

Program Committee

Anthony Ephremides (co-chair)
Thomas Ericson (co-chair)
Venkat Anantharam
Alexander Barg
Andrew Barron
Pascale Charpin
Martin Bossert
Gérard Cohen
Daniel J. Costello, Jr.
Imre Csiszár
Alfredo De Santis
Stefan Dodunekov
Nariman Farvardin
Meir Feder
G. David Forney, Jr.
Laszlo Györfi
Joachim Hagenauer
Bruce Hajek
Tor Helleseth
Michael Honig
Iiro Honkala
Johannes Huber
Tom Hoeholdt
Hideki Imai
Rolf Johannesson
Torleiv Kløve
Kingo Kobayashi
Sanjeev Kulkarni
Ueli Maurer
Urbashi Mitra
Prakash Narayan
Vincent Poor
Bixio Rimoldi
Paul Siegel
Wojciech Szpankowski
Ludo Tolhuizen
David Tse
Ugo Vaccaro
Han Vinck
Frans Willems

Acknowledgments

Grateful acknowledgment is given to the following organizations for their financial support of ISIT 2000:

TELECOM ITALIA

omni®

QUALCOMM®

ERICSSON

NOKIA
CONNECTING PEOPLE

Lucent Technologies
Bell Labs Innovations

AT&T

Table of Contents

Plenary Sessions

Monday 8:30 - 9:30 – Panel Discussion The Next Fifty Years of Information Theory and Beyond
Panelists: *Tom Cover, Robert Gallager, James Massey, Jacob Ziv*

Tuesday 8:30 - 9:30 – Shannon Lecture: Recursive Soft-decision Decoding Algorithms for Binary Linear Block Codes
Tadao Kasami

Wednesday 8:30 - 9:30 – Quantum Shannon Theory
Peter Shor

Thursday 8:30 - 9:30 – Shannon Lecture: Adaptive Filtering, Displacement Structure and Fast Modems
Thomas Kailath

Friday 8:30 - 9:30 – Control with Information Constraints: Information Theory Meets System Theory
Sanjoy Mitter

MOa – Monday, 9:40 - 11:00

Mathematical Methods for Coding Theory

On polynomial invariants of codes, matroids and the partition function
Alexander Barg 1

On the Hensel Lift of a Polynomial
Zhe-Xian Wan 2

On Superimposed Codes Based on Incidence Systems
Antony J. Macula, Pavel A. Vilenkin 3

Communication Complexity and Association Schemes
Ulrich Tamm 4

Special Classes of Codes I

Design of Efficient Erasure Codes with Differential Evolution
Amin Shokrollahi, Rainer Storn 5

On Multiple Insertion/Deletion Correcting Codes
T.G. Swart, H.C. Ferreira 6

On Unequal Error Protection Reed-Muller Codes
Dojun Rhee 7

Unidirectional Byte Error Correcting Codes for q-ary Data
Kiattichai Saowapa, Haruhiko Kaneko, Eiji Fujiwara 8

Codes on Graphs

Codes on Graphs: Normal Realization
G. David Forney Jr. 9

Dealing with short cycles in graphical codes
Arnaud Guyader, Eric Fabre 10

On Codes that Can Identify Vertices in Graphs
Gérard Cohen, Iiro Honkala, Antoine Lobstein, Gilles Zémor 11

Linear-Time Encodable and Decodable Irregular Graph Codes
Saejoon Kim, Stephen B. Wicker 12

Lossless Source Coding I

The Estimate for the Cost of Search Tree Constructed on an Arbitrary Set of Binary Words
Alexey Fedotov, Boris Ryabko 13

The Number of Optimal Binary One-Ended Codes
Zsolt Kukorelly 14

Coding of Ordered Trees
Kingo Kobayashi, Hiroyoshi Morita, Mamoru Hoshi 15
Universal Lossless Coding of Sources with Large and Unbounded Alphabets
En-Hui Yang, Yunwei Jia 16

Cryptography I

An Efficient Test for the Possibility of Information-Theoretic Key Agreement Secure Against Active Adversaries
Stefan Wolf 17
From Weak to Strong Information-Theoretic Key Agreement
Ueli Maurer, Stefan Wolf 18
Information-Theoretic Analysis of Information Hiding
Pierre Moulin, Joseph A. O'Sullivan 19
Information-Theoretically Secure Keyless Authentication
Valeri Korjik, Maxim Bakin 20

Multi-Terminal Information Theory

On Point-to-Point Communication Networks
Lihua Song, Raymond W. Yeung 21
The Gaussian Parallel Relay Network
Brett Schein, Robert G. Gallager 22
Static Broadcasting
Nadav Shulman, Meir Feder 23
Achievable Distortion Regions of Gaussian Broadcast Systems
Udar Mittal, Nam Phamdo 24

Testing and Estimation

Limits of Information, Markov Chains, and Projection
Andrew R. Barron 25
The Consistency of the BIC Markov Order Estimator
Imre Csiszár, Paul C. Shields 26
Large Deviations of Probability Rank
Erdal Arikan 27
Information-theoretic methods in testing the goodness of fit
László Györfi, G. Morvai, Igor Vajda 28

MOb – Monday, 11:20 - 12:40

Special Classes of Codes II

Decomposable Codes Based on Two-Dimensional Array Codes
Xiao-Hong Peng, P.G. Farrell 29
Bases of Rectangular Codes
Vladimir Sidorenko, J. Maucher, Martin Bossert 30
Cocyclic Hadamard Codes from Semifields
Parampalli Udaya, K.J. Horadam 31
New DbEC-TbED Codes Better Than the Gilbert-Varshamov Bound
Gui-Liang Feng, Xin-Wen Wu, T.R.N. Rao 32

Design of Convolutional Codes

Minimal and systematic convolutional codes over finite Abelian groups
Fabio Fagnani, Sandro Zampieri 33
On the Design of Convolutional Codes over Block Fading Channels
Marco Chiani, A. Conti, V. Tralli 34
Further Results on Unequal Error Protection of Convolutional Codes
Chung-Hsuan Wang, Chi-chao Chao 35

On the Computation of Weight Enumerators for Convolutional Codes
Cecilio Pimentel 36

Multiple Access Channels

The Binary Multiplying Channel without Feedback: New Rate Pairs in the Zero-Error Capacity Region
Ludo Tolhuizen 37
Error Exponents for the Two-User Poisson Multiple-Access Channel
Shraga Bross, Marat V. Burnashev, Shlomo Shamai (Shitz) 38
On the capacity of some uncoordinated multiple-access channels
Peter Gober 39
On the White Gaussian Multiple-Access Relay Channel
Gerhard Kramer, Adriaan J. de Lind van Wijngaarden 40

Lossless Source Coding I (cont.)

Compressing as well as the best tiling of an image
Wee Sun Lee 41
The Optimal Overflow and Underflow Probabilities with Variable-Length Coding for the General Source
Osamu Uchida, Te Sun Han 42
Minimum Conditional Entropy Context Quantization
Xiaolin Wu, Philip A. Chou, Xiaohui Xue 43
On the variance and the probability of length overflow of lossless codes
Ryo Nomura, Toshiyasu Matsushima, Shigeichi Hirasawa 44

Cryptography II: Watermarking

Identification in the Presence of Side Information with Application to Watermarking
Yossef Steinberg, Neri Merhav 45
Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding
Brian Chen, Gregory W. Wornell 46
Relationship between Quantization and Distribution Rates of Digitally Watermarked Data
Damianos Karakos, Adrian Papamarcou 47
On the Gaussian Watermarking Game
Aaron Cohen, Amos Lapidoth 48

Capacity of Timing Channels

An Information Theoretic Approach to Metering Schemes
Annalisa De Bonis, Barbara Masucci 49
Point Process Channel and Capacity of the Exponential Server Queue
Rajesh Sundaresan 50
The Jamming Game for Packet Timing Channels
James R. Giles, Bruce Hajek 51
Information Transmission over a Finite Buffer Channel
Suhas Diggavi, Matthias Grossglauser 52

Filtering

Output Distribution of the Burrows-Wheeler Transform
K. Visweswariah, S. Kulkarni, Sergio Verdú 53
Statistical Imaging and Complexity Regularization
Pierre Moulin, Juan Liu 54
ISI Channel Estimation Using Complementary Sequences
Predrag Spasojević, Costas N. Georghiades 55
Some Aspects of Multivariate Rayleigh and Exponential Distributions
Ranjan K. Mallik 56

MOc – Monday, 2:30 - 3:50

Codes in Non-Hamming Spaces

A New Decoding Algorithm for Spherical Codes Generated by Binary Partitions of Symmetric Pointsets
John Karlof, Guodong Liu 57

Slepian-Type codes on a Flat Torus
Sueli I.R. Costa, Edson Agustini, Marcelo Muniz, Reginaldo Palazzo Jr. 58

Decoding Algorithm for the High-Dimensional Discrete Torus Knot Code
Masayasu Hata, Eisaku Yamaguchi, Ichi Takumi, Yuuichi Hamasuna, Kenji Miyoshino 59

Extremal Polynomials for Codes in Polynomial Metric Spaces
Svetla Nikova, Ventsislav Nikov 60

Soft-Decision Decoding of Block Codes I

Algebraic Soft-Decision Decoding of Reed Solomon Codes
Ralf Kötter, Alexander Vardy 61

Soft Decision Decoding of Reed Solomon Codes
Vishakan Ponnampalam, Branka Vucetic 62

Recursive Decoding of Reed-Muller Codes
Ilya Dumer, Kirill Shabunov 63

Error Performance Analysis for Reliability-Based Decoding Algorithms
Marc P.C. Fossorier, Shu Lin 64

Analysis of Turbo Codes

Analysis of the Trellis Complexity of Interleavers and Turbo Codes
Roberto Garello, Guido Montorsi, Sergio Benedetto, Giovanni Cancellieri 65

Improving Turbo Decoding via Cross-Entropy Minimization
M. Eoin Buckley, Bhaskar Krishnamachari, Stephen B. Wicker, Joachim Hagenauer 66

Simplified Turbo Decoding for Binary Markov Channels
Javier Garcia-Frias, John D. Villasenor 67

Approximate Performance Analysis of Turbo Codes with Fixed Interleaver
Nam Phamdo, Jianqiu Zhang 68

Universal Lossless Source Coding and Prediction

A Universal Prediction Lemma and Applications to Universal Data Compression and Prediction
Jacob Ziv 69

On Sequential Strategies for Loss Functions with Memory
Neri Merhav, Erik Ordentlich, Gadiel Seroussi, Marcelo J. Weinberger 70

On Asymptotically Optimal Methods of Prediction and Adaptive Coding for Markov Sources with Unknown Memory
Boris Ryabko, Flemming Topsoe 71

A Technique for Prediction and Probability Assignment (PPA) in Lossless Data Compression
Nicklas Ekstrand, Ben Smeets 72

Coding Methods for Wireless Communications

On the Reliable Throughput Supported by Multiple-Antenna Rayleigh-Faded Links for QAM Coded Transmissions
Enzo Baccarelli, G. Di Blasio, A. Fasano, A. Zucchi 73

Code Design for Combined Channel Estimation and Error Correction Coding
Mikael Skoglund, Stefan Parkvall 74

Optimal 4- and 8-State Across-the-Subchannels TCM Encoders for DMT Systems
V. Shashidhar, B. Sundar Rajan, V. Umapathi Reddy 75

Coding for Noncoherent Communication
Dilip Warrier, Upamanyu Madhow, Ralf Kötter 76

Communication Network Performance and Measurement

Feedback Regulation for Sequencing and Routing in Multiclass Queueing Networks
Sean P. Meyn 77
Measurement-Based Network Monitoring: Missing Data Formulation and Scalability Analysis
Chuanyi Ji, Anwar Elwalid 78
Time-Varying Network Tomography: Router Link Data
Bin Yu, Jin Cao, Drew Davis, Scott Vander Wiel 79
Interval-valued Probability Modeling of Internet Traffic Variables
Pablo Fierens, Terrence L. Fine 80

Estimation I

Universal Linear Least-Squares Prediction
Andrew C. Singer, Meir Feder 81
Non-Linear MMSE Estimation and SbS-MAP Receivers
Stefano Galli 82
On the accuracy of estimating tail probabilities in queues
Assaf J. Zeevi 83
Estimation of the Covariance Matrix for Adaptive CFAR Detection in Compound-Gaussian Clutter
Ernesto Conte, Antonio De Maio, Giuseppe Ricci 84

MOd – Monday, 4:10 - 5:30

Product Codes

Bounded-Distance Soft Decision Decoding of Binary Product Codes
Ofer Amrani, Yair Be'ery 85
On Structure and Decoding of Product Codes
S.A. Miri, Amir K. Khandani 86
Low Complexity Maximum-Likelihood Decoding of Product Codes
Omar Al-Askary 87
Randomly Interleaved SPC Product Codes
D. Rankin, T.A. Gulliver 88

Soft-Decision Decoding of Block Codes II

Soft Decision Majority Decoding
Ilya Dumer, Rafail Krichevskiy 89
A^* ML Decoding of Linear Block codes on Band-Limited Channels
Svante Eriksson, Tor M. Aulin 90
Fast Soft-Decision Decoding of Linear Codes, Stochastic Resonance in Algorithms
Antoine Valembois 91
Minimum Norm Solution Based Approach to Decoding of Real Number BCH Codes
Nikola Rozic, Dinko Begusic, M. Vrdoljak 92

Woven Convolutional Codes

The Construction and Free Distance Estimation of Generalized Woven Codes with Outer Warp
Martin Bossert, Walter Schnug, Hans Dieterich, Sergo Shavgulidze 93
Woven Codes with Outer Block Codes
J. Freudenberger, Martin Bossert, V. Zyablov, S. Shavgulidze 94
Optimum Slope Convolutional Codes
Ralph Jordan, Jürgen Freudenberger, Viktor Pavlouchkov, Martin Bossert, Viktor Zyablov 95
Decoding of Woven Convolutional Codes and Simulation Results
Ralph Jordan, Walter Schnug, Martin Bossert, Stefan Höst, Rolf Johannesson, Viktor Zyablov 96

Universal Lossless Source Coding and Prediction (cont.)

Universal Prediction of Individual Binary Sequences in the Presence of Arbitrarily Varying, Memoryless Additive Noise
Tsachy Weissman, Neri Merhav 97
Worst-case Bounds for the Redundancy of Sequential Lossless Codes and for the Logarithmic Loss of Predictors
Nicolò Cesa-Bianchi, Gábor Lugosi 98
Filtering and Prediction of Individual Sequences Corrupted By Noise Using the Lempel-Ziv Algorithm
Anelia Baruch, Neri Merhav 99

Decoding for Intersymbol Interference Channels

Iterative Correction of ISI via Equalization and Decoding with Priors
Michael Tüchler, Ralf Kötter, Andrew C. Singer 100
Use of the List Viterbi Algorithm to Compute the Distance Spectrum of Trellis Codes and ISI Channels
Sabah Badri, Peter Hoeher 101
A New Successively Decodable Coding Technique for Intersymbol-Interference Channels
Tommy Guess, Mahesh K. Varanasi 102
Partitioning for SA(B,C) detectors on ISI AWGN channels
Andreas Cedergren, Tor M. Aulin 103

Packet Scheduling

Modeling of the LAN Traffic Microstructure Based on the Class A Noise Model
Xueshi Yang, Athina Petropulu, David Middleton 104
Statistical Multiplexing of Many Independent ATM-Streams with Temporally Constrained Long-Range Dependence
Sándor Csibi 105
Delay analysis for prioritized service of variable rate regenerative traffic sources
Michael Shalmon 106
Scheduling for Fair Allocation of Rates in Multirate Multicast Networks
Saswati Sarkar, Leandros Tassiulas 107

Estimation II

Optimal Group-theoretic Methods for Selective Motion Analysis: Detection, Estimation, Filtering and Reconstruction with Continuous and Discrete Spatio-Temporal Wavelets
Jean-Pierre Leduc 108
Channel Quality Estimation with Channel Error Counts for Adaptive Signaling in Wireless Communications
Michael B. Pursley, John M. Shea 109
Least Mean-Squared Error Polynomial Estimation in Systems with Uncertain Observations
Raquel Caballero-Aguila, Aurora Hermoso-Carazo, Josefa Linarez-Pérez 110
Asymptotics of the Bayesian Estimator of Hidden Markov Models
Laurent Mevel, Lorenzo Finesso 111

TUa – Tuesday, 9:40 - 11:00

Special Classes of Codes III

A Class of Sudan-decodable Codes
Rasmus R. Nielsen 112
Enumeration and Construction of all Binary Duadic Codes
Xin Li, Wei Sun, Yixian Yang, Zhengtao Zhang 113
Extremal Doubly-even Self-dual Cocyclic $|40, 20|$ Codes
Asha Baliga 114
A New Family of Optimal Codes Correcting Term Rank Errors
David Lund, Ernst M. Gabidulin, Bahram Honary 115

Trellises for Linear Block Codes

Subcode Graphs of Linear Block Codes
Thomas Mittelholzer 116
General Structure and Construction of Tail Biting Trellises for Linear Block Codes
Shu Lin, Rose Y. Shao 117
Minimal Tail-Biting Trellises for Linear MDS Codes over F_{p^m}
B. Sundar Rajan, G. Viswanath 118
Uniformly Efficient Trellises for Self-Dual Codes
Houshou Chen, John T. Coffey 119

Turbo Code Design

General Coding Theorems for Turbo-like Codes
Hui Jin, Robert J. McEliece 120
Irregular Turbocodes
Brendan J. Frey, David J.C. MacKay 121
Contradicting a Myth: Good Turbo Codes with large Memory Order
Peter Massey, Oscar Y. Takeshita, Daniel J. Costello Jr. 122
Chaotic Turbo Codes
Sorin Adrian Barbulescu, Andrew Guidi, Steven S. Pietrobon 123

Lossy Source Coding Theory

The Index Entropy in Mismatched Lossy Source Coding
Ram Zamir 124
A Zero-Delay Sequential Quantizer for Individual Sequences
Tamás Linder, Gábor Lugosi 125
The Redundancy of Successive Refinement Codes and Codes with Side Information
German Voronov, Meir Feder 126
All Sources are Nearly Successively Refinable
Luis Lastras, Toby Berger 127

Multiple Access

A Broadcast Approach for the Multiple-Access Slow Fading Channel
Shlomo Shamai (Shitz) 128
Multiuser Capacity in Block Fading with no Channel State Information
Shlomo Shamai (Shitz), Thomas L. Marzetta 129
Sum Capacity of DS-CDMA with Colored Noise
Pramod Viswanath, Venkath Anantharam 130
On Capacity and Spreading in CDMA Systems
Mehul Motani, Venugopal V. Veeravalli, Chris Heegard 131

Synchronisation and Acquisition

Suboptimal Schemes for Noncoherent Parallel Acquisition of Spreading Sequences in DS/SS Systems
Zhiyuan Yan, Dilip V. Sarwate 132
Analysis of Acquisition in WCDMA Systems
Sandip Sarkar 133
Maximum Likelihood Symbol Synchronization in Channels with Data Dependent Noise
A. Gameiro 134
On the Capacity of a Pulse Position Hopped CDMA System
Ola Wintzell, Dimitri K. Zigangirov, Kamil Sh. Zigangirov 135

Coded Modulation I

Differential Phase Shift Keying with Constellation Expansion Diversity
Lutz H.-J. Lampe, R.F.H. Fisher, Johannes B. Huber 136
Coded M-FSK for Power Line Communications
A. J. Han Vinck, Juergen Haering, Tadashi Wadayama 137
Error Performance of Multilevel Modulation Codes over Phase Noisy Fading Channels
Robert H. Morelos-Zaragoza, Motohiko Isaka, Hideki Imai 138

How Large is the Coding Gain for Multilevel Modulation Systems?
Gerd Beyer, Karin Engdahl, Kamil Sh. Zigangirov 139

TUb – Tuesday, 11:20 - 12:40

Codes over Non-Binary Alphabets

Type II Codes over F_4
Philippe Gaborit, Vera Pless, Patrick Solé, Oliver Atkin 140
On Type II Codes over F_4
Koichi Betsumiya, Aaron T. Gulliver, Masaaki Harada, Akihiro Munemasa 141
Error-correcting Codes over an Alphabet of Four Elements
Galina T. Bogdanova, Andries Brouwer, Stoian N. Kapralov, Patric Östergard, ... 142
A Construction of Ternary Constant-Composition Codes with Weight Three and Minimum Distance Four
Mattias Svanström 143

Information Storage I (Constrained Systems and Codes)

Capacity of weakly (d, k)-constrained sequences
Kees A. Schouhamer Immink, Augustus J.E.M. Janssen 144
On Codes that Avoid Specified Differences
Bruce E. Moision, Alon Orlitsky, Paul H. Siegel 145
Optimal Block Codes for M-ary Runlength-Limited Channels
Steven W. McLaughlin, Suparna Datta 146
Art of Constructing Low-complexity Encoders/Decoders for Constrained Block Codes
Dharmendra S. Modha, Brian H. Marcus 147

Iterative Decoding I

Cycle Length Distributions in Graphical Models for Iterative Decoding
Xian-ping Ge, David Eppstein, Padhraic Smyth 148
Efficient Decoding of Interleaved Linear Block Codes
Christoph Haslach, A.J. Han Vinck 149
Performance Limits of Concatenated Codes with Iterative Decoding
Sandrine Vialle, Joseph Boutros 150

Vector Quantization

On the Training Distortion of Vector Quantizers
Tamás Linder 151
Asymptotic Two-Stage Two-Dimensional Quantizer
Tsutomu Kawabata 152
On the Whiteness of High Resolution Quantization Errors
Harish Viswanathan, Ram Zamir 153
Worst-case rate of scalar vs. vector quantization
Alon Orlitsky 154

Information Spectrum

Achievable rates of random number generators for an arbitrary prescribed distribution from an arbitrary given distribution
Takahiro Yoshida, Toshiyasu Matsushima, Shigeichi Hirasawa 155
An Information-Spectrum Approach to Rate-Distortion Function with Side Information
Ken-ichi Iwata 156
General Formulas for Csiszár's Source Coding Cutoff Rates
Po-Ning Chen, Fady Alajaji 157
Coding Theorems on Shannon's Cipher System with a General Source
Hiroki Koga 158

Communication over Fading Channels

Adaptive Modulation Using Long Range Prediction for Flat Rayleigh Fading Channels
Shengquan Hu, Alexandra Duel-Hallen, Hans Hallen 159

Multidimensional Signals with Correlated Frequencies for Noncoherent Detection over the Rayleigh Channel
Céline Durand, Elie Bejjani, Joseph Boutros 160

Bandwidth-Efficient Exploitation of the Degrees of Freedom in a Multipath Fading Channel
Ashwin Ganesan, Akbar M. Sayeed 161

Performance of TETRA under Quasi-Synchronous Transmission over Rayleigh Fading Channels with Equalization
Michael Yip Ming, Francis C. M. Lau 162

Coded Modulation II

Complex Spherical Modulation for Noncoherent Communications
Mahesh K. Varanasi, Michael L. McCloud 163

Orbital Spherical 11-Designs whose Initial Point is Root of an Invariant Polynomial
Vladimir Sidel'nikov 164

Constellation Mappings for Two-Dimensional Non-Uniform Signalling
Glen Takahara, F. Alajaji, H. Kuai, N.C. Beaulieu 165

PAR Reduction via Constellation Shaping
Henry K. Kwok, Douglas L. Jones 166

TUc – Tuesday, 2:30 - 3:50

Algebraic Codes

Duadic Z4-Codes
Patrick Solé, Philippe Langevin 167

Results relating to code construction on a tower of function fields meeting the Drinfeld-Vladut bound
I. Aleshnikov, H. Stichtenoth, V. Deolalikar, P. Vijay Kumar, K. Shum 168

A Dual of Well-Behaving Type Designed Minimum Distance
Tomoharu Shibuya, Kohichi Sakaniwa 169

Bounds on the State Complexity of Geometric Goppa Codes
Tim Blackmore, Graham Norton 170

Iterative Decoding II

Iterative Decoding and Channel Estimation
Paul D. Alexander, Alex J. Grant 171

Iterative Decoding of Non-Systematic Turbo-Codes
Oliver M. Collins, Oscar Y. Takeshita, Daniel J. Costello Jr. 172

Iterative Source-Channel Decoding using Soft-In/Soft-Out Decoders
Norbert Görtz 173

Iterative Decoding Algorithms Updating Likelihood and Channel Values Based on Interim Hard Decision Results
Masayuki Ariyoshi, Iwao Sasase 174

Multi-User Lossy Source Coding

Asymptotic Performance of Multiple Description Lattice Quantizers
Vinay A. Vaishampayan, N.J.A. Sloane, Sergio Servetto 175

On Optimal Frame Expansions for Multiple Description Quantization
Sanjeev Mehrotra, Philip A. Chou 176

Multiple Description Quantization by Deterministic Annealing
Prashant Koulgi, Shankar L. Regunathan, Kenneth Rose 177

A Constructive Approach to Distributed Source Coding with Symmetric Rates
S. Sandeep Pradhan, Kannan Ramchandran, Ralf Kötter 178

Capacity Computations

Shannon Capacity of Large Odd Cycles
Tom Bohman, Miklós Ruszinkó, Lubos Thoma 179
Asymptotic Capacity of the Two-Dimensional Square Constraint
Zsigmond Nagy, Kenneth Zeger 180
Capacity of retro-information channels
Philippe Jacquet, Véronique Joly 181
On the evaluation of the capacity of channels with memory
Jean Conan 182

Cryptography and Coding I

Fourier Spectrum of Optimal Boolean Functions via Kasami's Identities
Anne Canteaut, Claude Carlet, Pascale Charpin, Caroline Fontaine 183
A Construction of Resilient Functions with High Nonlinearity
Thomas Johansson, Enes Pasalic 184
On the Structure and Numbers of Higher Order Correlation-Immune Functions
Yuriy Tarannikov 185
Large Weight Patterns Decoding in Goppa Codes and Application to Cryptography
Pierre Loidreau 186

Communication Systems

An Error Performance Analysis of Iterative Threshold Decoding
Christian Cardinal, David Haccoun, François Gagnon 187
Bandwidth Efficient Hybrid ARQ Schemes Using Turbo Codes
Adrish Banerjee, Daniel J. Costello Jr., Thomas E. Fuja 188
Convergence of Relative Frequency of Occurrence of Error Bursts on Channels with Memory
Mitsuru Hamada 189
Some low constant weight code designs for the parallel asynchronous communication scheme
Luca Tallini, Bella Bose 190

Turbo Coded Modulation I

Algorithm for Joint Decoding of Turbo Codes and M-ary Orthogonal Modulation
Cheng-Po Liang, Wayne E. Stark 191
Turbo Nonlinear CPFSK with Iterative Decoding
Bon-Jin Ku, Woong-Gon Kim, Ha-Young Yang, Dae-Sik Hong, Chang-Eon Kang 192
BER Bounds for Turbo Coded Modulation and their Application to Adaptive Modulation
Sriram Vishwanath, Andrea J. Goldsmith 193
Serial Turbo Trellis Coded Modulation with Rate-1 Inner Code
Dariush Divsalar, Sam Dolinar, F. Pollara 194

TUd – Tuesday, 4:10 - 5:30

Quasi-Cyclic Codes

Quasi-cyclic Goppa Codes
Tierry P. Berger 195
Algebraic Structure of Quasicyclic Codes
Kristine Lally, Patrick Fitzpatrick 196
New Results on Binary Quasi-Cyclic Codes
Zhi Chen 197
On a Sequence of Cyclic Codes with Minimum Distance Six
Danyo Danev, Jonas Olsson 198

Low Density Parity Check Codes

Design of Provably Good Low-Density Parity Check Codes
Tom J. Richardson, Amin Shokrollahi, Rüdiger Urbanke 199
Low Density Parity Check Codes Based on Finite Geometries: A Rediscovery
Yu Kou, Shu Lin, Marc P.C. Fossorier 200
Analytical Approach to Low-Density Convolutional Codes
K. Engdahl, M. Lentmaier, D.V. Truhachev, Kamil Sh. Zigangirov 201
On Gallager's Low-Density Parity-Check Codes
Gérard Battail 202
Exact Thresholds and Optimal Codes for the Binary Symmetric Channel and Gallager's Decoding Algorithm A
L. Bazzi, T. Richardson, R. Urbanke 203

Issues in Lossy Source Coding

Solving Lattice Codebook Enumeration Problem for Generalized Gaussian Sources
P. Loyer, J.M. Moureaux, Marc Antonini 204
Successive Refinement of Information with Reliability Criterion
Evgueni Haroutunian, Ashot N. Harutyunyan 205
Approximation of the Resource Bounded Complexity Distortion Function
Daby Sow, Alexandros Eleftheriadis 206
High-Rate Transform Coding: How High is High, and Does it Matter?
Vivek K. Goyal 207

Rate Distortion

The Rate Distortion Region for the Multiple Description Problem
Michael Fleming, Michelle Effros 208
On the Rate-Distortion Region for Multiple Descriptions
Fang-Wei Fu, Raymond W. Yeung 209
A Rate-Distortion Theorem Without Reference Letters
Takeshi Hashimoto 210
On the Rates-Reliability-Distortions and Partial Secrecy Region of a One-Stage Branching Communication System
E.A. Haroutunian, A.N. Harutyunyan, A.R. Ghazaryan, Edward C. van der Meulen 211

Cryptography and Coding II

Theoretical Analysis of a Correlation Attack based on Convolutional Codes
Frederik Jönsson, Thomas Johansson 212
Compared Performance of Fast Correlation Attacks on Stream Ciphers
Anne Canteaut, Michaël Trabbia 213
Novel Fast Correlation Attacks via Iterative Decoding of Punctured Simplex Codes
Miodrag J. Mihaljevic, Marc P.C. Fossorier, Hideki Imai 214
Using Low Density Parity Check Codes in the McEliece Cryptosystem
Chris Monico, Joachim Rosenthal, Amin Shokrollahi 215

Orthogonal Frequency Division Multiplexing Systems

A Class of Signal Processing Algorithms for Good Power/Bandwidth Tradeoffs with OFDM Transmission
Rui Dinis, António Gusmão 216
On the Existence and Construction of Good Codes with Low Peak-to-Average Power Ratios
Kenneth G. Paterson, Vahid Tarokh 217
On the Error Performance of 8-VSB TCM Decoder for ATSC Terrestrial Broadcasting of Digital Television
Dojun Rhee, Robert H. Morelos-Zaragoza 218
Channel Capacity of Clipped OFDM Systems
Hideki Ochiai, Hideki Imai 219

Turbo Coded Modulation II

Construction and Performance of q-ary Turbo Codes for use with M-ary Modulation Techniques
Gregory S. White, Daniel J. Costello Jr. 220
Multistage Turbo Decoding for Multilevel Superposition Coded Modulation Schemes
Marcelo E. Pellenz, Jaime Portugheis 221
Turbo Trellis Coded Modulation on Partially Coherent Fading Channels
Allen Risley, Benjamin J. Belzer, Yathian Zhu 222
On the Performance of Turbo Coded Modulation Systems with DD and NDA Phase Synchronization
Piotr Tyczka, Stephen G. Wilson 223

WEa – Wednesday, 9:40 - 11:00

Weights in Codes I

Fast calculation of the number of the minimum weight words for CRC codes
Peter S. Kazakov 224
An Algorithm for Computing Weight Distribution of Coset Leaders of Binary Linear Block Codes
Masaya Maeda, Toru Fujiwara 225
The Weight Distributions of Some Product Codes
Richard Andrew 226
Determination of the Asymptotic Largest Minimum Distance of Block codes
Tzong-Yow Lee, Po-Ning Chen, Yunghsiang S. Han 227

Sequential and List Decoding of Convolutional Codes

Regressive Channel Coding with Sequential Decoding for Embedded Source Coders
Thomas Stockhammer, Christian Weiss, Joachim Hagenauer 228
Probability of Deficient Decoding in Sequential Decoding
Takeshi Hashimoto 229
Bootstrap Sequential Decoding at High Spectral Efficiencies
Hermano Cabral, Daniel J. Costello Jr. 230
On Analysis of Noiseless Decision Feedback Scheme Using Fixed Size List Decoder for Tree Codes
Toshihiro Niinomi, Toshiyasu Matsushima, Shigeichi Hirasawa 231

Portfolios and Computation Problems

Performance of universal Portfolios in the stock market
Tom Cover, David Julian 232
An Adaptive Algorithm for Log-optimal Portfolio and its Theoretical Analysis
Zhongxing Ye, Jianguo Huang 233
Iterative Computation of Rate-Distortion Bounds for Scalable Source Coding
Ertem Tuncel, Kenneth Rose 234
Iterating the Arimoto-Blahut Algorithm for Faster Convergence
Jossy Sayir 235

Source-Channel Coding I

To Code or not to Code
Michael Gastpar, Bixio Rimoldi, Martin Vetterli 236
Source-Channel Coding Strategies: Tandem Coding vs. Channel-Optimized Quantization
Jongtae Lim, David L. Neuhoff 237
Iterative Source/Channel Decoding based on a Trellis Representation for Variable Length Codes
Rainer Bauer, Joachim Hagenauer 238
Progressive Image Transmission over Compound Packet Erasure Channels
Vinay Chande, Nariman Farvardin 239

Cryptography III

The Simple Ideal Cipher System
Boris Ryabko 240
Better than "Optimum" Homophonic Substitution
Valdemar C. da Rocha Jr., James L. Massey 241
Collusion-Secure Fingerprinting and B_2-Sequences
Gérard Cohen, Simon Litsyn, Gilles Zémor 242
A Calculus of Conditional Independence and its Applications in Cryptography
Ueli Maurer 243

Blind Multi-User Detection Algorithms

Blind Identification of MIMO Systems Based on Source Correlative Filtering
João Xavier, Victor Neves Barroso 244
Blind Source Separation Based on Multi-User Kurtosis Criteria
Constantinos B. Papadias 245
Independent Component Analysis for Blind Multiuser Detections
Anthony Kuh, Xiaohong Gong 246
Blind Adaptive Multiuser Detection with Averaging for Cellular Systems
Deepak Das, Mahesh K. Varanasi 247

Block and Trellis Coded Modulation

Iterative Multistage Decoding of BCM Codes
Diana Stojanović, Shu Lin, Marc P.C. Fossorier 248
A New Block-Coded Modulation Scheme for Rayleigh Fading Channel, Soft Output Decoding Issues
Shahram Yousefi, Erik S. Hons, Amir K. Khandani, Brendan J. Frey 249
Iterative Viterbi Algorithm for Concatenated Multidimensional TCM
Qi Wang, Lei Wei 250
Trellis Coded Modulation with More than One Redundancy Bit
The Cuong Dinh, Takeshi Hashimoto 251

WEb – Wednesday, 11:20 - 12:40

Weights in Codes II

Hardness of Approximating the Minimum Distance of a Linear Code
Daniele Micciancio, Ilya Dumer, Madhu Sudan 252
On the Minimum Distance of some Quadratic-Residue Codes
Markus Grassl 253
On the probability of undetected error
Iiro Honkala, Tero Laihonen 254
Projective Systems and Higher Weights
Hans Georg Schaathun 255

Information Storage II (Coding for Magnetic Recording)

Nonquasicatastrophic Maximum Transition Run Codes
Roy Cideciyan, Evangelos Eleftheriou 256
Simple Soft-Output Detection for Magnetic Recording Channels
Emina Soljanin 257
Performance Bounds for High Rate Linear Codes over Partial Response Channels
Tolga M. Duman, Erozan Kurtas 258
Concatenated Runlength Limited Codes with Soft-Decision Decoding
Evelio Martín García Fernández, Renato Baldini Filho 259

Applications of Convolutional Codes

Pruned Convolutional Codes for Flexible Unequal Error-Protection Against Insertion/Deletion/Reversal Errors
B. Brink, H.C. Ferreira, W.A. Clarke 260
Free Distance Lower Bounds for Unequal Error-Protection Convolutional Codes
Tamar Danon, Shraga I. Bross 261
DC-Free Error-Correcting Codes Based on Convolutional Codes
Mao-Ching Chiu 262
DC-Free Binary Convolutional Coding
Tadashi Wadayama, A.J. Han Vinck 263

Source-Channel Coding I (cont.)

Improving the Performance of Variable-Length Encoded Systems Through Cooperation Between Source and Channel Decoders
Ahsun H. Murad, Thomas E. Fuja 264
Source Optimized Channel Codes (SOCCs) for Parameter Protection
Stefan Heinen, Peter Vary 265
Combined Source/Channel (De-)Coding: Can A Priori Information be used Twice?
Thomas Hindelang, T. Fingscheidt, N. Seshadri, R.V. Cox 266

Cryptography IV

Global Broadcast by Broadcasts Among Subsets of Players
Matthias Fitzi, Ueli Maurer 267
Performance of a Secure Wireless Transmission Method
Havish Koorapaty, Amer Hassan 268
A New Identity-based Conference Key Distribution Scheme
Sheng-bo Xu, Henk van Tilborg 269
An Information Theoretic Model for Distributed Key Distribution
Carlo Blundo, Paolo D'Arco 270

Joint Multi-User Detection Algorithms

Adaptive Joint Detection and Decoding in Flat-Fading Channels via Mixture Kalman Filtering
Rong Chen, Xiaodong Wang, Jun S. Liu 271
Adaptive Maximum Likelihood Multiuser Detection
Deva K. Borah, Predrag B. Rapajic 272
Adaptive Bayesan Multiuser Detection
Xiaodong Wang, Rong Chen 273
Joint Detection in Multi-User Systems via Iterative Processing
Christian Schlegel 274

Quantum Information Theory

Quantum Error Detection
Alexei Ashikhmin, Alexander Barg, Emanuel Knill, Simon Litsyn 275
Multiuser detection in a quantum channel
Julio I. Concha, H. Vincent Poor 276
Quantum Gaussian Channels
A. S. Holevo, O. Hirota 277
Quantum Arithmetic Coding
Isaac L. Chuang, Dharmendra S. Modha 278

THa – Thursday, 9:40 - 11:00

Information Storage III (Capacity of Multi-Dimensional Constrained Systems)

Positive Capacity Region of Two-dimensional Asymmetric Run Length Constrained Channels
Akiko Kato, Kenneth Zeger 279

New Upper and Lower Bounds on the Channel Capacity of Read/Write Isolated Memory
Mordecai J. Golin, Xuerong Yong, Yuanping Zhang, Li Sheng 280
Zero Capacity Region of Multidimensional Run Length Constraints
Hisashi Ito, Akiko Kato, Zsigmond Nagy, Kenneth Zeger 281
Upper Bound on the Capacity of Constrained Three-Dimensional Codes
Soren Forchhammer 282

Space-Time Code Constructions

Space-Time Codes Based on Hadamard Matrices
Martin Bossert, Ernst M. Gabidulin, Paul Lusina 283
Space-Time Codes Based on Rank Codes
Ernst M. Gabidulin, Martin Bossert, Paul Lusina 284
Extensions to the Theory of Differential Space-Time Modulation
Brian L. Hughes 285
Concatenation of Error-Correcting Codes and Multiple Transmit Antennas
Xiaodong Li, Harish Viswanathan, Howard Huang 286

Bounds on Code Performance

An Algorithm to Compute the Free Distance of Turbo Codes
Roberto Garello, Paola Pierleoni, Sergio Benedetto, Guido Montorsi 287
Upper bounds to error probabilities of coded systems beyond the cutoff rate
Dariush Divsalar, Ezio Biglieri 288
An Upper Bound on the Number of Errors Corrected by a Convolutional Code
Jørn Justesen 289
Bounds on the Maximum Likelihood Decoding Error Probability of Low Density Parity Check Codes
Gadi Miller, David Burshtein 290

Construction of Convolutional Codes

Punctured Recursive Convolutional Encoders and their Applications in Turbo Codes
Ba-Zhong Shen, Ara Patapoutian, Peter McEwen 291
On the Search for Self-Doubly Orthogonal Codes
Brice Baechler, David Haccoun, François Gagnon 292
On Rate-$k/2k$ Self-Dual Convolutional Codes
Ajay Dholakia 293
Construction Results for MDS-Convolutional Codes
Roxana Smarandache, Heide Gluesing-Luerssen, Joachim Rosenthal 294

Universal Lossless Source Coding

A Universal Lossless Resolution Scalable Progressive Image Code
John C. Kieffer, Ross Stites, En-Hui Yang 295
Data Compression Via Binary Decision Diagrams
John C. Kieffer, Philippe Flajolet, En-Hui Yang 296
On Modeling and Ordering for Embedded Image Coding
Erik Ordentlich, Marcelo J. Weinberger, Gadiel Seroussi 297
Universal Lossless Data Compression with Side Information by using a Conditional MPM Grammar Transform
En-Hui Yang, A. Kaltchenko, John C. Kieffer 298

Sequences I

Balanced and Almost Balanced Binary Sequences of Period $p^m - 1$ with Optimal Autocorrelation Using the Polynomial $(z+1)^d + az^d + b$ over $GF(p^m)$
Jong-Seon No, Habong Chung, Hong-Yeop Song, Kyeongcheol Yang, Jung-Do Lee, Tor Helleseth 299
Inverse Hadamard Transforms of Two-Level Autocorrelation Sequences
Guang Gong, Solomon W. Golomb 300
Crosscorrelation Functions of m-Sequences and their Decimation Sequences
Zhengtao Zhang, Wei Sun, Yixian Yang, Zhengming Hu, Xin Li 301

Constabent Properties of Golay-Davis-Jedwab Sequences
Matthew G. Parker 302

Outage Minimization for Fading Channels

Outage Analysis for Multiple Access Channel with Rayleigh Fading
Ido Bettesh, Shlomo Shamai (Shitz) 303
An MGF-Based Numerical Technique for the Outage Probability Evaluation of Diversity Systems
Young-Chai Ko, Mohamed-Slim Alouini, Marvin K. Simon 304
Minimum Outage Probability and Optimal Power Allocation for Fading Multiple-Access Channels
Lifang Li, Andrea J. Goldsmith 305
Error Bounds for the Amplitude Limited Flat Fading Channel
Walid K. M. Ahmed, Peter J. McLane 306

THb – Thursday, 11:20 - 12:40

Information Storage IV (Coding and Detection for Two-Dimensional Storage Devices)

Efficient Coding Schemes for the Hard-Square Model
Ron M. Roth, Paul H. Siegel, Jack K. Wolf 307
Two-Dimensional Codes for Second Order Spectral Null Constraints
Hiroshi Kamabe 308
Convolutional code and 2-Dimensional PRML Class IV for Multi-track Magnetic Recording System
Naoto Kogo, Norimichi Hirano, Ryuji Kohno 309
Demodulation Techniques for Full-Surface Data
William Weeks IV 310
Two-Dimensional Interleaving Schemes with Repetitions: Constructions and Bounds
Tuvi Etzion, Alexander Vardy 311

Aspects of Space-Time Codes

Space-Time Precoding with Imperfect Feedback
Eugene Visotsky, Upamanyu Madhow 312
Space-Time Autocoding: Arbitrarily Reliable Communication in a Single Fading Interval
Thomas L. Marzetta, Bertrand Hochwald, Babak Hassibi 313
A Rank Criterion for QAM Space-Time Codes
Youjian Liu, Michael P. Fitz, Oscar Y. Takeshita 314
EM-Based Sequence Estimation for Space-Time Codes Systems
Yingxue Li, Costas N. Georghiades, G. Huang 315

Iterative Decoding III

The Turbo Decoding Algorithm and its Phase Trajectories
Dakshi Agrawal, Alexander Vardy 316
Thresholds of Turbo Codes
Tom J. Richardson, Rüdiger Urbanke 317
Gaussian Approximation for Sum-Product Decoding of Low-Density Parity-Check Codes
Sae-Young Chung, Rüdiger Urbanke, Tom J. Richardson 318
Analysing the Turbo Decoder Using the Gaussian Approximation
Hesham El Gamal, A. Roger Hammons Jr. 319

Pattern Recognition and Detection

Performance Improvement in ATR from Dimensionality Reduction
Natalia A. Schmid, Joseph A. O'Sullivan 320
Principal Curves with Bounded Turn
Sathyakarma Sandilya, S.R. Kulkarni 321
Reduced-State BCJR-type Algorithms
Giulio Colavolpe, Gianluigi Ferrari, Riccardo Raheli 322

On Model Selection and Concavity for Finite Mixture Models
Igor V. Cadez, Padhraic Smyth 323

Universal Lossless Source Coding (cont.)

A Generalized Minmax Bound for Universal Coding
Jorma Rissanen 324
Universal Noiseless Codes for Sources of Arbitrary Entropy
Abraham Wyner, Dean Foster, Robert Stine 325
On the Redundancy of Universal Lossless Coding for General Piecewise Stationary Sources
Gil Shamir, Daniel J. Costello Jr. 326
On the Performance of Recency-Rank and Block-Sorting Universal Lossless Data Compression Algorithms
Jun Muramatsu 327

Sequences II

A new family of ternary sequences with ideal two-level autocorrelation function
Tor Helleseth, P. Vijay Kumar, Halvard Movik Martinsen 328
Ternary m-Sequences with Three-Valued Crosscorrelation Function: Two New Decimations
Hans Dobbertin, Tor Helleseth, P. Vijay Kumar, Halvard Movik Martinsen 329
Reverse-Complement Similarity Codes for DNA Sequences
Arkadii D'yachkov, Pavel A. Vilenkin, David Torney, P. Scott White 330
Golay Complementary Sequences for OFDM with 16-QAM
Cornelia Roessing 331

Parallel and Successive Interference Cancellation CDMA Receivers

Linear Parallel Interference Cancellation Using Fixed Weighting Factors for Long-Code CDMA
Dongning Guo, Lars K. Rasmussen 332
On CDMA Transmission over Mismatched Fading Channels employing MMSE-Receivers and Successive Cancellation
Alexander Lampe 333
On Linear Parallel Interference Cancellation
M. Motani, D.R. Brown, C.R. Johnson Jr., H. Vincent Poor 334
Adaptive Multiuser Parallel-Decision-Feedback with Iterative Decoding
Michael L. Honig, Graeme Woodward, Paul D. Alexander 335

THc – Thursday, 2:30 - 3:50

Further Results on Space-Time Codes

CDMA Coding and Decoding Methods for Space-Time Block Codes
Jifeng Geng, Li-chung Chu, Urbashi Mitra, Michael P. Fitz 336
Multiple Antennas and Representation Theory
Babak Hassibi, Bertrand Hochwald, Amin Shokrollahi, Wim Sweldens 337
The Expectation-Maximization Algorithm for Space-Time Communications
Carmela Cozzo, Brian L. Hughes 338
Further Results on the Algebraic Design of Space-Time codes
A. Roger Hammons Jr., Hesham El Gamal 339

Tail-Biting Codes

Best Tailbiting Convolutional Encoders Using a Priori Information
Marc Handlery, John B. Anderson 340
Searching for Tailbiting Codes with Large Minimum Distances
Irina E. Bocharova, Boris D. Kudryashov, Rolf Johannesson, Per Stahl 341
Decoding of Codes Based on Their Tail Biting Trellises
Rose Y. Shao, Shu Lin, Marc P.C. Fossorier 342
The Effect of the Tailbiting Restriction on Feedback Encoders
Per Stahl, John B. Anderson, Rolf Johannesson 343

Lossless Source Coding II

On Instantaneous Codes for Zero-Error Coding of Two Correlated Sources
Ying-On Yan, Toby Berger 344
Multi-Value Match Length Function for Data Compression
S. Mohammadali Khosravifard, M. Nasiri-Kenari 345
Asymptotic Properties on the Codeword Length Distribution of Optimal FV Codes for General Sources
Hiroki Koga, Hirosuke Yamamoto, Naoto Yamaguchi 346
Almost Surely Complete Parsing and Variable-to-Variable Length Coding
Mikihiko Nishiara, Hiroyoshi Morita 347

Channels with Side Information

Signaling for the Gaussian Channel with Side Information at the Transmitter
Frans M.J. Willems 348
Capacities of Time-V'arying Multiple-Access Channels with Side Information
Arnab Das, Prakash Narayan 349
Fourier and the White Gaussian Multiple-Access Channel with Feedback
Gerhard Kramer 350
Geometric Proof of Rate-Distortion Function of Gaussian Sources with Side Information at the Decoder
S. Sandeep Pradhan, Kannan Ramchandran 351

Sequences III

A Comparison of two schemes for generating DC-free RLL Sequences
Kees A. Schouhamer Immink, Wang Yong Hong Wilson 352
Design of Binary Sequences with Optimal Frame Synchronization Property
Young Joon Song 353
Random Number Generation via Homophonic Coding
Andrei Fionov 354

CDMA Receiver Design

A New Class of Multiuser CDMA Receivers Based on The Minimum Mean-Output-Energy Strategy
Stefano Buzzi, Marco Lops, Antonia Maria Tulino 355
MMSE Multiuser Detection for Noncoherent Non-Orthogonal Multipulse Modulation
Michael L. McCloud, Louis L. Scharf 356
A New Group Detection Strategy for DS/CDMA Systems
Stefano Buzzi, Marco Lops, Giuseppe Ricci 357
Adaptive Linear-Quadratic Receivers for Time-Varying, Frequency-Selective Code-Division-Multiple-Access Channels
Richard J. Barton, Jian-Jun Ni 358

Detection I

On Error-Free Filtering under Dependent Distortions
M.S. Pinsker, Vyacheslav V. Prelov 359
Recovery of Not Necessarily Band-Limited Signals from Noisy Observations
Adam Krzyzak, Ewaryst Rafajlowicz, Miroslav Pawlak 360
Linear Almost-Periodically Time-Variant Filtering of Generalized Almost-Cyclostationary Signals
Luciano Izzo, Antonio Napolitano 361

THd – Thursday, 4:10 - 5:30

Bounding Techniques for Space-Time Codes

Sphere Decoding of Space-Time Codes
Oussama Damen, Ammar Chkeif, Jean-Claude Belfiore 362
Space-Time Cut-off Rate for the Flat Rayleigh Fading Channel
Alfred O. Hero, Thomas L. Marzetta 363

Sphere Packing in the Grassmann Manifold: a Geometric Approach to the Noncoherent Multi-Antenna Channel
Lizhong Zheng, David N.C. Tse 364
Multiple-Antenna Signal Constellations for Fading Channels
Dakshi Agrawal, Thomas J. Richardson, Rüdiger Urbanke 365

Concatenated Coding

Extending the Evaluation of Serial Concatenated Turbo Code Performance to Longer Block Lengths
Andrew J. Viterbi, Audrey M. Viterbi 366
An Interactive Concatenated Turbo Coding System
Ye Liu, Heng Tang, Shu Lin, Marc P.C. Fossorier 367
Simultaneous zero-tailing of parallel concatenated codes
Marten van Dijk, Sebastian Egner, Ravi Motwani, Arie Koppelaar 368
Performance of Turbo Codes with a Single-Error Correcting BCH Outer Code
Hyun Cheol Kim, Pil Joong Lee 369

Huffman Coding

Asymptotic Average Redundancy of Huffman (and Shannon-Fano) Block Codes
Wojciech Szpankowski 370
Byte-oriented Decoding of Canonical Huffman Codes
Yakov Nekritch 371
A New Upper Bound on the Data Expansion of Huffman Codes
Jia-Pei Shen, John Gill 372
The complexity of minimum redundancy coding
Tjalling Tjalkens 373

Search Strategies

Some Results on the Classification of N Objects in M Classes with at Least c Objects in Each Class
Bruno Cernuschi-Frías 374
The Mastermind game and the rigidity of the Hamming space
Gregory Kabatianski, V.S. Lebedev, J. Thorpe 375
Strategy for Data Transmission over Binary Channels with Noiseless Feedback and Upper Bound on the Number of Questions in Searching with Lies
Vladimir Balakirsky 376
Perfect, Minimally Adaptive, Error-Correcting Searching Strategies
Ferdinando Cicalese, Daniele Mundici, Ugo Vaccaro 377

Sequences IV

Lower Bound on the Total Squared Correlation of the Bandwidth Constrained, Time-Limited Signal Sets
Ha Hoang Nguyen, E. Shwedyk 378
Design of Spread Spectrum Sequences Using Ergodic Theory
Chi-Chung Chen, Ezio Biglieri, K. Yao 379
Two-Dimensional Sequence Estimation
Richard E. Blahut, Loren E. Laybourn 380
Efficient Coding for High-Order Spectral-Null Sequences
Yan Xin, Ivan J. Fair 381

Asymptotic Analysis of Multi-User Systems

Distributions of the Output MAI of Linear MMSE Multiuser Receivers in DS-CDMA Systems
Junshan Zhang, Edwin K.P. Chong, David N.C. Tse 382
Alpha-Stable Models of Multiuser Interference
Brian L. Hughes 383
Asymptotic Performance of M-Estimator-Based Multiuser Detectors in Rayleigh Fading Non-Gaussian Channels
H. Vincent Poor, Mario Tanda 384
Large System Error Probability of Multiuser Decision Feedback Receivers
Rapeepat Ratasuk, Michael H. Honig 385

Detection II

Second Order Asymptotic Optimality of Sequential Design and Change-Point Detection
M.B. Malyutov, I.I. Tsitovich 386
Convex-Constrained Maximum-Likelihood Detection in CDMA
Peng Hui Tan, Lars K. Rasmussen, Teng Joon Lim 387
UMP, ALR and GLR Tests and Some Applications to Coherent Radar Detection
Mostafa Derakhtian, Mohammad M. Nayebi 388
Approximate Simultaneous Orthogonal Expansions. Applications to Mean-Square Estimation and Signal Detection Problems
Jesús Navarro-Moreno, Juan Carlos Ruiz-Molina, Antonia Oya 389

FRa – Friday, 9:40 - 11:00

Structure of Codes I

Maximal Number of Constant Weight Vertices of the Unit n-cube contained in a k-dimensional Subspace
Rudolf Ahlswede, H. Aydinian, L. Khachatrian 390
Constant-Weight Code Bounds from Spherical Code Bounds
Erik Agrell, Alexander Vardy, Kenneth Zeger 391
On the Covering Radius of Ternary Negacyclic Codes with Length up to 26
Tsonka Baicheva 392
Multicovering Bounds from Relative Covering Radii
Iiro Honkala, Andrew Klapper 393

Decoding Methods I

A Simple Decoding Algorithm for the $|24, 12, 8|$ extended Golay Code
I. Boyarinov, I. Martin, B. Honary 394
Limited-Trial Generalized Minimum Distance Decoding with Fixed Erasing
Jos Weber, Khaled A.S. Abdel-Ghaffar 395
An Improvement to GMD-like Decoding Algorithms
Hitoshi Tokushige, Takuya Koumoto, Tadao Kasami 396
Totally Self-Checking Decoders for Hamming SEC Codes
Igor M. Boyarinov 397

Performance and Analysis of Convolutional Codes

On the Decoding Bit Error Probability for Binary Convolutional Codes
Rolf Johannesson, James L. Massey, Per Stahl 398
An Analytical Technique for Exact Error State Probability in Soft Decision Viterbi Decoding
Hideki Yoshikawa, Ikuo Oka, Chikato Fujiwara 399
AWGN Channel Convolutional Decoding is less Complex than BSC Decoding
John B. Anderson 400
Symbol Reliability Estimation Using Code Trellis Degeneration for QLI Codes
Masato Tajima, Atsushi Hatano, Keiji Takida, Zenshiro Kawasaki 401

Source-Channel Coding II

Snake-in-the-Box Codes as Robust Quantizer Index Assignments
Sungill Kim, David L. Neuhoff 402
VQ-Based Hybrid Digital-Analog Joint Source-Channel Coding
Mikael Skoglund, Nam Phamdo, Fady Alajaji 403
Optimal Linear Labelling for the Minimisation of both Source and Channel Distortion
Jean-Claude Belfiore, Xavier Giraud, Jorge Rodriguez-Guisantes 404
Robust Signal Compression using Joint Fixed- and Variable-length Coding
Aydin Alatan, John W. Woods 405

Wireless Access Protocols

ARQ Protocols for the Gaussian Collision Channel
Giuseppe Caire, Daniela Tuninetti 406
Capacity of Time-Slotted ALOHA Systems
Muriel Médard, Sean P. Meyn, Jianyi Huang, Andrea J. Goldsmith 407
On Stability of DS-CDMA Data Networks with Code Combining
Rajiv Vijayakumar, Kimberly M. Wasserman 408
Buffer Control for Communication over Fading Channels
Randall Berry, Robert G. Gallager 409

Capacity of Fading Channels and Optical Channels

Capacity of PPM on Gaussian and Webb Channels
Sam Dolinar, D. Divsalar, J. Hamkins, F. Pollara 410
Capacity of multiple-antenna Rayleigh channel with a limited transmit diversity
Alexei Gorokhov 411
Channel Capacity in Evenly Correlated Rayleigh Fading with Different Adaptive Transmission Schemes and Maximal Ratio Combining
Ranjan K. Mallik, Moe Z. Win 412
Capacity of nearly-decomposable Markovian fading channels under asymmetric receiver-sender side information
Muriel Médard, R. Srikant 413

Estimation and Filtering

Rényi Information Divergence via Measure Transformations on Minimal Spanning Trees
Alfred O. Hero, Olivier J.J. Michel 414
On the Interpretation of the APP Algortihm as an LLR Filter
Ingmar Land, Peter Hoeher, Ulrich Sorger 415
Minimum Bandwidth Basis Functions for the Fourth-Moment Bandwidth Measure
Eric A. Fain, Mahesh K. Varanasi 416
Neuro-Dynamic Programming and Rollout Algorithms. An Overview
Dimitri P. Bertsekas 417

FRb – Friday, 11:20 - 12:40

Decoding Methods II

A system-theoretic derivation of the Welch-Berlekamp algorithm
Margreet Kuijper 418
Very High-Speed Reed-Solomon Decoders
Dilip V. Sarwate, Naresh R. Shanbhag 419
Euclid's Algorithm and LFSR synthesis
Parampalli Udaya 420
On Syndrome Generation and Error Location Search in the Decoding of Hermitian Codes
Chung-Chin Lu, Heng-Shun Wang, Jia-Pyn Chen 421

Efficient Decoding of Binary Codes

An All-Analog Ring Network for Turbo-Detection of Convolutionally Encoded DPSK Signals
Joachim Hagenauer, Andrew Schaefer, Christian Weiss 422
On the Efficiency of Some Suboptimal Algorithms for Bit Decoding of Binary Codes
Elke Offer, Emina Soljanin 423
An Efficient MAP Decoding Algorithm Using a Section Trellis Diagram
Ryujiro Shibuya, Yuichi Kaji, Tadao Kasami 424
On the Analog Implementation of the APP (BCJR) Algorithm
Matthias Mörz, Joachim Hagenauer, Elke Offer 425

Fix-Free and Error Recovering Codes

On Fix-Free Codes
Chunxuan Ye, Raymond W. Yeung 426
Variable-Rate Codes for Synchronization with Timing
Navin Kashyap, David L. Neuhoff 427
Error Containment in Compressed Data Using Sync Markers
Aaron Kiely, Sam Dolinar, Matthew Klimesh, Adina Matache 428
Error Recovery for Ziv-Lempel Coding by Using UEP Schemes
Eiji Fujiwara, Hongyuan Chen, Masoto Kitakami 429

Channel Capacity and Coding

Optimal Encoding Over Uncertain Channels with Decoding Delay Constraints
Philip A. Whiting, Edmund Yeh 430
Competitive Equilibrium in the Gaussian Interference Channel
Wei Yu, John M. Cioffi 431
Capacity-Achieving Distributions for Non-Gaussian Additive Noise Channels
Arnab Das 432
The Binary Jitter Channel: A New Model for Magnetic Recording
Dieter Arnold, Aleksandar Kavcic, Ralf Kötter, H.-A. Loeliger, Pascal O. Vontobel 433

Wireless Sensor Networks

The Traffic Carrying Capacity of Wireless Networks
P. Gupta, P.R. Kumar 434
Sequential Signal Encoding and Estimation for Wireless Sensor Networks
Haralabos C. Papadopoulos 435
Information Theory of Wireless Sensor Networks: the n-helper Gaussian Case
Mohiuddin Ahmed, Gregory Pottie 436
Optimal Binary Distributed Detection
Wei Shi, Thomas W. Sun, Richard Wesel 437

Spectral Efficiency of CDMA Systems

CDMA with fading: Effective bandwidth and spreading-coding tradeoff
Ezio Biglieri, Giuseppe Caire, Giorgio Taricco, Emanuele Viterbo 438
Spectral efficiency of Low-Complexity Multiuser Detectors
Ralf R. Müller, Sergio Verdú 439
Evaluation of the Spectral Efficiency of Spread-Spectrum Multiple-Access Systems
Maja Bystrom, J.W. Modestino 440
Asymptotic Analysis of Data-Aided Channel Estimation Algorithms for Synchronous CDMA Systems
Jamie S. Evans 441

Signal Processing I

On Minimal α-Mean Error Parameter Transmission Over Poisson Channel
Marat Burnashev, Yury Kutoyants 442
Real-Time ARMA Identification in the Case of Missing Observations
Élisabeth Lahalle, Gilles Fleury, Jacques Oksman 443
Fault-Tolerant Dynamic Systems
Christoforos Hadjicostis, G.C. Verghese 444
On the Necessary Density for Spectrum-blind Nonuniform Sampling
Michael Gastpar, Yoram Bresler 445

FRc – Friday, 2:30 - 3:50

Decoding Methods III

Decoding the 6-error-Correcting Z_4-linear Calderbank-McGuire code
Jyrki Lahtonen 446

On Algebraic Decoding of the Z_4-Linear Goethals-Like Codes
Kalle Ranto 447
Gröbner Bases and Alternant Codes over Galois Rings
Eimear Byrne, Patrick Fitzpatrick 448
$O(\log_2 m)$ Iterative Algorithm for Multiplicative Inversion in $GF(2^m)$
Sumio Morioka, Yasunao Katayama 449

Design of Interleavers for Turbo Codes

Interleavers for Unpunctured Symmetric Turbo Codes
Johann A. Briffa, Victor Buttigieg 450
Interleaver Design Using Backtracking and Spreading Methods
Marco Breiling, Stein Peeters, Johannes B. Huber 451
An Interleaver Design Algorithm based on a Cost Matrix for Turbo Codes
Didier Le Ruyet, Hong Sun, Han Vu Thien 452
Interleaver design for Turbo codes
Hamid R. Sadjadpour, N.J.A. Sloane, G. Nebe, M. Salehi 453

Random Number Generation

Source Code with Cost as a Nonuniform Random Number Generator
Te Sun Han, Osamu Uchida 454
Random Number Approximation Problem for Discrete Memoryless Sources
Yasutada Oohama 455
On Rate of Source Conversion by Concatenating Code/Parse Trees
Hiroyoshi Morita, Kingo Kobayashi, Mamoru Hoshi 456
Almost Sure Convergence Theorems of Rate of Coin Tosses for Random Number Generation by Interval Algorithm
Tomohiko Uyematsu, Fumio Kanaya 457

Gaussian Channels

A new upper bound on the reliability function of the Gaussian channel
A. Ashikhmin, Alexander Barg, Simon Litsyn 458
AWGN Coding Theorems from Ensemble Weight Enumerators
Dariush Divsalar, Sam Dolinar, Hui Jin, Robert J. McEliece 459
Gaussian ISI Channels and the Generalized Likelihood Ratio Test
Amos Lapidoth, Emre Telatar 460
Lower Bound to the Feedback Capacity of the Colored Gaussian Noise Channel
Thierry Klein, Robert G. Gallager 461

Cryptography V

Traitor Traceable Signature Scheme
Yuji Watanabe, Yuliang Zheng, Hideki Imai 462
An Efficient Traitor Tracing Scheme for Broadcast Encryption
Maki Yoshida, Toru Fujiwara 463
Inherently Large Traceability of Broadcast Encryption Scheme
Kaoru Kurosawa, Takuya Yoshida, Yvo Desmedt 464
Reducing Oblivious String Transfer to Universal Oblivious Transfer
Stefan Wolf 465

Resource Allocation and Power Control for Multi-User Systems

Asymptotically Optimal Waterfilling in Multiple Antenna Multiple Access Channels
Pramod Viswanath, David N.C. Tse, Venkat Anantharam 466
A Resource Pooling Result for a CDMA Antenna Array
Stephen V. Hanly, David N.C. Tse 467
Optimal Dynamic Power Control for CDMA Systems
Jean-François Chamberland, Venugopal V. Veeravalli 468
Admission Control and Resource Allocation for DS-CDMA Networks with Multiple Traffic Classes
Rong-Rong Chen, Upamanyu Madhow 469

Signal Processing II

Evaluation for Convergence of Wavelet-Based Estimators on Fractional Brownian Motion
Shuhji Kawasaki, Hiroyoshi Morita 470
A New Reverse Jacket Transform based on Hadamard Matrix
Moon Ho Lee 471
Generalized Sylvester-Type Hadamard Matrices
Jong-Seon No, Hong-Yeop Song 472
Local LDP for the Shape of Random Young Diagram with Restrictions on Length and Height of Steps
Volodia Blinovsky 473

FRd – Friday, 4:10 - 5:30

Structure of Codes II

Local and Interweight Spectra of Perfect Binary Codes
A. Yu Vasil'eva 474
Some Results on Symbol Error-Correcting Codes
C.L. Chen 475
A New Scheme for Building Good Self-Dual Block Codes
Jean-Claude Carlach, Ayoub Otmani, Cyril Vervoux 476
Watermark Codes: Reliable Communication over Insertion/Deletion Channels
Matthew C. Davey, David J.C. MacKay 477

List Decoding

Fast Computation of Roots of Polynomials over Function Fields and Fast List Decoding of Algebraic Geometric Codes
Xin-Wen Wu, Paul H. Siegel 478
A fast interpolation method for list decoding of RS and algebraic-geometric codes
Shojiro Sakata, Yukio Numakami, Masaya Fujisawa 479
Bounds on List Decoding of MDS Codes
Jørn Justesen, Tom Hoeholdt 480
Vector symbol decoding with list inner symbol decisions
John J. Metzner 481

Iterative Decoding IV

Selectable Delay Turbo Decoding
Stephen G. Wilson, Munevver Kaya 482
Soft Output Viterbi Algorithm (SOVA) for Non-binary Turbo Codes
Jun Tan, Gordon L. Stüber 483
Convergence Analysis of Turbo-Decoding of Product Codes
Assaf Sella, Yair Be'ery 484
Turbo-Decoding as a Numerical Analysis Problem
Pär Moqvist, Tor M. Aulin 485

Some Special Transmission Problems

Efficient Reconstruction at the Output of a Discrete Memoryless Channel
Vladimir I. Levenshtein 486
Multi-Resolution Channel Codes
Hanying Feng, Michelle Effros 487
Transmission of a Slowly Varying Markov Signal over Memoryless Channels
Mark S. Pinsker, V.V. Prelov, Edward C. van der Meulen 488
Splitting the Scheduling Headache
Kevin Foltz, Jehoshua Bruck 489

Properties of Information Measures

Information projections revisited
Imre Csiszár, Frantisek Matús 490
Properties of the Information Value Decomposition
Joseph A. O'Sullivan 491
A Group-Theoretic Approach to Information Inequalities
Ho-leung Chan, Raymond W. Yeung 492
Toward a Theory of Information Processing
Sinan Sinanovic, Don H. Johnson 493

Multi-Access For Fading Channels

Minimizing Transmit Power for Fading Multiple-Access Channels
Michael Mecking 494
On Multi-Antenna Receiver Principles for Correlated Rayleigh Fading Channels
Anders Hansson, Tor M. Aulin 495
Achievable rate region for spatial multiplexing systems using the MMSE criterion
Hemanth Sampath, Arogyaswami Paulraj 496
Error Control Coding Schemes for Multiple Channels
Ahmed Mokhtar, Amer Hassan 497

Stochastic Processes

On the Linear Structure of Self-Similar Processes
Carl J. Nuzman, H. Vincent Poor 498
Analytic Variations on the Redundancy Rates of Renewal Processes
Philippe Flajolet, Wojciech Szpankowski 499
"Any-time" Capacity and A Separation Theorem For Tracking Unstable Processes
Anant Sahai 500
On an Identification Algorithm of a Markov Chain
Tohru Kohda, Hiroshi Fujisaki 501

On polynomial invariants of codes, matroids, and the partition function

A. Barg
Bell Labs, Lucent Technologies
Murray Hill, NJ 07974, USA
and IPPI RAN, Moscow
abarg@research.bell-labs.com

Abstract — **A linear code can be thought of as a vector matroid represented by the columns of code's generator matrix; a well-known result in this context is Greene's theorem on a connection of the weight polynomial of the code and the Tutte polynomial of the matroid. We examine this connection from the coding-theoretic viewpoint, building upon the rank polynomial of the code. This enables us**

- **to relate the weight polynomial of codes and the reliability polynomial of linear matroids and to prove new bounds on the latter;**
- **to prove that the partition polynomial of the Potts model equals the weight polynomial of the cocycle code of the underlying graph, and**
- **to give a simple proof of Greene's theorem and its generalization.**

I. INTRODUCTION

Let C be a linear code of length n and let $E = \{1, 2, \dots, n\}$ be its coordinate set. The weight polynomial of C is defined as $\mathcal{A}(x,y) = \sum_{i=0}^{n} A_i x^{n-i} y^i$, where $\mathcal{A}_i$ is the number of vectors of Hamming weight i in C. Let G be a generator matrix of C. By $G(F)$ we denote the submatrix of G formed by the columns with numbers in $F \subset E$. The *rank polynomial* of C is defined as $\mathcal{U}(x,y) = \sum_{u=0}^{n} \sum_{v=0}^{k} \mathcal{U}_u^v x^u y^v$, where

$$\mathcal{U}_u^v = |\{F \subseteq E \mid |F| = u, \mathrm{rk}(\mathbf{G}(F)) = v\}|$$

The polynomials $\mathcal{A}(x,y)$ and $\mathcal{U}(x,y)$ are connected by the following relation, equivalent to Greene's theorem [3].

Theorem 1:

$$\mathcal{A}(x,y) = y^n |C| \mathcal{U}\Big(\frac{x-y}{y}, \frac{1}{q}\Big) \tag{1}$$

The code C can be also thought of as a (vector) matroid M represented by the column space of G; so given M, we call C the code of M, denoted $C(M)$.

II. RELIABILITY POLYNOMIAL

Let M be a linear matroid of rank k on the ground set E of size n defined by its representation over $\mathbb{F}_q$ and let $\mathcal{U}_i^i$ be its number of independent sets of size i. The *(all-terminal) reliability polynomial* of M, by definition, is

$$\mathcal{R}(M; x, y) := \sum_{i=0}^{k} \mathcal{U}_i^i x^{n-i} y^i. \tag{2}$$

The terminology is motivated by the special case of cographic matroids. Namely, let $G(V,E)$ be a connected graph and let M be a matroid whose independent sets are given by subsets of edges whose removal does not make G disconnected. Suppose that each edge in E is removed with probability p. Then the probability that upon completion of this process the graph remains connected is given by $\mathcal{R}(M; p, 1-p)$. Reliability of graphs and matroids has been a subject of continued interest in combinatorics [2]. The main result of this section is:

Theorem 2: *Let $\mathcal{A}(x,y)$ be the weight polynomial of the linear code $C(M)$. Then*

$$\mathcal{R}(M; p, 1-p) \le \mathcal{U}_k^k p^{n-k} (1-p)^k + \mathcal{A}(1,p) - 1. \tag{3}$$

In this way the reliability polynomial can be related to the probability of undetected error for linear codes; the upper bounds on the latter are used in the paper to derive new upper bounds on $\mathcal{R}(M; p, 1-p)$.

III. PARTITION FUNCTION

Let $\Gamma = (V, E)$ be a finite graph with $|E| = n$ edges and $c(\Gamma)$ connected components. Consider the Potts model of interaction for a physical system represented by Γ [4]. Under this model each vertex in V can be in one of q possible states; an allocation of states to all the vertices defines a state σ of the system or a coloring of V with q colors. The partition function of the Potts model is defined as follows:

$$Z(y) = \sum_{\sigma} y^{-|U(\sigma)|},$$

where the sum is over all possible states σ of the system and $U(\sigma)$ is the subset of edges with both ends of the same color.

Theorem 3: *Let $\mathcal{A}(x,y)$ be the weight polynomial of the q-ary cocycle code of Γ. Then*

$$\mathcal{A}(1,y) = q^{-c(\Gamma)} y^n Z(y).$$

Further details are found in [1]

REFERENCES

[1] A. Barg, "On polynomial invariants of codes, matroids, and the partition function," DIMACS Report 99-54 (http://dimacs.rutgers.edu/TechnicalReports).

[2] C. J. Colbourn, *The combinatorics of network reliability*, Oxford Univ. Press, New York, 1987.

[3] C. Greene, *Weight enumeration and the geometry of linear codes*, Stud. Appl. Math. **55** (1976), 119–128.

[4] D. J. A. Welsh, *Complexity: knots, colourings and counting*, LMS Lect. Notes Series, vol. 186, Cambridge Univ. Press, 1993.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On the Hensel Lift of a Polynomial

Zhe-Xian Wan
Dept of Information Technology
Lund University
P.O. Box 118
SE-221 00 Lund, Sweden
e-mail: wan@it.lth.se

Abstract — **Denote by R the Galois ring of characteristic p^e and cardinality p^{em}, where p is a prime and e and m are positive integers. Let $g(x)$ be a monic polynomial over $\mathbb{F}_{p^m}$. A polynomial $f(x)$ over R is defined to be a Hensel lift of $g(x)$ in $R[x]$ if $\overline{f}(x) = g(x)$, where $-$ is the natural homomorphism from R onto $\mathbb{F}_{p^m}$, and there is a positive integer n not divisible by p such that $f(x)$ divides $x^n - 1$ in $R[x]$. It is proved that $g(x)$ has a unique Hensel lift in $R[x]$ if and only if $g(x)$ has no multiple roots and $x \nmid g(x)$. An algorithm to compute the Hensel lift is also given.**

I. Definition

In 1995 the following definition of the Hensel lift of a polynomial appeared in [1].

Let $h_2 \in \mathbb{F}_2[x]$ be of degree $m > 0$ and assume that $h_2|(x^l - 1)$ and l is minimal subject to this property. There is a unique monic polynomial $h \in \mathbb{Z}_4[x]$ of degree m such that $\overline{h} = h_2$ and $h|(x^l - 1)$ in $\mathbb{Z}_4[x]$. This polynomial is called the Hensel lift of $h_2(x)$.

In the above definition the condition that l is odd should be added. A counter-example when l is even is: $h_2(x) = (x-1)^2(x^2+x+1)$, $h_2 \mid (x^6-1)$ in $\mathbb{F}_2[x]$, $h = (x^2-1)(x^2+x+1)$ and $h' = (x^2-1)(x^2-x+1)$.

The formulation of the above definition involves some statements which should be proved. Now we suggest a simpler definition which can be formulated for an arbitrary Galois ring. For Galois rings, see [2] and [3].

Let $g(x)$ be a monic polynomial over $\mathbb{F}_{p^m}$. A monic polynomial $f(x)$ over R is called a **Hensel lift** of $g(x)$ if $\overline{f}(x) = g(x)$ and there is a positive integer n not divisible by p such that $f(x)|(x^n - 1)$ in $R[x]$.

II. Existence and Uniqueness

Proposition 1. A monic polynomial $g(x)$ over $\mathbb{F}_{p^m}$ has a Hensel lift $f(x)$ over R if and only if $g(x)$ has no multiple roots and $x \nmid g(x)$ in $\mathbb{F}_{p^m}[x]$.

Lemma 2. Let n_1 and n_2 be positive integers and $n = \gcd(n_1, n_2)$. Then $x^n - 1 = \gcd(x^{n_1} - 1, x^{n_2} - 1)$ in $\mathbb{F}_{p^m}[x]$, $(x^n - 1)|(x^{n_1} - 1)$ in $R[x]$, and $(x^n - 1)|(x^{n_2} - 1)$ in $R[x]$.

Proposition 3. Let $g(x)$ be a monic polynomial over $\mathbb{F}_{p^m}$ without multiple roots and $x \nmid g(x)$ in $\mathbb{F}_{p^m}[x]$. Then $g(x)$ has a unique Hensel lift in $R[x]$.

III. An Algorithm to Compute the Hensel Lift

Based on Propositions 1 and 3 of the proceeding section we formulate the following algorithm for computing the Hensel lift of a monic polynomial over $\mathbb{F}_{p^m}$ in $R[x]$.

Algorithm Given a monic polynomial $g(x)$ of degree > 0 over $\mathbb{F}_{p^m}$ to compute the Hensel lift of $g(x)$ in $R[x]$ we proceed in the following steps.

1. Test whether $x|g(x)$ in $\mathbb{F}_{p^m}[x]$.
   If yes, we are finished and $g(x)$ has no Hensel lift in $R[x]$.
   If no, go to step 2.
2. Compute $\gcd(g(x), g'(x))$ and let it be $d(x)$.
   If $\deg d(x) > 0$, we are finished and $g(x)$ has no Hensel lift in $R[x]$.
   If $\deg d(x) = 0$, go to step 3.
3. Factorize $g(x)$ into a product of distinct monic irreducible polynomials over $\mathbb{F}_{p^m}$ by Berlekamp's Algorithm. Let the result be
   $$g(x) = g_1(x)g_2(x)\dots g_r(x),$$
   where $g_1(x), g_2(x), \dots, g_r(x)$ are distinct monic irreducible polynomial over $\mathbb{F}_{p^m}$. Let $\deg g_i(x) = n_i, i = 1, 2, \dots, r$ and go to step 4.
4. Compute $\mathrm{lcm}[p^{mn_1} - 1, p^{mn_2} - 1, \dots, p^{mn_r} - 1]$. Let the result be n, then p does not divide n and $g(x)|(x^n - 1)$. Go to step 5.
5. Divide $x^n - 1$ by $g(x)$ by division algorithm. Let the quotient be $g_1(x)$. Then $x^n - 1 = g(x)g_1(x)$ and $\gcd(g(x), g_1(x)) = 1$. Go to step 6.
6. By the constructive proof of Hensel's Lemma construct two coprime monic polynomials $f(x)$, $f_1(x) \in R[x]$ such that $x^n - 1 = f(x)f_1(x)$ in $R[x]$ and $\overline{f}(x) = g(x), \overline{f}_1(x) = g_1(x)$. Then $f(x)$ is the Hensel lift of $g(x)$ in $R[x]$. □

When $\mathbb{F}_{p^m} = \mathbb{F}_2$ and $R = \mathbb{Z}_4$, the Hensel lift of a polynomial $g(x)$ over $\mathbb{F}_2$ without multiple roots and not divisible by x can be calculated by using Graeffe's method for finding a polynomial whose roots are the squares of the roots of $g(x)$, see [4] and [5].

References

[1] Bonnecaze, A., Sole, P, and Calderbank, A. R., "Quaternary quadratic residue codes and unimodular lattices," *IEEE Trans. Inform. Theory* **41**(1995), 366–377.

[2] Krull, W., "Algebraische Theorie der Ringe," *Math. Ann.* **92**(1924), 183–213.

[3] MacDonald, B. R., *Finite Rings with Identity*, Marcel Dekker, 1974.

[4] Uspensky, J. V., *Theory of Equations*, McGraw-Hill, 1948.

[5] Wan, Z.-X., *Quaternary Codes*, World Scientific, Singapore, 1997.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On Superimposed Codes Based on Incidence Systems

Antony J. Macula
State University of New York
College at Geneseo
Department of Mathematics
Geneseo, NY, 14454, USA
e-mail: macula@geneseo.edu

Pavel A. Vilenkin[1]
Moscow State University
Faculty of Mechanics & Mathematics
Department of Probability Theory
Moscow, 119899, Russia
e-mail: paul@vilenkin.dnttm.ru

Abstract — **Binary superimposed codes were introduced by W.H.Kauts and R.C.Singleton in 1964 [1]. In [2] a concept of superimposed code distance was suggested. In 1996 a new construction based on the incidence of the finite sets was suggested [3]. It was studied and generalized in [4, 5]. We consider the further extension of this construction, which allows to create new superimposed codes from the existing ones. We also find the superimposed distance for this construction. Part of this work was presented in [6].**

I. Notations and Definitions

Definition 1. An *incidence system* is a triplet $\mathcal{I} = (\mathcal{A}, \mathcal{B}, \prec)$, where $\mathcal{A}$ and $\mathcal{B}$ are finite sets and $\prec$ is an incidence relation between them, i.e. for any $\mathbf{a} \in \mathcal{A}$ and $\mathbf{b} \in \mathcal{B}$ either $\mathbf{a} \prec \mathbf{b}$, or $\mathbf{a} \not\prec \mathbf{b}$. Put $N = N(\mathcal{I}) \triangleq |\mathcal{A}|$ and $t = t(\mathcal{I}) \triangleq |\mathcal{B}|$. An *incidence matrix* of $\mathcal{I}$ is binary $N \times t$ matrix $X(\mathcal{I})$, which rows and columns are indexed by elements $\mathbf{a} \in \mathcal{A}$ and $\mathbf{b} \in \mathcal{B}$, respectively, and an element $x_{\mathbf{a}}(\mathbf{b}) = 1$ iff $\mathbf{a} \prec \mathbf{b}$.

For an incidence system $\mathcal{I}$ and an integer $s \geq 0$ put

$$\mathcal{P}_s(\mathcal{I}) \triangleq \left\{(\tau, \mathbf{b}) : \tau \subset \mathcal{B}, |\tau| \leq s, \mathbf{b} \in \mathcal{B} \backslash \tau\right\}.$$

Definition 2. A pair $(\tau, \mathbf{b}) \in \mathcal{P}_s(\mathcal{I})$ is called *disjunctive* if the *disjunctive set* of this pair $\mathbf{D}(\tau, \mathbf{b}) \neq \varnothing$, where

$$\mathbf{D}(\tau, \mathbf{b}) \triangleq \left\{\mathbf{a} \in \mathcal{A} : \mathbf{a} \prec \mathbf{b}, \mathbf{a} \not\prec \mathbf{b}' \text{ for } \mathbf{b}' \in \tau\right\}.$$

Definition 3. For a system $\mathcal{I}$ and an integer $s \geq 0$ the value

$$\mathcal{D}_s(\mathcal{I}) \triangleq \min_{(\tau, \mathbf{b}) \in \mathcal{P}_s(\mathcal{I})} |\mathbf{D}(\tau, \mathbf{b})|$$

is called the *superimposed s-distance* of $\mathcal{I}$.

Definition 4. If a superimposed s-distance $\mathcal{D}_s(\mathcal{I}) > 0$ (i.e. all pairs $(\tau, \mathbf{b}) \in \mathcal{P}_s(\mathcal{I})$ are disjunctive) then $\mathcal{I}$ is called an *s-disjoint system.* In this case the incidence matrix $X(\mathcal{I})$ is called a *superimposed code* of *strength* s, *size* $t(\mathcal{I})$ and *length* $N(\mathcal{I})$ [1, 2]. The value $\mathcal{D}_s(\mathcal{I})$ is called the *superimposed distance* of this code [2].

II. Description of the Construction

Let $n > m \geq h \geq 1$ be integers and $I_k \triangleq (A_k, B_k, \prec_k)$ be arbitrary incidence systems, $1 \leq k \leq n$. In this section we define a new incidence system $\mathcal{I} = \mathcal{I}(n, m, h, I_1, \ldots, I_n)$.

Consider a new *zero* symbol "0". For each $k = 1, \ldots, n$ define the new incidence system $I_k^0 \triangleq (A_k^0, B_k^0, \prec_k^0)$, where $A_k^0 \triangleq A_k \cup \{0\}$, $B_k^0 \triangleq B_k \cup \{0\}$, and the relation $\prec_k^0$ is defined as follows: 1) $0 \prec_k^0 b$ for any $b \in B_k^0$; 2) $a \not\prec_k^0 0$ for any $a \in A_k$; 3) at the sets A_k and B_k relation $\prec_k^0$ is the same as $\prec_k$.

Put $\mathcal{I}(n, m, h, I_1, \ldots, I_n) \triangleq (\mathcal{A}, \mathcal{B}, \prec)$, where the sets

$$\mathcal{A} \triangleq \left\{\mathbf{a} = (a_1, \ldots, a_n) : a_k \in A_k^0, |\mathbf{a}| = h\right\},$$
$$\mathcal{B} \triangleq \left\{\mathbf{b} = (b_1, \ldots, b_n) : b_k \in B_k^0, |\mathbf{b}| = m\right\},$$

where $|\mathbf{a}|$ and $|\mathbf{b}|$ denote the number of non-zero components in vectors $\mathbf{a}$ and $\mathbf{b}$, respectively, and the incidence relation $\prec$ between $\mathcal{A}$ and $\mathcal{B}$ is defined component-wise, i.e. $\mathbf{a} \prec \mathbf{b}$ if and only if $a_k \prec_k^0 b_k$ for all $k = 1, \ldots, n$.

This construction generalizes those which were considered before [3, 4, 5].

III. Properties of $\mathcal{I} = \mathcal{I}(n, m, h, I_1, \ldots, I_n)$

Theorem 1. *Assume that $1 \leq s \leq h$ and the system I_k is s-disjunct for all $k \in \{1, \ldots, n\}$. Then $\mathcal{I}$ is also s-disjunct.*

Theorem 2. *Assume that $s \geq 1$ and the system $\mathcal{I}$ is s-disjunct. Then I_k is also s-disjunct for each $k \in \{1, \ldots, n\}$.*

For positive integers s and h denote by $\mathcal{V}_h(s)$ the set of vectors $\mathbf{v} = (v_1, \ldots, v_h)$, which components v_k are non-negative integers, and the sum $v_1 + \cdots + v_h = s$. For each vector $\mathbf{v}$ denote by $|\mathbf{v}|$ the number of positive components v_k.

Theorem 3. *Let $n > m \geq h \geq 1$ be integers and I be an arbitrary incidence system. For any $s \geq 1$ the superimposed s-distance of the incidence system $\mathcal{I} = \mathcal{I}(n, m, h, I, \ldots, I)$ has the form*

$$\mathcal{D}_s(\mathcal{I}) = \min \binom{m - |\mathbf{v}|}{h - |\mathbf{v}|} \prod_{k=1}^{h} \mathcal{D}_{v_k}(I),$$

where the minimum is taken over all vectors $\mathbf{v} \in \mathcal{V}_h(s)$, for which $|\mathbf{v}| \leq s$.

In general case, when the systems I_k are not the same, the formula for $\mathcal{D}_s(\mathcal{I})$ can be found in [6].

References

[1] W. H. Kauts and R. C. Singleton, "Nonrandom Binary Superimposed Codes," *IEEE Trans. Inform. Theory*, vol. 10, pp. 363–377, 1964.

[2] A. G. D'yachkov, V. V. Rykov and A. M. Rashad, "Superimposed Distance Codes," *Prob. of Control and Inform. Theory*, vol. 18, pp. 237–250, 1989.

[3] A. J. Macula, "Simple Construction of d-disjunct Matrices with Certain Constant Weights," *Discrete Mathematics*, vol. 162, pp. 311–312, 1996.

[4] P. A. Vilenkin, "On Constructions of List–Decoding Superimposed Codes," *Proc. of ACCT-6*, Pskov, Russia, 1998, pp. 228–231.

[5] A. G. D'yachkov, A. J. Macula, V. V. Rykov and P. A. Vilenkin, "Probabilistic q-ary Nonadaptive Group Testing and DNA Library Screening in the Absence and Presence of Errors," To appear in *J. of Stat. Planning and Inference.*

[6] P. A. Vilenkin, "One Construction of Superimposed Codes," *Proc. of Conference "Paul Erdos and His Mathematics"*, Budapest, Hungary, 1999, pp. 259–264.

[1]The work of P. Vilenkin was supported by the Russian Foundation of Basic Research, grant 98-01-00241.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Communication Complexity and Association Schemes

Ulrich Tamm
Dept. of Mathematics
Univ. of Bielefeld
P. O. Box 100131
33501 Bielefeld, Germany
tamm@mathematik.uni-bielefeld.de

I. Introduction

Let $D_0, \ldots, D_n$ be the $\{0,1\}$-matrices forming an association scheme. Since $\sum_{k=0}^{n} D_k$ is the all-one matrix, a linear combination $\sum_{k=0}^{n} c_k D_k$ can be regarded as the matrix $(f(x,y))_{x,y}$ representing the function f defined by $f(x,y) = c_k$ if (x,y) is in relation corresponding to matrix D_k. Parameters of functions thus obtained may now be studied exploiting properties of the association scheme.

One such parameter is the communication complexity $C(f)$, which is the number of bits that two persons have to exchange in order to evaluate $f(x,y)$, when initially one person only knows x and the other person only knows y. Communication complexity turned out to be an important topic in computer science, cf. [4]. Connections between communication complexity and information theory are discussed in [2] and [3]. The function under consideration is the function

$$f(x,y) = \begin{cases} 1 & \text{if } x,y \text{ are in relation } k, k \text{ odd} \\ 0 & \text{if } x,y \text{ are in relation } k, k \text{ even} \end{cases}$$

The communication complexity can be excatly determined if for $z = 0, 1$ all eigenvalues of the matrices

$$M_z(f) = \sum_{k \equiv z \bmod 2} D_k$$

are different from 0. Already in [5] we derived the following identity for the Krawtchouk polynomials $K_k(i,q,n)$.

Theorem 1 [5]: For $z = 0, 1$ it is

$$\sum_{k \equiv z (\bmod 2)} K_k(i,q,n) = \begin{cases} \frac{1}{2}(q^n + (-1)^z(2-q)^n) & i = 0 \\ (-1)^z 2^{i-1}(2-q)^{n-i+1} & i \geq 1 \end{cases}$$

The idea of proof in [6] is to exploit the simultaneous diagonalizability of the matrices $D_0, \ldots, D_n$ of the association scheme and a recurrence formula for their eigenvalues due to Delsarte [1]

$$F(i,k,n) = b^k F(i-1,k,n-1) - b^{k-1} F(i-1,k-1,n-1)$$

The Krawtchouk polynomials and also the Eberlein polynomials $E_k(i,n,l) = \sum_{j=0}^{k} (-1)^j \binom{i}{j} \binom{n-i}{k-j} \binom{l-n-i}{k-j}$ obey this recursion with $b = 1$

If the function f is defined on the Johnson scheme, then the eigenvalues of $M_z(f)$ for $z = 0, 1$ are linear combinations of the Eberlein polynomials

$$e_i(z,n,q) = \sum_{k \equiv z \bmod 2} E_k(i,n,l), \quad i = 0, \ldots, n$$

Theorem 2: For the function f when defined on the Johnson scheme the matrices $M_z(f)$, $z = 0, 1$, have full rank if for all $i = 1, \cdots, n$ the Krawtchouk polynomials $K_{n-i+1}(n-i+1, l+2i-2, 2)$ are different from 0.

Proof: First observe that the eigenvalues $e_0(z,n,l)$ (and $n \geq 1$) are both positive for $z = 0, 1$ as the sum of positive terms and hence different from 0.

$$\begin{aligned} e_i(0,n,l) &= e_{i-1}(0,n-1,l+2) - e_{i-1}(1,n-1,l+2) \\ &= 2^{i-1} \sum_{k=0}^{n-i+1} (-1)^k E_k(0,n-i+1,l+2i-2) \\ &= (-1)^{n-i+1} 2^{i-1} K_{n-i+1}(n-i+1, l+2i-2, 2) \end{aligned}$$

So the problem here is to determine, when a Krawtchouk polynomial $K_k(k,m,2)$ (the degree and the first variable being the same) can be 0. This is possible for m even and $k = \frac{m}{2}$. We didn't find any other parameter pair (k,m) with this property.

A third family of orthogonal polynomials obeying the above recursion are the b-analogues of the Krawtchouk polynomials

$$\sum_{j=0}^{k} (-1)^j b^{\binom{j}{2}} \binom{i}{j}_b \binom{n-i}{k-j}_b \prod_{t=0}^{k-j-1} (cb^n - b^{i+t})$$

where $\binom{m}{s}_b$ denotes the Gaussian binomial coefficient. The eigenvalues of the association schemes of bilinear forms over $GF(b)$ have as parameters a prime power b and $c = b^r$ for some nonnegative integer r. The eigenvalues of the association schemes of alternating bilinear forms have as parameters $b = p^2$ the square of a prime p and $c = p$ or $c = \frac{1}{p}$ (cf. [1]). By calculation modulo 2 it can be derived

Theorem 3: Let a function f be defined as above on the association scheme of bilinear forms over $GF(b)$ or on the association scheme of alternating bilinear forms. Further let the prime p defining the parameters b and c be odd. Then the matrices $M_z(f)$, $z = 0, 1$, have full rank if $b-1$ is not a power of 2.

References

[1] P. Delsarte, "Properties and applications of the recursion $F(i+1, k+1, n+1) = q^{k+1}F(i,k+1,n) - q^k F(i,k,n)$", *SIAM J. Appl. Math.* 31, 1976, 262-270.

[2] R. M. Karp, "ISIT'98 Plenary Lecture Report: Variations on the theme of 'Twenty Questions' ", *IEEE Information Theory Society Newsletter*, Vol. 49, No. 1, March 1999, 1-5 and 21-22.

[3] J. Körner and A. Orlitsky, "Zero-Error Information Theory", *IEEE Trans. Inform. Theory*, Commemorative Issue, 44, 1998, 2207 - 2229.

[4] E. Kushilevitz and N. Nisan, *Communication complexity*, Cambridge University Press, 1997.

[5] U. Tamm, "Communication complexity of sum - type functions invariant under translation", *Inform. and Computation* 116, 1995, 162 - 173.

[6] U. Tamm, "Communication complexity and orthogonal polynomials", *Proceedings of the Workshop "Codes and Association Schemes"*, AMS-DIMACS Series, submitted.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Design of Efficient Erasure Codes with Differential Evolution

Amin Shokrollahi
Bell Laboratories, Room 2C-381
700 Mountain Ave
Murray Hill, NJ 07974, USA
e-mail:
amin@research.bell-labs.com

Rainer Storn
Infineon Technologies
Balanstr. 73
D-81541 München, Germany
e-mail:
rainer.storn@infineon.com

Abstract — **The design of practical and powerful codes for protection against erasures can be reduced to optimizing solutions of a highly nonlinear constraint satisfaction problem. In this paper we will attack this problem using the Differential Evolution approach and significantly improve results previously obtained using classical optimization procedures.**

I. Introduction

Based on the theoretical results proved in [1], we will in this paper attack a nonlinear constrained satisfaction problem the solutions of which correspond to highly efficient codes. The optimization problem involved will be attacked by Differential Evolution, a robust optimizer which has proved quite effective for similar types of problems.

The codes from [1] are built from sparse bipartite graphs and generalize a classic construction of Gallager [3]. After collecting the information contained in the received bits, the algorithm removes the corresponding variable nodes from the graph together with all edges emanating from them. Then, at each round, it looks for a check-node of degree one, copies its content into its unique neighbor, updates the values, and removes the variable node and all edges emanating from it from the graph. The decoder is successful if the final graph is empty. It was shown in [1] that if the graph is sampled uniformly at random from the ensemble of graphs with degree distributions (λ, ρ) (see below for a definition), then the algorithm successfully recovers from a random δ-fraction of erasures with high probability iff $\delta\lambda(1-\rho(1-x)) < x$ for $x \in (0, \delta)$. If $\lambda(x) = \sum_i \lambda_i x^{i-1}$ and $\rho(x) = \sum_i \rho_i x^{i-1}$, then we say that the graph has degree distribution (λ, ρ) if the fraction of edges connected to a variable (check) node of degree i is λ_i (ρ_i). The task at hand is now to find appropriate polynomials λ and ρ with nonnegative coefficients that give rise to a code of a given rate such that the above inequality is satisfied for a large value of δ.

II. Differential evolution

The code design problem as described above is a nonlinear constraint satisfaction problem with continuous space parameters, a problem class where Differential Evolution (DE) [2] has proven to be very effective. The main properties of DE are (1) Initialization in which, similar to evolutionay strategies, a random first generation of vectors is created which changes over time according to (2) mutation, and (3) recombination, (4) selection of the survivors, and (5) the stopping criterion. What gives DE its name is the differential nature of the mutation step, in which at each round random pairwise differences of two pairs of population vectors are added to population members. The recombination scheme follows usual evolutionary algorithms. The reader is invited to consult [2] for more information on DE.

III. Code design

For designing the code, we started by fixing the rate of the code and randomly producing degree distributions giving rise to codes of that rate. For doing this, note first that the conditions relating the coefficients of $\lambda(x)$ and $\rho(x)$ force the free coefficients of these polynomials to lie in a finite polytope. Our first task is then to choose random elements from this polytope. To achieve this, we implemented a different strategy, known as the "Queen's move":we started with some point inside the polytope constructed deterministically, and repeated the following procedure between 50 and 100 times: we randomly selected a line through the point, and randomly selected a point on that line inside the polytope. This gave us one population member. For the next members, we repeated the whole procedure again, until all the (initial) population members were generated. To reduce the dimensionality of the problem, we did not let the node degrees on the left and the right take on all possible node degrees in a given range. Rather, we experimented with the idea to force to zero those λ_i and ρ_k which have small values and to not treat them as free parameters subject to optimization. Typically, we chose the node degrees in the following way: on the left hand side, we chose the degrees 2, 3, a highest degree (between 20 and 30) and one degree in between. On the right hand side, we chose two consecutive degrees, either 7 and 8, or 8 and 9. By way of an example, we mention of the rate 1/2 sequences that we found with our method: $\lambda(x) = 0.26328x + 0.18020x^2 + 0.27000x^6 + 0.28649x^{29}$, $\rho(x) = 0.63407x^7 + 0.36593x^8$. The highest δ value for this sequence is 0.4955. It can be shown that, given the highest possible value attainable with the average degrees of the graphs induced by these distributions is 0.4985. Hence, this sequence is within less than 1% of the optimum. Other very good sequences will be presented in the talk.

References

[1] M. Luby, M. Mitzenmacher, M.A. Shokrollahi, D. Spielman, and V. Stemann. Practical loss-resilient codes. In *Proceedings of the 29th annual ACM Symposium on Theory of Computing*, pages 150–159, 1997.

[2] K. Price and R. Storn. Differential evolution - a simple and efficient heuristic for global optimization over continuous spaces. *Journal of Global Optimization*, 11:341–359, 1997.

[3] R. G. Gallager. *Low Density Parity-Check Codes.* MIT Press, Cambridge, MA, 1963.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On Multiple Insertion/Deletion Correcting Codes

T.G. Swart
Department Electrical and
Electronic Engineering
Rand Afrikaans University
PO Box 524
Auckland Park, 2006
South Africa
e-mail: tswart@eng.rau.ac.za

H.C. Ferreira
Department Electrical and
Electronic Engineering
Rand Afrikaans University
PO Box 524
Auckland Park, 2006
South Africa
e-mail: hcf@ing1.rau.ac.za

Abstract — **In this paper, new results on insertion and/or deletion correcting codes are presented. Firstly, new properties relating codewords to subwords are investigated. Secondly, a new error correcting scheme based on convolutional coding, is proposed.**

I. Codewords and computer search

An alternative way of representing binary words is used which simplifies the process of determining subwords after insertion/deletion errors. All the binary words are characterized by the length of runs present in the word as well as the starting bit, e.g. $10000100 \rightarrow 1412/1$. In the case of deletion errors, all the subwords can be obtained by decreasing the size of each run present in the word. If the first run's size is 1 and it is deleted, the starting bit will change. If any other run of size 1 is deleted, the two neighbouring runs will merge. For insertion errors, the subwords are obtained by adding bits either to the beginning or the end of the word, increasing the size of the runs or by splitting existing runs.

Assume that binary words of length n are used and that s denotes the number of insertion and/or deletion errors. Since a binary word and its complement have complementary subwords, it is only necessary to compute the subwords of 2^{n-1} words. Complementing the starting bit of the already calculated words/subwords forms the other 2^{n-1} words/subwords. This method is used to construct subword books that contain the subwords of all 2^n binary words after $s = 1$ errors. Using the $s = 1$ subword book and repeating the procedure on all the subwords, a $s = 2$ subword book can be formed. By searching the subword books, codewords can be chosen that do not have a common subword. Cardinalities of codebooks found by computer searching $s = 2$ subword books will be presented and compared to known $s = 2$ correcting codebooks by Helberg [1].

By inspecting the subword books and using generating functions, it is possible to determine the number of subwords that a binary word will produce. The number of subwords after deletions is dependable on the runs in the word. Let x denote the binary codeword and $\tau(x)$ be the number of runs in x. In the case of $s = 1$ deletions, $\tau(x)$ subwords will be formed. Let $\lambda(x, y)$ indicate the size of the y-th run in x. For $s = 2$ deletions, the number of subwords will be given by:

$$\frac{1}{2}(p^2 + q^2 + 2pq - p + q) - r \qquad (1)$$

where p is the number of $\lambda(x, y) = 1$, q the number of $\lambda(x, y) \geq 2$ and r the number of $\lambda(x, y) = 1$, where $2 \leq y \leq \tau(x) - 1$. The number of new words after insertions is dependable on the length of the word. For $s = 1$ insertion there will be $n + 2$ new words. For $s = 2$ insertions it is given by:

$$\frac{1}{2}(n^2 + 5n + 8) \qquad (2)$$

Because the number of new words for insertions is set, this fact can be used to establish an upperbound. According to Levenshtein, a code capable of correcting s deletions will also be able to correct s deletions and/or insertions [2]. Therefore this insertion upperbound provides an upperbound for s-correcting codes in general.

II. New proposed scheme

We further present a new coding scheme in part based on a parallel convolution encoder. Insertion/deletion errors result in a long burst error after the error occurred. This means that any bits received after an insertion/deletion error can not be used in error correcting. For this reason it is proposed that encoding proceed as normal, up to a certain length, but that the encoded data be sent in reverse over the channel. This results in an encoded data stream that is able to detect errors in the coming data, with the assumption that data already received is correct or already corrected by the decoder. Two encoders with rates $R = \frac{1}{3}$ and $R = \frac{1}{4}$ are presented. Both encoders are able to correct insertion, deletion or reversal errors, given that the channel is limited to one type of error.

Whenever an insertion/deletion error occurs and the syndrome indicates an error, a bit is deleted/inserted in a certain place relative to the syndrome error and the syndromes recalculated. Since the inserted/deleted bit will not always be in the correct position, there is a possibility of a short burst of reversal errors. The new syndrome can then be used to correct these errors. In the case of reversal errors, the syndrome can be used as is done for error correction.

References

[1] A. S. J. Helberg & H. C. Ferreira, "Multiple insertion/deletion correcting codes," submitted to IEEE Transactions on Information Theory, 1998.

[2] V. I. Levenshtein, "Binary codes capable of correcting deletions, insertions and reversals," *Sov. Phys - Dokl*, vol. 10, no. 8, pp. 707–710, February 1966.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On Unequal Error Protection Reed-Muller Codes

Dojun Rhee[1]
LSI LOGIC Corporation
e-mail: drhee@lsil.com

Abstract — **It is well known that Reed-Muller (RM) codes are not an linear unequal error protection (LUEP) code because the set of minimum-weight vectors span Reed-Muller codes (punctured or not) [1,2]. In this paper, we showed that most of RM codes are LUEP codes if RM codes are encoded with recursively decomposed trellis oriented generator matrix (TOGM) and maximum-likelihood trellis decoding (MLTD) is used.**

I. Introduction

Uneqaul error protection codes protect some information bits against a great number of errors than other information bits. LUEP codes were first introduced by Masnick and Wolf [3]. Boyarinov and Katsman [4] found conditions for linear codes to be LUEP. Let C be and (n,k,d) linear code. It is shown in [1] that if the minimum-weight vectors of a linear code C does not span it, then C is an LUEP code. It is well known that their set of minimum-weight vectors span RM codes (punctured or not) [2]. Therefore, RM codes are not LUEP codes in algebraic decoding. In the soft-decision maximum likelihood decoding, bit-error-rate of RM code depends on the weight distribution of code. If non-systematic GM is used for encoding the RM code and soft-decision maximum likelohood decoding is used in decoding, different set of information bits has a different bit-error-rate since each other has different weight distribution. Therefore, even though RM code is not an LUEP code in algebraci decoding, RM code is an LUEP code in soft-decision maximum likelihood decoding if systematic GM is not used for encoding.

Especially, in this paper, LUEP RM codes are constructed by using recursively decomposed TOGM for encoding. Simulations show that bit-error-rate of some information bits is almost twice better than that of the other information bits. By using the recursive decomposition, a simple trellis diagram with parallel structure for the **RM** code is devised. In ML trellis decoding, information bits are retrieved directly from the labeling of the trellis.

II. Recursive Decomposition of Reed-Muller Codes and Its Trellis

Let $RM(r,m)$ denote the r-th order binary **RM** code of length 2^m[1,2]. This code has minimum Hamming distance $d = 2^{m-r}$ and the dimension

$$K(r,m) = 1 + \begin{pmatrix} m \\ 1 \end{pmatrix} + \cdots + \begin{pmatrix} m \\ r \end{pmatrix}.$$

Let T be a (2,1,2) binary linear code with following generator matrix $G_T = \begin{pmatrix} 1 & 1 \end{pmatrix}$. And let W be a (2,2,1) binary linear code with following generator matrix $G_W = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Let $[RM(r,m-1)/RM(r-1,m-1)]$ denotes the set of representatives of the cosets of $RM(r-1,m-1)$ in $RM(r,m-1)$ and $G(r,r-1,m-1)$ be the generator matrix for the $[RM(r,m-1)/RM(r-1.m-1)]$ coset code and $E(r,r-1,m-1)$ be the dimension of $[RM(r,m-1)/RM(r-1,m-1)]$. Then the generator matrix for $RM(r,m)$ is as following $G(r,m) = G(r,r-1,m-1) \bigotimes G_T \bigoplus G(r-1,r-2,m-2) \bigotimes G_T \bigotimes G_W \bigoplus G(r-2,m-2) \bigotimes G_W \bigotimes G_W$ where $\bigotimes$ and $\bigoplus$ denotes the direct product and direct addition. Therefore, $K(r,m) = E(r,r-1,m-1) + 2 \times E(r,r-2,m-2) + 4 \times K(r-2,m-2)$. Let $K = K(r,m) = K_1 + K_2 + K_3 = E(r,r-1,m-1) + 2 \times E(r,r-2,m-2) + 4 \times K(r-2,m-2)$. Let W_1, W_2, and W_3 be weight distribution of $G(r,r-1,m-1) \bigotimes G_T \bigoplus$, $G(r-1,r-2,m-2) \bigotimes G_T \bigotimes G_W \bigoplus$, and $G(r-2,m-2) \bigotimes G_W \bigotimes G_W$, respectively. Then bit-error-rate of K_1, K_2, and K_3 information bits depend on weight distribution of W_1, W_2, and W_3 respectively.

III. Examples and Simulation Results

Consider the $RM(2,5)$ code which is a (32, 16) **RM** code of Hamming distance 8. Let $\mathbf{b} = (b_1, b_2, \cdots, b_{16})$ be the 16 information bits and $\mathbf{v} = (v_1, v_2, \cdots, v_{32})$ be the the corresponding codeword in $RM(2,5)$. Then

$$\begin{aligned} \mathbf{v} &= \mathbf{b}\, G(2,5) \\ &= (b_1,b_2,b_3,b_4,b_5,b_6)\, G(2,1,4) \bigotimes G_T \bigoplus \\ &\quad (b_7,b_8,b_9,b_{12},b_{13},b_{14})\, G(2,1,3) \bigotimes G_T \bigotimes G_W \bigoplus \\ &\quad (b_{10},b_{11},b_{15},b_{16})\, G(0.3) \bigotimes G_W \bigotimes G_W \end{aligned}$$

where $\mathbf{0_N}$ means N consecutive zeros. The first 6 bits, b_1,b_2,b_3,b_4,b_5,b_6, select one of the 64-subtrellises. For the left (16,5,8) code, (b_7,b_8,b_9) selects one of the 8-subtrellises which are of length 16. Then b_{10} selects a codeword in the left (8,1,8) code and b_{11} selects a codeword in the right (8,1,8) code. For the right (16,5,8) code, (b_{12},b_{13},b_{14}) selects one of 8 subtrellises which are of length 16. Then b_{15} selects a codeword in the left (8,1,8) code and b_{16} selects a codeword in the right (8,1,8) code. Simulation results shows that group of $b_{10},b_{11},b_{15},b_{16}$ achieves about 0.14 dB coding gain over groups of b_1,b_2,b_3,b_4,b_5,b_6 and $b_7,b_8,b_9,b_{12},b_{13},b_{14}$.

References

[1] F. J. Macwilliams and N. J. A. Sloane, *The Theory of Error-Correcting codes*, North-Holland, Netherland, 1988.

[2] Robert H. Morelos-Zaragoza and Shu Lin, "On Primitive BCH Codes with Unequal Error Protection Capabilities," *IEEE Trans. on Inform. Theory*, Vol. 41, No. 3, pp. 788-790, May 1995.

[3] Burt Masnick and Jack Wolf, "On Linear Unequal Error Protection Codes," *IEEE Trans. on Inform. Theory*, Vol. 3, No. 4, pp. 600-607, May 1967.

[4] I. M. Boyarinov and G. L. Katsman, "Linear Unequal Error Protection Codes," *IEEE Trans. on Inform. Theory*, Vol. 3, No. 27, pp. 168-175, May 1981.

[1]This work was supported by LSI LOGIC Corporation.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Unidirectional Byte Error Correcting Codes for q-Ary Data

Kiattichai Saowapa, Haruhiko Kaneko, and Eiji Fujiwara
Graduate School of Information Science and Engineering, Tokyo Institute of Technology
2-12-1 O-okayama, Meguro-ku, Tokyo, 152-8552, Japan
e-mail: {kung,hkaneko,fujiwara}@cs.titech.ac.jp

Abstract — **This paper presents a class of codes protecting data on two-dimensional symbology against errors caused by stain, tear, scratch or blurring.**

I. Introduction

In two-dimensional symbology[1], nonbinary character such as alphabet, number, etc., is two-dimensionally expressed as pattern of black and white pixels, denoted as binary '1' or '0', in the record media. These pixels are sometimes disturbed by stain, tear, scratch or blurring, and these make black pixels changed into white ones, or vice versa. These disturbances result in unidirectional errors[2][3] in a binary space.

Each nonbinary character is usually expressed in a block of binary digits with fixed size, called byte. In some digital systems, 2^b b-bit byte patterns are not fully assigned to q-ary characters, that is, the total number of q-ary characters used in the system, q, is less than 2^b. Therefore, the remaining $(2^b - q)$ b-bit byte patterns, are not used in the systems, which gives possibility to design efficient codes.

This paper proposes a class of codes for q-ary data which can correct single unidirectional b-bit byte errors in a binary space, called q-ary single unidirectional b-bit byte error correcting (1-UbEC) codes, with $q < 2^b$.

II. Code Construction

Let a, c be elements in Galois field $GF(p_1)$, i.e., $a, c \in GF(p_1)$, and b, d be elements in Galois field $GF(p_2)$, i.e., $b, c \in GF(p_2)$. The set $R(p_1, p_2)$ with $p_1 \times p_2$ elements defined by the following conditions is a ring:

(1) $<a,b> \in R(p_1,p_2)$,

(2) $<a,b> \oplus <c,d> \equiv <a +_1 c, b +_2 d>$,

(3) $<a,b> \otimes <c,d> \equiv <a \times_1 c, b \times_2 d>$,

where $+_i$ and $\times_i$ are additive and multiplicative operations between two elements in $GF(p_i)$, i=1,2, respectively.

Theorem 1 *Let $\mathbf{H}_i$ be a parity check matrix of an $(n_i, n_i - r)$ systematic single error correcting code over $GF(p_i)$, where i=1,2, as shown below:*

$$\mathbf{H}_1 = \left[\mathbf{h}'_1 \ \mathbf{h}'_2 \ \ldots \ \mathbf{h}'_{n_1} \right], \mathbf{H}_2 = \left[\mathbf{h}''_1 \ \mathbf{h}''_2 \ \ldots \ \mathbf{h}''_{n_2} \right],$$

where $\mathbf{h}'_i = (a_0 \ \ldots \ a_{r-1})^T$, $a_l \in GF(p_1)$, $0 \le l < r$, and $\mathbf{h}''_j = (b_0 \ \ldots \ b_{r-1})^T$, $b_l \in GF(p_2)$, $0 \le l < r$. The linear code defined by the following parity check matrix $\mathbf{H}_0$ over $R(p_1, p_2)$ is a code capable of correcting single errors with type $<\alpha, \beta>$.

$$\mathbf{H}_0 = \left[<\mathbf{h}'_1, \mathbf{h}''_1> \ldots <\mathbf{h}'_1, \mathbf{h}''_{n_2}> \mid \ldots \mid <\mathbf{h}'_{n_1}, \mathbf{h}''_1> \ldots <\mathbf{h}'_{n_1}, \mathbf{h}''_{n_2}> \right]$$

Here, $<\mathbf{h}'_i, \mathbf{h}''_j>$ $(0 \le i < n_1, \ 0 \le j < n_2)$ represents vector $(<a_0, b_0> \ \ldots \ <a_{r-1}, b_{r-1}>)^T$. □

The code construction requires function f which maps from set V containing binary vectors with length b to $R(p_1, p_2)$, i.e., $f : V \to R(p_1, p_2)$, satisfying the following three conditions:

(i) if $f(\mathbf{i}) = f(\mathbf{j})$, then $\mathbf{i} = \mathbf{j}$,

(ii) if $(f(\mathbf{i}) = <a,b>) \wedge (f(\mathbf{j}) = <a,d>) \wedge (b \neq d)$, then weight of $\mathbf{i}$ is equal to that of $\mathbf{j}$,

(iii) if $(f(\mathbf{i}) = <a,b>) \wedge (f(\mathbf{j}) = <c,b>) \wedge (a \neq c)$, then $\mathbf{i}$ and $\mathbf{j}$ are unordered,

where $\mathbf{i}$ and $\mathbf{j}$ are binary vectors each having length b.

Encoding Procedure: The following notations are used in the algorithm to construct q-ary 1-UbEC codes.

d_i: q-Ary character, $1 \le i \le K$.

$<a_i, b_i>$: Information element in $R(p_1, p_2)$, $1 \le i \le K$.

$<\tilde{a}_j, \tilde{b}_j>$: Check element in $R(p_1, p_2)$, $1 \le j \le R$.

$\mathbf{d}_i$: Binary information vector with length b, $1 \le i \le K$.

$\mathbf{p}_j$: Binary check vector with length b, $1 \le j \le R$.

f^{-1}: Inverse function of f.

g: One-to-one function from set of q-ary characters to set $\{f(\mathbf{x}) | \forall \mathbf{x} \in V\}$.

h: One-to-one function from $R(p_1, p_2)$ to set of $p_1 \times p_2$ binary vectors each having length b.

Let $(d_1, d_2, \ldots, d_K)$ be an input q-ary information vector. Under the above preparation, encoding is shown as follows:

1) Determine the function $f : V \to R(p_1, p_2)$, where V has q vectors, $q \le 2^b$.

2) Obtain information element $<a_i, b_i>$ by $<a_i, b_i> = g(d_i)$, where $1 \le i \le K$.

3) Obtain check element $< \tilde{a}_j, \tilde{b}_j >$, $1 \le j \le R$, which satisfies the following equation:
$\mathbf{0} = (<a_1, b_1>, \ldots, <b_K, b_K>, <\tilde{a}_1, \tilde{b}_1>, \ldots, <\tilde{a}_R, \tilde{b}_R>) \cdot \mathbf{H}^T$,
where $\mathbf{H}$ is an $R \times (K + R)$ shortened matrix of $\mathbf{H}_0$, and $\mathbf{0}$ is a $1 \times (K + R)$ zero matrix.

4) Obtain $\mathbf{d}_i = f^{-1}(<a_i, b_i>)$ for $1 \le i \le K$ and $\mathbf{p}_j = h($ $<\tilde{a}_j, \tilde{b}_j>)$ for $1 \le j \le R$. Finally, $(\mathbf{d}_1, \mathbf{d}_2, \ldots, \mathbf{d}_K, \mathbf{p}_1, \ldots, \mathbf{p}_R)$ shows the encoded output.

III. Evaluation

Fig 1. shows that the codes are more efficient than the conventional codes which can correct single unidirectional byte errors with $q = 2^b$, i.e., 2^b-ary 1-UbEC codes[3] and the single symmetric byte error correcting codes [2].

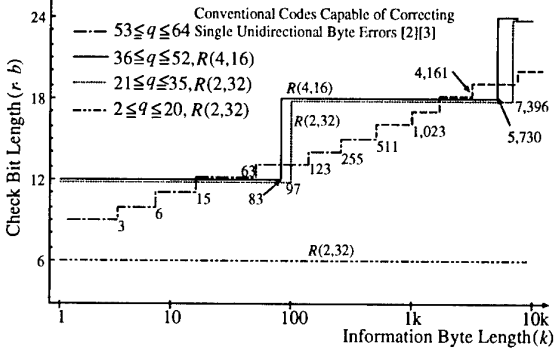


Fig.1: Relation between the information byte-length and the check bit-length for q-ary 1-UbEC codes, where $b = 6$.

References

[1] T. Pavlidis, J. Swartz, Y. P. Wang, "Information encoding with two-dimensional bar codes," *Computer*, Vol. 25, No. 6, pp. 18-28, Jun. 1992.

[2] T. R. N. Rao and E. Fujiwara, *Error Control Coding for Computer Systems*, Englewood Cliffs, Nj: Prentice-Hall, 1989.

[3] B. Bose and S. Al-Bassam, "Byte Unidirectional Error Correcting and Detecting Codes," *IEEE Trans. Comp.*, Vol. 41, No. 12, pp. 1601-1606, Dec. 1992.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Codes on Graphs: Normal Realizations

G. David Forney, Jr.
M.I.T.
e-mail: forney@lids.mit.edu

Abstract — **Wiberg *et al.* [6] proposed graphical code realizations using three kinds of elements: symbol variables, state variables and local constraints. We focus on normal realizations, namely Wiberg-type realizations in which all symbol variables have degree 1 and state variables have degree 2.**

A natural graphical model of a normal realization represents states by leaf edges, states by ordinary edges, and local constraints by vertices. Any such graph may be decoded by message-passing (the sum-product algorithm).

We show that any Wiberg-type realization may be put into normal form without essential change in its graph or its decoding complexity.

Group or linear codes are realized by group or linear realizations. We show that an appropriately defined dual of a group or linear normal realization realizes the dual group or linear code. The symbol variables, state variables and graph topology of the dual realization are unchanged, while local constraints are replaced by their duals.

I. Summary

Tanner [5] founded the subject of "codes on graphs," building on Gallager's work on low-density parity-check (LDPC) codes [2]. A "Tanner graph" is a bipartite graph in which there are two types of vertices, representing symbol variables and local constraints (*e.g.*, parity checks). Tanner also developed the algorithm now generically known as the "message-passing" or "sum-product" algorithm for decoding codes on graphs, generalizing Gallager's APP (*a posteriori* probability) decoding algorithm, and proved that this algorithm performs exact APP decoding on arbitrary cycle-free graphs.

Wiberg *et al.* [6] made an important advance by introducing a third type of vertex, representing state variables. They thus made connections with trellis representations of codes, and with turbo codes and turbo decoding algorithms. Since this work, "codes on graphs" have become the common intellectual foundation for the study both of moderate-complexity codes such as traditional block and convolutional codes, and of capacity-approaching codes such as turbo codes and LDPC codes [1, 3]. The more powerful codes are based on graphs with cycles; their graph-based decoding algorithms have been shown empirically to work very well, even though few theorems are known for graphs with cycles.

In this paper, we consider Wiberg-type realizations in which symbol variables and state variables are restricted to degrees 1 and 2, respectively, called normal realizations. We show that such a restriction involves no loss of generality nor increase in graphical or decoding complexity. With this restriction, we are able to prove a powerful and general duality theorem which applies to group or linear graphical models of arbitrary topology— in particular, to graphs with cycles.

A Wiberg-type realization [6] is based on a set of symbol variables $\{A_k, k \in I_{\mathcal{A}}\}$, a set of state variables $\{S_j, j \in I_{\mathcal{S}}\}$, and a set of local constraints $\{C_i, i \in I_{\mathcal{C}}\}$, constraining some subset of the variables. The realization generates a code C consisting of all symbol configurations $\mathbf{a}$ that occur as part of some global symbol/state configuration $(\mathbf{a}, \mathbf{s})$ that satisfies all local constraints. In the linear or group case, each variable is a vector space or group, the local constraints are linear or group codes, and the code C is then a linear or group code.

The *degree* of a variable is the number of local constraints in which it is involved. A Wiberg-type realization is *normal* if the degree of each symbol variable is 1 and of each state variable is 2. For example, a conventional state realization (trellis) has local constraints corresponding to trellis sections that involve triples $(s_k, a_k, s_{k+1}), k \in \mathbb{Z}$, and thus is normal.

A normal realization is naturally represented by a *normal graph* consisting of degree-1 *leaf edges* representing symbol variables A_k, degree-2 *ordinary edges* representing state variables S_j, and *vertices* representing local constraints C_i. An edge is connected to a vertex if the corresponding variable is involved in the corresponding local constraint.

It is easy to show that any Wiberg-type realization may be converted to a normal realization by replicating variables. The normal graph of the resulting realization looks essentially the same as the Wiberg-type graph of the original realization, and may be decoded with the same complexity.

The *dual realization* of a group or linear normal realization is the realization in which each variable is replaced by its character group (the same variable, if its alphabet is finite), each local code is replaced by its dual code, and a sign inverter is inserted in each ordinary edge. We prove that a dual realization realizes the dual group or linear code, regardless of the topology of the associated normal graph. This result greatly generalizes Mittelholzer's result [4] for dual trellises, and shows that the dual of any code may be realized by use of the same graph and same state spaces as the primal code.

References

[1] S. M. Aji and R. J. McEliece, "The generalized distributive law," *IEEE Trans. Inform. Theory*, vol. 46, pp. 325–344, Mar. 2000.

[2] R. G. Gallager, "Low-density parity-check codes," *IRE Trans. Inform. Theory*, vol. IT-8, pp. 21–28, Jan. 1962.

[3] F. R. Kschischang, B. J. Frey and H.-A. Loeliger, "Factor graphs and the sum-product algorithm," submitted to *IEEE Trans. Inform. Theory*, July 1998.

[4] T. Mittelholzer, "Convolutional codes over groups: A pragmatic approach," *Proc. 33d Allerton Conf. Commun. Control Comput.* (Allerton, IL), pp. 380–381, Sept. 1995.

[5] R. M. Tanner, "A recursive approach to low-complexity codes," *IEEE Trans. Inform. Theory*, vol. IT-27, pp. 533–547, Sept. 1981.

[6] N. Wiberg, H.-A. Loeliger and R. Kötter, "Codes and iterative decoding on general graphs," *Euro. Trans. Telecomm.*, vol. 6, pp. 513–525, Sept./Oct. 1995.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Dealing with short cycles in graphical codes

Arnaud Guyader, Eric Fabre
Irisa, Campus de Beaulieu, 35042
Rennes cedex, France
e-mail: name@irisa.fr

Abstract — **The graphical representation of codes has opened the way to soft decoding by belief propagation (BP), which extends the usual soft Viterbi decoding. This simple algorithm is most often used for constructing and evaluating graphical codes. We show that belief propagation on graphs is not always appropriate and that the algorithmic resources for graphical models are far more extended than BP. In particular, we propose new approximate decoders based on the "conditioning technique" to solve the short cycles problem of graphical codes.**

I. Introduction

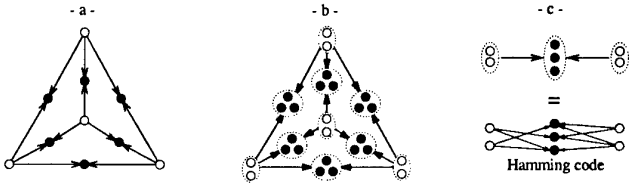
On graphical representations, turbo-decoding is equivalent to the belief propagation (BP) algorithm [1]. BP on graphs converges to the exact posterior marginals as long as the graph has a *tree structure* [3]. Surprisingly, the algorithm still provides a good approximation of posterior marginals even under the presence of cycles, as turbo-codes have revealed. This holds in particular when the graph has "long" cycles since, around a given variable, it can be well-approximated by a tree: measurements too far away from a given node have little influence on this node.

The graphical construction of codes and decoders looks very promising, but it may be somewhat misleading however, because *the construction relies on a single algorithm*, which induces a confusion between the properties of the code itself, and those of the decoding algorithm. A "good" graphical code can be understood as a structure providing the highest degree of protection to each bit. This suggests high correlations between variables of the graph, so that many measurements bring information on each bit. This, in turn, suggests "compact graphs" containing many short cycles. But such graphs are precisely those for which BP is not expected to work well. This may explain why good graphical codes found up to now usually rely on large graphs.

However, bayesian estimation for graphical models starts with BP, but also provides a wide range of techniques to deal with cyclic graphs. In particular, *exact computations* can be performed despite the presence of cycles. The price to pay is an increased complexity of the algorithm. The most interesting point is that exact and approximate methods can be mixed, which allows us to tune the trade-off between complexity and precision.

II. Experimental framework: two-scale codes

There is an easy way of augmenting the compacity of a graphical code at low price, without disturbing too much its apparent structure (cf figure): simple parity bits can be replaced by an ordinary algebraic code, whence the name *two-scale codes* (cf Tanner in [2]). Re-expanding the coarse scale structure to evidence each bit reveals that many cycles have been introduced in the fine scale. The figure gives an example



of such a code, seen at two different scales. One can imagine two algorithms for decoding this $(26, 8)$ code: either BP on the fine scale graph (-b-), or BP on the coarse scale graph (-a-), i.e. the tetrahedron. Simulation results show that both algorithms converge rapidly, but the second one is much better. This phenomenon reveals that correlation between variables of the graph plays a central role in the performance of an estimation algorithm, and in particular that short cycles perturbs BP very much.

III. Dealing with short cycles: beyond belief propagation

Conditioning. Markov field theory explains a simple and elegant result: conditionally to a given variable X_a in the field, the remaining variables still obey a Markov field, the graph of which is obtained simply by removing vertex X_a from the original graph. Let us consider a graphical model composed of one cycle only. Removing one vertex in the graph opens the cycle, which yields a simple Markov chain structure, that is amenable to *exact estimation* through BP. This is the basis of the conditioning method, the originality of which is to propose a way of properly handling the variable that has been removed.

Approximate conditioning. One interesting aspect of the conditioning method is to offer an alternate solution to the agregation procedure, which gets back to a tree (the "junction tree") by grouping variables. However, the overall complexities of both methods are similar in many cases. But conditioning has another interesting point: it leads to new approximate decoding algorithms that mix the conditioning method with approximate BP on graphs with cycles. The idea is to break only part of the cycles, and in particular short cycles, in order to obtain a simplified graph on which belief propagation will perform well. This simple strategy gives excellent results, at low cost, on graphical codes that resist the BP algorithms.

References

[1] R.J. McEliece, D.J.C. MacKay, J.-F. Cheng, "Turbo decoding as an instance of Pearl's belief propagation algorithm," IEEE J. on Sel. Areas in Com., vol. 16, no. 2, feb. 98.

[2] R. M. Tanner, "A recursive approach to low complexity codes," *IEEE Transactions on Information Theory*, sep. 81.

[3] J. Pearl, "Fusion, propagation and structuring in belief networks," Artificial Intelligence 29, pp. 241-288, 86.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On Codes that Can Identify Vertices in Graphs

G. Cohen
ENST, URA 820
Département INFRES
46 rue Barrault
75634 Paris cedex 13, France
cohen@infres.enst.fr

I. Honkala
University of Turku
Department of Mathematics
20014 Turku, Finland
honkala@utu.fi

A. Lobstein
ENST, URA 820
Département INFRES
46 rue Barrault
75634 Paris cedex 13, France
lobstein@infres.enst.fr

G. Zémor
ENST, URA 820
Département INFRES
46 rue Barrault
75634 Paris cedex 13, France
zemor@infres.enst.fr

Abstract — **In a graph $G = (V, E)$, a subset of vertices C (= code) is called t-identifying if for all $v \in V$ the sets $B_t(v) \cap C$ consisting of all elements of C within distance t from v are nonempty and different. We study some properties of these codes.**

I. Introduction

Let $G = (V, E)$ be an undirected connected graph (finite or infinite). We denote by

$$B_t(v) = \{x \in V : d(x, v) \leq t\}$$

the ball of radius t centred at the vertex $v \in V$, where $d(x, v)$ equals the number of edges in a shortest path between v and x. If $d(x, v) \leq t$, then we say that x covers v (and vice versa).

A code C is a nonempty subset of V. Its elements are called codewords. The code C is a t-identifying code if the sets $B_t(v) \cap C$, $v \in V$, are all nonempty and different.

This definition is motivated by fault diagnosis in multiprocessor systems: a multiprocessor system can be modeled as an undirected graph where the vertices are processors and the edges the links in the system. For testing the system and locating one faulty processor, a set of processors is selected and each selected processor is assigned the task of testing the vertices within distance t, for malfunction. Whenever it detects a fault of any kind, an error message is issued, specifying only its origin. The minimum number of selected processors needed is the minimum size of a t-identifying code.

II. A New Lower Bound for Infinite Grids

We focus on the following four infinite 2-dimensional grids:
- the square grid, G_1;
- the square grid with one diagonal (or triangular grid), G_2;
- the square grid with two diagonals, G_3;
- the hexagonal grid, G_4.

A simple lower bound (see [12]) states that the smallest possible density $d_t^{(i)}$ of a t-identifying code in G_i $(i = 1, 2, 3, 4)$ satisfies

$$d_t^{(i)} \geq \frac{2}{B_t^{(i)} + 1},$$

where $B_t^{(i)}$ denotes the size of a ball of radius t in G_i (size independent of the centre of the ball). Since for $i = 1, 2, 3, 4$, these sizes are given by polynomials of the second degree in t, we have a lower bound on the density in $\Omega(t^{-2})$. For the four grids, we improve this to $\Omega(t^{-1})$.

III. Nonexistence of Perfect Codes for $t > 1$

A perfect t-identifying code is such that all codewords are covered only by themselves, and all non codewords are covered by exactly two codewords. A perfect 1-identifying code in G_2 is given in [12].

We prove that in any graph, no nontrivial perfect t-identifying code exists unless $t = 1$.

IV. Complexity

We prove that the following problem is NP-complete:
INSTANCE: a graph $G = (V, E)$, an integer k;
QUESTION: is there a 1-identifying code $C \subset V$ of size at most k?

References

[1] U. Blass, I. Honkala, S. Litsyn, "Bounds on identifying codes," *Discrete Math.*, to appear.

[2] U. Blass, I. Honkala, S. Litsyn, "On binary codes for identification," *J. Combin. Des.*, to appear.

[3] G. Cohen, S. Gravier, I. Honkala, A. Lobstein, M. Mollard, C. Payan, G. Zémor, "Improved identifying codes for the grid," *Electron. J. Combin.*, Comments to 6(1), R19, 1999.

[4] G. Cohen, I. Honkala, A. Lobstein, G. Zémor, "New bounds for codes identifying vertices in graphs," *Electron. J. Combin.*, vol. 6(1), R19, 1999.

[5] G. Cohen, I. Honkala, A. Lobstein, G. Zémor, "On codes identifying vertices in the two-dimensional square lattice with diagonals," submitted.

[6] G. Cohen, I. Honkala, A. Lobstein, G. Zémor, "Bounds for codes identifying vertices in the hexagonal grid," *SIAM J. Discrete Math.*, submitted.

[7] G. Cohen, I. Honkala, A. Lobstein, G. Zémor, "On identifying codes," *DIMACS*, submitted.

[8] G. Exoo, "Computational results on identifying t-codes," preprint.

[9] T. W. Haynes, S. T. Hedetniemi, P. J. Slater, *Fundamentals of Domination in Graphs*, New York: Marcel Dekker, 1998.

[10] I. Honkala, "On the identifying radius of codes." In: Proceedings of the 7th Nordic Combinatorial Conference (eds. T. Harju and I. Honkala), Turku, 1999.

[11] I. Honkala, T. Laihonen, S. Ranto, "On codes identifying sets of vertices in Hamming spaces," *Designs, Codes and Cryptography*, submitted.

[12] M. G. Karpovsky, K. Chakrabarty, L. B. Levitin, "On a new class of codes for identifying vertices in graphs," *IEEE Trans. Inform. Theory*, vol. 44, pp. 599–611, 1998.

[13] M. G. Karpovsky, K. Chakrabarty, L. B. Levitin, D. R. Avresky, "On the covering of vertices for fault diagnosis in hypercubes," *Inform. Process. Lett.*, vol. 69, pp. 99–103, 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Linear-Time Encodable and Decodable Irregular Graph Codes

Saejoon Kim and Stephen B. Wicker[1]
School of Electrical Engineering, Cornell University, Ithaca, NY 14583

Abstract — **Randomized constructions are presented for a family of linear-time encodable and decodable error-correcting codes using irregular expander graphs. These codes can be encoded in constant time and decoded in at most logarithmic time if a linear number of processors are used.**

I. Introduction

We construct a family of linear-time encodable and decodable error-correcting codes. These codes can also be encoded by circuits of linear-size and constant depth and decoded by circuits of linear-size and at most logarithmic depth. The size of a circuit is defined as the number of vertices, while the depth of a circuit is defined as the maximum length of a directed path in the circuit. The use of irregular expanders is motivated by a recent indication that irregular graphs give better decoding performance than regular graphs [2].

II. Error Reducing Codes

We refer to message nodes as left nodes and check node as right nodes. We will further use x and c to represent left and right nodes, respectively.

Definition 1 *A code $\mathcal{R}$ of rn message bits and $(1-r)n$ check bits is an error reducing code of rate r, error reduction ϵ, and reducible distance δ if there exists an algorithm that, given an input word that differs from a codeword $w \in \mathcal{R}$ in at most $\mu \leq \delta n$ message bits and $\nu \leq \delta n$ check bits, outputs a word that differs from w in at most $\epsilon\nu$ messages bits.*

Definition 2 *A bipartite graph is an (α, β) expander if any subset S consisting of at most a fraction α of left nodes has at least $\beta|\delta(S)|$ right node neighbors, where $\delta(S)$ is the set of edges attached to nodes in S.*

We will sometimes refer to an (α, β) expander of rn left nodes and $(1-r)n$ right nodes as an $(rn, (1-r)n, \alpha, \beta)$ expander.

Theorem 3 *If B is an irregular $(\alpha, \frac{3}{4} + \frac{2}{d_{x,min}})$ expander where $d_{x,min}$ is the minimum degree on the left nodes of B, then $\mathcal{R}(B)$ is an error reducing code of error reduction $\frac{1}{2}$ and reducible distance $\frac{\alpha}{2d_{x,max}}$, where $d_{x,max}$ is the maximum degree on the left nodes of B.*

Theorem 4 *If B is an irregular $(\alpha, \frac{9}{10} + \frac{3}{d_{x,min}})$ expander and $d_{x,min} \geq \frac{8}{9} d_{x,max}$ where $d_{x,min}$ and $d_{x,max}$ are the minimum and maximum degrees on the left nodes of B, then $\mathcal{R}(B)$ is an error reducing code of error reduction $\frac{1}{2}$ and reducible distance $\frac{\alpha}{2}$.*

[1]This work was supported by NSF Grant NCR-9725251.

III. Encoding and Decoding

The cascading method that we use in our construction was originally developed by Luby *et al.* for the construction of erasure codes [1]. Let each graph in the set $\{B_i\}$ of irregular expander graphs have $\alpha^i k$ left nodes and $\alpha^{i+1}k$ right nodes. We associate each graph with an error reducing code $\mathcal{R}(B_i)$ that has $\alpha^i k$ message bits and $\alpha^{i+1}k$ check bits, $0 \leq i \leq m$. We also use an error correcting code C that has $\alpha^{m+1}k$ message bits and $\frac{\alpha^{m+2}k}{1-\alpha}$ check bits. To decode $\mathcal{C}(B_0, \cdots, B_m, C)$, we simply decode the individual codes $\mathcal{R}(B_0), \cdots, \mathcal{R}(B_m), C$ in reverse order. By choosing a code C that can be encoded and decoded in quadratic time and choosing m such that $\alpha^{m+1}k \approx \sqrt{k}$, we insure that the code $\mathcal{C}(B_0, \cdots, B_m, C)$ can be encoded and decoded in linear time.

Theorem 5 *Let B_i be an irregular $(\alpha^i k, \alpha^{i+1}k, \alpha, \frac{3}{4} + \frac{2}{d_{x,min}})$ expander where $d_{x,min}$ is the minimum degree of the left nodes of B_i, $0 \leq i \leq m$. Let C be an error correcting code of $\alpha^{m+1}k$ message bits and $\frac{\alpha^{m+2}k}{1-\alpha}$ check bits, $\alpha^{m+1}k \approx \sqrt{k}$, that can correct a random $\frac{\alpha}{2d_{x,max}}$ fraction of errors, where $d_{x,max}$ is the maximum degree of the left nodes of a B_i. Then $\mathcal{C}(B_0, \cdots, B_m, C)$ is a rate $1-\alpha$ error-correcting code that can be encoded in linear time and can correct a random $\frac{\alpha}{2d_{x,max}}$ fraction of errors in linear time.*

Theorem 6 *Let B_i be an irregular $(\alpha^i k, \alpha^{i+1}k, \alpha, \frac{9}{10} + \frac{3}{d_{x,min}})$ expander, $d_{x,min} \geq \frac{8}{9} d_{x,max}$, where $d_{x,min}$ and $d_{x,max}$ are the minimum and maximum degrees of the left nodes of B_i, $0 \leq i \leq m$. Let C be an error correcting code of $\alpha^{m+1}k$ message bits and $\frac{\alpha^{m+2}k}{1-\alpha}$ check bits, $\alpha^{m+1}k \approx \sqrt{k}$, that can correct a random $\frac{\alpha}{2}$ fraction of errors. Then $\mathcal{C}(B_0, \cdots, B_m, C)$ is a rate $1-\alpha$ error-correcting code that can be encoded by a linear-size circuit of constant depth and can correct a random $\frac{\alpha}{2}$ fraction of errors in a linear-size circuit of at most logarithmic depth.*

References

[1] M.G. Luby, M. Mitzenmacher, M.A. Shokrollahi, D.A. Spielman and V. Stemann, "Practical Loss-Resilient Codes," in *Proc. 29th Symp. on Theory of Computing*, 1997, pp. 150-159.

[2] M.G. Luby, M. Mitzenmacher, M.A. Shokrollahi and D.A. Spielman, "Analysis of Low Density Codes and Improved Designs Using Irregular Graphs," manuscript.

[3] D.A. Spielman, "Linear-Time Encodable and Decodable Error-Correcting Codes." *IEEE Trans. Inform. Theory*, vol. 42, no. 6, pp. 1723-1731, Nov. 1996.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

The Estimate for the Cost of a Search Tree Constructed on an Arbitrary Set of Binary Words

Alexey Fedotov
Department of Information Technologies
Institute of Computational Technologies
Ac. Lavrentjev Ave., 6
630090 Novosibirsk, Russia
e-mail: lesha@adm.ict.nsc.ru

Boris Ryabko[1]
Department of Appl. math and Cybernetics
Sibirean State University of Computer Science
Kirov str., 86
630102 Novosibirsk, Russia
e-mail: ryabko@neic.nsk.su

Abstract — **Simple algorithm constructing search trees for the given set of binary words is presented. It is shown that the average cost of result of this algorithm, and, hence, the average cost of the optimum search tree is near to their natural lower bound.**

I. Introduction

The problem of construction of a binary search tree for any set of binary words has wide applications in computer science, biology, mineralogy, etc. Construction of a tree of minimum cost has attracted attention of many authors [1], [2], [3]. It is known to be an NP-hard problem [4], therefore the problem arises to find simple algorithms for constructing nearly optimum trees. We show in this paper that there is a simple algorithm to construct search trees which are sufficiently close to the optimum tree on average. By means of this algorithm we prove that for the optimum tree the average number of bits to be checked is near to its natural lower bound, i. e., the binary logarithm of the number of given words: their difference is less than 1.04 bit.

II. Statement of the Problem and the Main Result

Let a set of m binary words of length n, ($m \geq 0$, $n \geq 1$) be given. Let us define the cost of the search tree L by the equality $C(L) = \frac{1}{m}\sum_{i=1}^{m} L_i$, where L_i is the number of bits required for identification of the i-th word.

We denote by $\mathcal{S}_{n,m}$ the set of the initial data, i. e. the collection of all sets of m binary words of length n ($n \geq \log_2 m$).

Now let us assume that an algorithm F builds a tree $F(S)$ from the set $S \in \mathcal{S}_{n,m}$. As we will further consider randomized algorithms, it will be convenient to denote by $\bar{C}(F(S))$ the expectation of the cost of the tree $C(F(S))$ related to the measure given by the considered algorithm. Let us define now the average cost $t_{n,m}(F)$ of the algorithm F as follows:

$$t_{n,m}(F) = \frac{1}{\operatorname{Card}\mathcal{S}_{n,m}} \sum_{S \in \mathcal{S}_{n,m}} \bar{C}(F(S)),$$

where $\operatorname{Card}\mathcal{S}_{n,m}$ means the cardinality of the set $\mathcal{S}_{n,m}$.

Now we consider, perhaps, the simplest randomized algorithm of construction of a search tree, which will be denoted by R. Its work can be described as follows.

Description of the algorithm R This algorithm makes a binary search tree from an arbitrary set of m binary words of length n. If the given set contains only one word then the algorithm returns the simplest tree consisting of one leaf and stops.

Otherwise, the randomly chosen position is brought into correspondence with the root of the tree. For each of the parts, into which this check divides the entire set of words, the search tree is constructed by the same method.

The main result of this paper is the following theorem:

Theorem 1 *For the average cost of the algorithm R the following inequality holds:*

$$t_{n,m}(R) \leq \log_2 m + \frac{29}{28} - \frac{\log_2(2m)}{m}. \qquad (1)$$

From this result the following corollary is readily deduced:

Corollary 1 *Let F_{opt} be the algorithm which builds an optimum tree for each data set. Then*

$$t_{n,m}(F_{opt}) \leq \log_2 m + \frac{29}{28} - \frac{\log_2(2m)}{m}.$$

The following corollary contains the estimate for the cost of the search tree constructed by R for almost-all data sets, instead of the average estimate. It is an obvious consequence from the Markov-Chebyshev inequality.

Corollary 2 *Let us assign equal probability to every set S from the set of initial data $\mathcal{S}_{n,m}$ ($m \geq 2$, $n \geq \log_2 m$). Then for every $\epsilon > 0$ the inequality holds:*

$$P\{S : \bar{C}(R(S)) < (1+\epsilon)\log_2 m\} \geq 1 - \frac{29/28}{\epsilon \log_2 m}.$$

The same estimate evidently holds for the cost of the optimum search tree.

Acknowledgments

The authors express their gratitude to M. A. Alekseyev for useful discussions.

References

[1] D. Knuth, *The Art of Computer Programming.* Adisson-Wesley, vol. 3, 1973.

[2] R. Ahlswede and I. Wegener, *Suchprobleme.* B. G. Teubner Stuttgart, 1979.

[3] R. Krichevsky, *Universal Compression and Retrieval.* Kluwer Academic Publishers, 1994.

[4] M. Garey and D. Johnson, *Computers and Intractability.* W. H. Freeman and C., 1979.

[1]This work was supported by RFBR Grant 98-01-00772.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

The Number of Optimal Binary One-Ended Codes

Zsolt Kukorelly[1]
Information Coding Laboratory, University of California, San Diego
kukorell@code.ucsd.edu

Abstract — **Binary prefix-free codes in which all codewords end with "1" are considered. A recursion is given to construct all "optimal" 1-ended codes and to compute the number of such codes with n codewords.**

I. Introduction and Definitions

The problem of finding an optimal D-ary prefix-free code for coding a source with finite output alphabet and known output probabilities has been solved by Huffman [4]. In [1], Berger and Yeung considered the same problem restricted to binary codes whose codewords all end with a "1". As all codes with the same multiset of codeword lengths are equivalent and form an equivalence class, it is enough to look at only one code in each class. Berger and Yeung found a family of classes called *potential classes*, which contains all optimal codes. In [2], Capocelli et al. restricted the family of classes in which all optimal codes must lie to the *e-potential classes*. Golin and Chan [3] found a polynomial-time algorithm for finding the best one-ended code for a given probability distribution.

Our contribution is to determine the family of optimal codes exactly. We also give a method to compute, for any $n \geq 1$, the number of optimal classes of codes with n codewords.

We consider probabilities in non-increasing order and collect them into a *probability vector* $\boldsymbol{p} = (p_1, \ldots, p_n)$. A code with codeword lengths $w_1 \leq \cdots \leq w_n$ has *length vector* $\boldsymbol{w} = (w_1, \ldots, w_n)$ and *multiplicity vector* $\boldsymbol{x} = (x_1, \ldots, x_{\max_i w_i})$, where x_i is the number of codewords of length i. Length vectors and multiplicity vectors determine each other uniquely. Our optimality criterion is the following.

For length vectors $\boldsymbol{w}$ and $\boldsymbol{v}$ with n components, $\boldsymbol{w}$ is *better* than $\boldsymbol{v}$ if $\sum_{i=1}^{n} w_i p_i \leq \sum_{i=1}^{n} v_i p_i$ for all probability vectors $\boldsymbol{p}$ and if there is at least one probability vector for which equality does not hold. This defines a partial ordering. A code with length vector $\boldsymbol{w}$ is *better* than a code with length vector $\boldsymbol{v}$ if $\boldsymbol{w}$ is better than $\boldsymbol{v}$. A multiplicity vector $\boldsymbol{x}$ (corresponding to a length vector $\boldsymbol{w}$) is *better* than a multiplicity vector $\boldsymbol{y}$ (corresponding to a length vector $\boldsymbol{v}$) if $\boldsymbol{w}$ is better than $\boldsymbol{v}$.

A length vector is *optimal* if there is no better length vector of the same length. Optimal multiplicity vectors and optimal codes are defined accordingly.

II. All Optimal Multiplicity Vectors

Theorem 1: Let $f(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i 2^{-i} + x_n 2^{-n}$. A multiplicity vector is optimal if and only if it has one of the following forms ($\boldsymbol{X}$ is a binary string that can be empty):

- $(\boldsymbol{X}, a, b, b, b)$ with $b - a \geq 2$ even and $f(\boldsymbol{X}, a, b) = 1$;
- $(\boldsymbol{X}, a, b, b, b-1)$ with $b - a \geq 2$ even and $f(\boldsymbol{X}, a, b) = 1$;
- $(\boldsymbol{X}, a, a, a, b)$ with $1 \leq b \leq a$ and $f(\boldsymbol{X}, a) = 1$.

[1]This work was performed while the author was with the Signal and Information Processing Laboratory, ETH Zürich, Zurich, Switzerland.

Theorem 2: From the optimal multiplicity vector $(1, 1, 1, 1)$, the following operations on multiplicity vectors allow to construct all optimal multiplicity vectors; moreover, the construction is unique in the sense that every optimal multiplicity vector can be constructed by only one sequence of operations:

- $(\boldsymbol{X}, a, a, a, b) \longmapsto (\boldsymbol{X}, a, a, a, b+1) \quad (1 \leq b \leq a-1)$;
- $(\boldsymbol{X}, a, b, b, b) \longmapsto (\boldsymbol{X}, a, b, b, b, 1)$ and $\longmapsto (\boldsymbol{X}, a-1, b+1, b+1, b) \quad (b - a \geq 0 \text{ even}, a \geq 1)$;
- $(\boldsymbol{X}, 0, b, b, b) \longmapsto (\boldsymbol{X}, 0, b, b, b, 1) \quad (b \geq 2 \text{ even})$;
- $(\boldsymbol{X}, a, b, b, b-1) \longmapsto (\boldsymbol{X}, a, b, b, b) \quad (b - a \geq 2 \text{ even})$;

Corollary: Denote by $A(n)$ the number of optimal multiplicity vectors whose components sum to n. Then $A(n) = \sum_{0 \leq a < n/3} \sum_{1 \leq b < n/3} g(n, a, b)$, where g behaves as follows: for $1 \leq n \leq 4$, $g(n, a, b) = 1$ if and only if $a = b = 1$ and $g(n, a, b) = 0$ otherwise. For $n \geq 5$, g satisfies the following recursions:

1. $g(n, b, 1) = \sum_{\substack{a=0 \\ b-a \text{ even}}}^{b} g(n-1, a, b) \quad (b \geq 1)$;
2. $g(n, a, b) = g(n-1, a, b-1) \quad (2 \leq b \leq a)$;
3. $g(n, a, b) = g(n-1, a, b-1) \quad (b - a \geq 2 \text{ even}, a \geq 0)$;
4. $g(n, a, b) = g(n-1, a+1, b) \quad (b - a \geq 1 \text{ odd}, a \geq 0)$.

The table below gives the first values of $A(n)$.

n	$A(n)$	n	$A(n)$	n	$A(n)$	n	$A(n)$
1	1	11	13	21	174	31	1574
2	1	12	17	22	219	32	1929
3	1	13	23	23	278	33	2362
4	1	14	30	24	348	34	2881
5	2	15	39	25	437	35	3511
6	3	16	50	26	544	36	4264
7	4	17	65	27	678	37	5174
8	5	18	83	28	839	38	6258
9	7	19	107	29	1039	39	7560
10	9	20	136	30	1279	40	9107

Tab. 1: The number $A(n)$ of optimal length vectors of length n.

References

[1] T. Berger, R. W. Yeung, 'Optimum "1"-ended binary prefix codes', *IEEE Trans. Inform. Theory*, Vol. IT-36, pp. 1435-1441, Nov. 1990.

[2] R. M. Capocelli, A. De Santis, G. Persiano, 'Binary prefix codes ending in a "1" ', *IEEE Trans. Inform. Theory*, Vol. IT-40, pp. 1296-1302, Jul. 1994.

[3] M. Golin and S. Chan, "A Dynamic Programming Algorithm for Constructing Optimal "1"-ended Binary Prefix-Free Codes", *Proc. IEEE Intl. Symp. on Inform. Theory* (Cambridge, MA, USA), p. 45, August 1998.

[4] D. A. Huffman, "A method for the construction of minimum redundancy codes", *Proc. IRE*, Vol. 40, pp. 1098-1101, 1952.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Coding of Ordered Trees

Kingo Kobayashi
University of
Electro-Communications,
Chofu, Tokyo 182-8585, Japan
kingo@ice.uec.ac.jp

Hiroyoshi Morita
University of
Electro-Communications,
Chofu, Tokyo 182-8585, Japan

Mamoru Hoshi
University of
Electro-Communications,
Chofu, Tokyo 182-8585, Japan

Abstract — **We study the asymptotic growth of ordered trees, and give important insights in coding of trees from the information theoretic viewpoint. Specifically, we give the optimal length function in a sense that the Kraft inequality is satisfied with equality. It will be revealed that the commonly used pre-order coding for special classes of trees are asymptotically tight, but not always for many of trees.**

I. k-ARY TREES AND GENERALIZED CATALAN NUMBERS

For $k \geq 2$ we define a k-ary tree T as follows: either T is empty or it has a specific node called its root that is connected to $T_1, T_2, \ldots, T_k$, each of which is a k-ary tree. We denote by $\mathcal{T}_k^{(m)}$ the set of all k-ary trees with m internal nodes. The cardinality $c_{k,m}$ of $\mathcal{T}_k^{(m)}$ is known as the generalized Catalan number,

$$c_{k,m} = \frac{1}{km+1}\binom{km+1}{m}. \tag{1}$$

Although each k-ary tree having m internal nodes is often identified with a binary pre-order prefix sequence of length $km+1$, the following theorem suggests the existence of more efficient code for k-ary trees when k is greater than two.

Theorem 1 [1] For $k \geq 2$, we have

$$\sum_{m=0}^{\infty} c_{k,m} 2^{-\{g(k)m + \log_2(k/(k-1))\}} = 1, \tag{2}$$

where $g(k) = k\log_2 k - (k-1)\log_2(k-1) = kh(1/k)$ and $h(p) = -p\log_2 p - (1-p)\log_2(1-p)$ is the binary entropy function.

II. **k**-ARY TREES

Let us extend the results of the k-ary tree in the previous section to that of the **k**-ary tree, where $\mathbf{k} = (k_1, k_2, \ldots, k_s)$ is a vector of positive distinct integers.

Thus, a **k**-ary tree T is recursively defined either to be a single node (leaf) or to have a specific node called its root that is connected to $T_1, T_2, \ldots, T_{k_i}$ for some k_i, each of which is a **k**-ary tree. We denote by $\mathcal{T}_{\mathbf{k}}^{(n)}$ the set of all **k**-ary trees with n nodes, including both external and internal nodes together.

From the symbolic consideration, it can be deduced that the generating function

$$U = U_{\mathbf{k}}(z) = \sum_{n=0}^{\infty} u_{\mathbf{k},n} z^n \tag{3}$$

satisfies the following functional equation:

$$U = z + zU^{k_1} + zU^{k_2} + \cdots + zU^{k_s}, \tag{4}$$

where $u_{\mathbf{k},n}$ is the cardinality of $\mathcal{T}_{\mathbf{k}}^{(n)}$, that is, the number of **k**-ary trees of size n.

Then, the coefficient $u_{\mathbf{k},n}$ is given by using the generalized Catalan numbers,

$$u_{\mathbf{k},n} = \sum_{1+\sum_{i=1}^{s} k_i n_i = n} \frac{1}{n}\binom{n}{n_1, n_2, \cdots, n_s, n-\sum_{i=1}^{s} n_i}. \tag{5}$$

Each term in the above sum (5) represents the number of trees which have n_i internal nodes having k_i outgoing branches for $i = 1, \ldots, s$.

The next theorem answer the size of which term in the above sum is maximum.

Theorem 2

$$\min_{u>0} \frac{1 + u^{k_1} + u^{k_2} + \cdots + u^{k_s}}{u} = \max_{\substack{\sum_{i=0}^{s} p_i = 1 \\ \sum_{i=1}^{s} k_i p_i = 1}} e^{H(p_0, p_1, \ldots, p_s)}, \tag{6}$$

where $H(p_0, p_1, \ldots, p_s) = \sum_{i=0}^{s} -p_i \log p_i$ is the entropy.

III. OPTIMUM LENGTH FUNCTION FOR **k**-ARY TREE CODE

Setting

$$\kappa = \frac{1}{\rho} = \frac{1 + \tilde{u}^{k_1} + \cdots + \tilde{u}^{k_s}}{\tilde{u}}, \tag{7}$$

where

$$1 + \tilde{u}^{k_1} + \tilde{u}^{k_2} + \cdots + \tilde{u}^{k_s} = k_1\tilde{u}^{k_1} + k_2\tilde{u}^{k_2} + \cdots + k_s\tilde{u}^{k_s}, \tag{8}$$

we can deduce from analytical considerations that ρ is the dominant positive singularity of $U_{\mathbf{k}}(z)$, and

$$U_{\mathbf{k}}(\rho) = U_{\mathbf{k}}(\kappa^{-1}) = \tilde{u}. \tag{9}$$

That is, we have

Theorem 3

$$\sum_{n=1}^{\infty} u_{\mathbf{k},n} e^{-\{(\log\kappa)n + \log\tilde{u}\}} = 1. \tag{10}$$

Thus, the length function $l_{\mathbf{k}}(n) = (\log\kappa)n + \log\tilde{u}$ satisfies the Kraft inequality with equality. This function is best possible in a sense that the coefficient of the linear term cannot be made smaller than $\log\kappa$ so far as we want to have separable codes for **k**-ary trees.

REFERENCES

[1] K.Kobayashi, H.Morita and M.Hoshi, "Enumerative Coding for k-ary Trees," *Proceedings of the 1997 IEEE International Symposium on Information Theory*, p.423, 1997.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Universal Lossless Coding of Sources with Large and Unbounded Alphabets[1]

En-hui Yang and Yunwei Jia
Dept. of E&CE, University of Waterloo, Waterloo, ON, Canada N2L 3G1
Emails: ehyang@bbcr.uwaterloo.ca yjia@bbcr.uwaterloo.ca

Abstract — **A multilevel arithmetic coding algorithm is proposed to encode data sequences with large or unbounded source alphabets. The algorithm is universal in the sense that it can achieve asymptotically the entropy rate of any independently and identically distributed integer source with a finite or infinite alphabet, as long as the mean value is finite.**

I. Introduction

In many data compression systems, one often has to efficiently compress integer sequences. For example, in run-length coding, one has to efficiently encode a sequence of runs of 0's and 1's, which is transformed from the original binary sequence; in grammar-based coding[4], one has to efficiently compress a sequence of integers with potentially unbounded number of distinct integers.

When the size of the alphabet from which data sequences are drawn is large enough, however, the problem of universal compression of these data sequences is not as simple as it may look like. Due to the well-known underflow and overflow problems, finite precision implementations of the traditional adaptive arithmetic coding[2] cannot work if the size of the source alphabet exceeds a certain limit. On the other hand, although some existing coding schemes such as the Golomb codes, Elias codes[1], and their variants can process integer sequences with infinite alphabets, they are not universal in the sense that, for most memoryless sources, their compression rates are strictly above the entropy rates of these sources.

In this study, we propose a new practical coding method, called multilevel arithmetic coding, to encode data sequences with large or even unbounded alphabets. For any data sequence $X = x_1x_2\cdots x_n$ to be compressed, let S_X denote the set that consists of all the distinct symbols appearing in X. In general, as X gets longer and longer, S_X may grow without bound. This new method converts the dynamically changing set S_X into a dynamic tree, whose leaves represent small subsets of S_X and, together, form a partition of S_X. For each symbol x_i in the sequence X, let y_i denote the path in the tree from the root to the leaf containing the symbol x_i. Let z_i denote the index of x_i in the corresponding leaf sub-alphabet. The sequence X is then fully represented by the sequences $Y = y_1y_2\cdots y_n$ and $Z = z_1z_2\cdots z_n$. From information theory, we have

$$H(X) = H(Y,Z) = H(Y) + H(Z|Y), \qquad (1)$$

where $H(X)$, $H(Y,Z)$, and $H(Y)$ are the empirical entropy of the input sequence X, the path and index sequence (Y,Z), and the path sequence Y, respectively, and where $H(Z|Y)$ is the empirical conditional entropy of the index sequence given the path sequence. The above equation implies that to encode X, one may instead encode Y first and then conditionally encode Z given Y. This forms the information theoretical basis for the proposed multilevel arithmetic coding algorithm.

II. Algorithm Description and Optimality Result

Consider the general case that the alphabet may increase without bound, and the decoder does not know how it grows. To encode such a data sequence $X = x_1x_2\cdots x_n$, we combine Elias coding[1] with a dynamically updated binary search tree. The proposed algorithm works as follows: For each symbol x_i in the input sequence, if it has not appeared before in $x_1\cdots x_{i-1}$, use the Elias code to encode x_i and then add this symbol to the corresponding leaf sub-alphabet and update the tree structure; if x_i has appeared before, then encode the corresponding path in the dynamic tree and the index in the corresponding leaf sub-alphabet. For the details about how the dynamic tree is updated, and other details of the algorithm, please see the full paper[3]. Here we just give the following theorem without proof.

Theorem 1 *For any i.i.d. integer source $\{x_i\}_{i=1}^{\infty}$ with finite mean, the proposed algorithm can achieve asymptotically the entropy rate of the source.*

III. Conclusion

The advantages of the proposed algorithm over the traditional adaptive arithmetic coding algorithm are two folds: (1) the proposed algorithm can be used to encode any data sequence no matter whether the corresponding source alphabet is finite or infinite, while the traditional adaptive arithmetic coding algorithm can work only for data sequences with bounded, small alphabets; (2) in the situation in which the traditional adaptive arithmetic coding algorithm can work, the proposed algorithm can reduce coding complexity and improve compression performance.

[1]This work was supported in part by the Natural Sciences and Engineering Research Council of Canada under Grant RGPIN203035-98, by the Premier's Research Excellence Awards of Ontarion, and by the Communications and Information Technology Ontario.

References

[1] P. Elias,"Universal codeword sets and representations of the integers," *IEEE Trans. Inform. Theory*, Vol.IT-21, pp. 194–203, 1975.

[2] I.H. Witten, R. Neal and J. G. Cleary, "Arithmetic coding for data compression", *Comm. for ACM*, 30(6), pp. 520–540, June 1987.

[3] E.-H. Yang and Y. Jia, "Universal lossless coding of sources with large or unbounded alphabets," in *Numbers,Information and Complexity*, Kluwer, pp. 421-442, 2000.

[4] E.-H. Yang and J. C. Kieffer, "Efficient universal lossless data compression algorithms based on a greedy sequential grammar transform — Part one: without context models", will appear in *IEEE Trans. Inform. Theory*, May 2000.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

An Efficient Test for the Possibility of Information-Theoretic Key Agreement Secure Against Active Adversaries

Stefan Wolf [1]

Abstract — **We describe a mechanical model for representing discrete distributions and show that it leads to an efficient test for the possibility of key agreement unconditionally secure against active adversaries.**

I. Motivation

Assume that two parties Alice and Bob have access to independent realizations of the random variables X and Y, respectively, and that an adversary Eve knows Z. Let P_{XYZ} be the joint distribution of the three random variables. Can Alice generate a string M such that Bob is convinced that M comes from Alice and not from Eve? Clearly, the answer to this question depends on P_{XYZ}, more precisely, on the following property of P_{XYZ}.

Definition 1. Let X, Y, and Z be random variables. Then X *is simulatable by* Z *with respect to* Y, denoted by $\mathrm{sim}_Y(Z \to X)$, if there exists a conditional distribution $P_{\overline{X}|Z}$ such that $P_{\overline{X}Y} = P_{XY}$ holds, where $P_{\overline{X}Y} = \sum P_{YZ} \cdot P_{\overline{X}|Z}$.

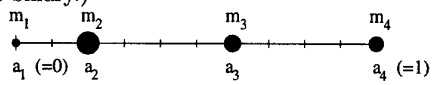
It is not surprising that Eve can impersonate Alice towards Bob if and only if $\mathrm{sim}_Y(Z \to X)$ holds. In case of non-simulatability, the string M can be a sufficiently long block of independent realizations of X.

Another, closely related, application of the simulatability condition is the following. The XYZ-scenario was considered with respect to the question whether Alice and Bob can, by communication over an insecure channel, generate a secret key S about which the adversary has virtually no information. As the important quantities in this context, the secret-key rate $S(X;Y||Z)$, with respect to *passive* adversaries, and the *robust* secret-key rate $S^*(X;Y||Z)$, secure against *active* adversaries with complete control over the communication channel, were defined [1]. It was shown that either $S^*(X;Y||Z) = S(X;Y||Z)$ or $S^*(X;Y||Z) = 0$ holds, and that the simulatability condition separates the two cases: If neither $\mathrm{sim}_Y(Z \to X)$ nor $\mathrm{sim}_X(Z \to Y)$ holds, then secret-key agreement secure against active adversaries is possible at the same rate as against passive wire-tappers, but completely impossible otherwise.

Unfortunately, the simulatability condition is a priori not very helpful since it is not clear how it can be verified in finite time, let alone efficiently. It is the goal of this note to present a new intuitive formalism based on a mechanical model, and to show that this leads to efficient criteria for simulatability.

II. A Mechanical Model for Discrete Distributions and Channels

Let us consider the following representation of joint distributions of discrete random variables U and V. For simplicity, we assume that V is binary, i.e., $\mathcal{V} = \{v_0, v_1\}$. Then the constellation $M_{U \leftarrow V}$ is defined by the list of pairs $M_{U \leftarrow V} := (P_U(u), P_{V|U=u}(v_0))_{U \in \mathcal{U}}$. The pairs of such a constellation $M = (m_i, a_i)_{i=1\ldots l}$ can be represented as mass points in the interval $[0,1]$, where m_i determines the mass of a point, and a_i is its position. (This representation is one-dimensional because V is binary.)



Definition 2. Let $M = (m_i, a_i)_{i=1\ldots l}$ be a constellation with $\sum m_i = 1$. The center of gravity of M is defined as $\sum m_i a_i$. We say that a constellation $M' = (m'_i, a'_i)_{i=1,\ldots,l'}$ is derived from M by *mass splitting* if it arises from M by replacing a pair (m_i, a_i) by two pairs (pm_i, a_i) and $((1-p)m_i, a_i)$ for some $0 \le p \le 1$. Furthermore, M' is derived from M by *mass union* if two pairs (m_i, a_i) and (m_j, a_j) are replaced by the single pair $(m_i + m_j, (m_i a_i + m_j a_j)/(m_i + m_j))$, corresponding to the sum mass in the center of gravity of the two masses. We call mass splitting and mass union *basic mass operations*. Neither of them changes the center of gravity. A constellation M is called *stronger* than M', denoted by $M \rightsquigarrow M'$, if there exists a finite sequence of basic operations that transforms M into M'.

Note first that $\mathrm{sim}_Y(Z \to X)$ is equivalent to $M_{Z \leftarrow Y} \rightsquigarrow M_{X \leftarrow Y}$. The reason is that a channel $P_{\overline{X}|Z}$ can be translated into a sequence of basic mass operations in the mechanical model, and vice versa. However, this does not directly lead to an efficiently verifiable criterion for simulatability. It is only a reformulation of the condition. We now define a property of a pair of mass constellations which is efficiently checkable and equivalent to one constellation being stronger than the other.

Definition 3. For a mass constellation M and for $0 < t \le 1$, we denote by $\ell_t(M)$ the leftmost masses of M of total amount t. A constellation M' is called *more centered* than M, denoted by $M' \prec M$, if for all t, $c(\ell_t(M')) \ge c(\ell_t(M))$ holds, where $c(S)$ stands for the center of gravity of a set S of masses.

Given two mass constellations M and M', this condition can be checked in linear time. Indeed, note that $M' \prec M$ is equivalent to the fact that for every $1 \le k < l'$, the center of the set of masses $m'_1, \ldots, m'_k$ is not left of (i.e., smaller than) the center of $\ell_{m'_1 + \cdots + m'_k}(M)$.

Theorem 1. *Let P_{XYZ} be the joint distribution of random variables X, Y, and Z, where Y is binary. Then $\mathrm{sim}_Y(Z \to X)$ is equivalent to $M_{X \leftarrow Y} \prec M_{Z \leftarrow Y}$.*

If Y is N-ary, the distribution can be represented in an $(N-1)$-dimensional space. However, the straight-forward generalization of the above condition is not always sufficient. It is an open problem to find an efficient test for the general case.

References

[1] U. Maurer, "Information-theoretically secure secret-key agreement by NOT authenticated public discussion," *EUROCRYPT '97*, LNCS, vol. 1233, pp. 209–225, 1997.

[1]Department of Computer Science, ETH Zürich, CH-8092 Zürich, Switzerland. E-mail: wolf@inf.ethz.ch

0-7803-5857-0/00/$10.00 ©2000 IEEE.

From Weak to Strong Information-Theoretic Key Agreement

Ueli Maurer [1] Stefan Wolf [1]

Abstract — **In the original definitions of information-theoretic secret-key agreement, the required secrecy condition was too weak. We show, by a generic reduction, that it can be strengthened without any effect on the achievable key-generation rate.**

I. Models of Information-Theoretic Secret-Key Agreement

Motivated by Wyner's wire-tap channel [7], different settings for information-theoretic secret-key agreement have been proposed by Csiszár and Körner [3] and Maurer [5]. Whereas in the model of [3], Alice is connected to Bob and Eve by a noisy broadcast channel characterized by $P_{YZ|X}$ (Alice sends X and Bob and Eve receive Y and Z, respectively), only correlated information, but not insecure communication is regarded as a resource in the model of [5]. Here, the parties Alice and Bob are connected by a noiseless and authentic but otherwise insecure channel and have access to random variables X and Y, respectively, whereas the adversary knows Z.

In both settings, the capability of generating a secret key has been defined asymptotically as the maximal achievable key-generation rate (i.e., the number of resulting key bits per channel use or per realization of the triple XYZ, respectively) such that the adversary obtains information at an arbitrarily small rate only. The corresponding quantities were called the *secrecy capacity* $C_S(P_{YZ|X})$ [3] and the *secret-key rate* $S(X;Y||Z)$ [5], respectively. However, the secrecy condition which only limits the *rate* at which Eve obtains information about the key does not imply that the adversary's information is bounded in an absolute sense, let alone negligibly small. This is clearly unsatisfactory and motivated the definition of strong variants of secrecy capacity $\overline{C_S}(P_{YZ|X})$ [2] and secret-key rate $\overline{S}(X;Y||Z)$ [4], requiring that the adversary's information about the resulting key is small in total.

In [4], a lower bound on $\overline{S}(X;Y||Z)$ was shown, whereas in [2], a result similar to Corollary 2 below was proved (with techniques different from ours). In this note we describe a generic method for strengthening the security of any information-theoretic key agreement by using only a negligible amount of extra communication from Alice to Bob and such that the effective key-generation rate is asymptotically equal to the rate with respect to the weak definition.

II. A General Method for Strengthening the Security

Definition 1. Let $\varepsilon > 0$ be a real number and let N be a positive integer. A *weak key agreement with parameters ε and N* ($KA(\varepsilon, N)$ for short) between two parties Alice and Bob and with respect to an adversary Eve outputs three random variables S_A, S_B, and U, known to Alice, Bob, and Eve, respectively, such that $\mathrm{Prob}[S_A \neq S_B] < \varepsilon$, $H(S_A) \geq (1-\varepsilon)N$, and $I(S_A;U) < \varepsilon N$ hold.

Such key agreement is called *strong*, denoted by $\overline{KA}(\varepsilon, N)$, if the random variables S_A, S_B, and U satisfy the following more restrictive conditions. There must exist a string S with $\mathrm{Prob}[S = S_A = S_B] > 1-\varepsilon$, $H(S) = \log|\mathcal{S}| \geq (1-\varepsilon)N$, and $I(S;U) < \varepsilon$.

Theorem 1. *Assume that a noiseless channel from Alice to Bob is given to which Eve has perfect read access. Then weak key agreement can be converted into strong key agreement such that the key is generated asymptotically at the same rate and the amount of required extra communication is asymptotically vanishing. More precisely, for every $\varepsilon > 0$ there exists $\alpha > 0$ such that for all sufficiently large M and for all sufficiently large N, $\overline{KA}(\varepsilon, N)$ can be reduced to $K = (1+o(1))N/M$ realizations of $KA(\alpha, M)$ such that the length $\mathrm{len}(C)$ of the message C sent over the insecure channel by Alice is of order $\mathrm{len}(C) = o(N)$.*

The proof idea is as follows. First, weak key agreement is repeated many times. Then, error correction information is sent from Alice to Bob (and hence to Eve), allowing Bob to reconstruct Alice's sequence of weak keys with high probability. Finally, this string is transformed into a highly secret key by *privacy amplification*. Universal hashing, as proposed in [1], is not a good choice for hashing the string in this situation since the required amount of communication, i.e., the specification of a particular function from the universal class, would be too high (thus reducing the achievable key-generation rate in the broadcast-channel model). As a new method in this context, we use *extractors* [6] instead. This allows for keeping the extra communication negligible.

Theorem 1 directly implies that in both models described above, the secrecy requirements can be strengthened without effect on the achievable key-generation rates.

Corollary 2. $\overline{C_S}(P_{YZ|X}) = C_S(P_{YZ|X})$.

Corollary 3. $\overline{S}(X;Y||Z) = S(X;Y||Z)$.

References

[1] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Transactions on Information Theory*, Vol. 41, No. 6, pp. 1915–1923, 1995.

[2] I. Csiszár, "Almost independence and secrecy capacity (in Russian)," in *Problems of Information Transmission (PPI)*, Vol. 32, No. 1, pp. 48–57, 1996.

[3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, Vol. 24, No. 3, pp. 339–348, 1978.

[4] U. M. Maurer, "The strong secret key rate of discrete random triples," in *Communication and Cryptography – Two Sides of One Tapestry*, Kluwer Academic Publishers, pp. 271–285, 1994.

[5] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, Vol. 39, No. 3, pp. 733–742, 1993.

[6] S. P. Vadhan, "Extracting all the randomness from a weakly random source," *Electronic Colloquium on Computational Complexity*, Tech. Rep. TR98-047, 1998.

[7] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, Vol. 54, No. 8, pp. 1355–1387, 1975.

[1]Department of Computer Science, ETH Zürich, CH-8092 Zürich, Switzerland. E-mail: {maurer,wolf}@inf.ethz.ch

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Information–Theoretic Analysis of Information Hiding

Pierre Moulin[1]
Univ. of Illinois, Beckman Institute and ECE Dept
405 N. Mathews Ave., Urbana, IL 61801
moulin@ifp.uiuc.edu

Joseph A. O'Sullivan
Washington Univ., Dept of Electrical Engineering
St Louis, MO 63130
jao@ee.wustl.edu

Abstract — **Information hiding is analyzed as a communication game between an information hider and an attacker, in which side information is available to the information hider and to the decoder. Capacity formulas are derived.**

I. Statement of the Problem

Information hiding is an emerging research area which encompasses applications such as watermarking, fingerprinting, and steganography. This paper extends results from [1]; see [2] for more details.

Consider a host–data source producing random variables $\tilde{X}$ taking values in a finite alphabet $\mathcal{X}$, a cryptographic–key source producing random variables $K \in \mathcal{K}$, and a message source producing a message M from a message set $\mathcal{M}$. The *host data* is a sequence $\tilde{X}^N = (\tilde{X}_1, \cdots, \tilde{X}_N)$. A cryptographic key $K^N = (K_1, \cdots, K_N)$ is available both at the encoder and the decoder. In particular, K^N enables the use of randomized codes. The pairs (X_i, K_i) are i.i.d. $p(\tilde{x}, k)$. This model includes $K = \tilde{X}$ as a special case [1]. The message M is uniformly distributed over the message set $\mathcal{M}$. The information hider passes $\tilde{X}^N$, K^N, and the message m through an embedding function f_N, producing *composite data* X^N that are made publicly available[1]. Next, the attacker passes X^N through a random attack channel $Q^N(y^N|x^N)$ to produce corrupted data Y^N, in an attempt to remove traces of M.

Both the embedding and the attack are subject to distortion constraints, respectively $Ed^N(\tilde{x}^N, f_N(\tilde{x}^N, m, k^N)) \leq D_1$ and $Ed^N(x^N, y^N) \leq D_2$, where $d^N(x^N, y^N) = \frac{1}{N}\sum_{k=1}^N d(x_k, y_k)$ is a distortion function on N-tuples. Here $d : \mathcal{X} \times \mathcal{X} \to \mathbb{R}_+$ is a bounded, nonnegative function.

The rate of the code is $R = \frac{1}{N}\log|\mathcal{M}|$. The average probability of error is $P_{e,N} = \frac{1}{|\mathcal{M}|}\sum_m P(\phi_N(Y^N, K^N) \neq m \mid M = m)$, where ϕ_N is the decoding function. A rate R is achievable for distortions (D_1, D_2), if there is a sequence of codes $(\mathcal{M}, f_n, \phi_N)$ subject to distortion D_1, with rates $R_N > R$ such that $P_{e,N} \to 0$ as $N \to \infty$, for any attack subject to distortion D_2. The *information–hiding capacity* $C(D_1, D_2)$ is the supremum of all achievable rates for distortions (D_1, D_2).

II. Main Result

Consider first memoryless attack channels. Define a *covert channel* $\tilde{Q}(x, u|\tilde{x}, k)$ (to be designed by the information hider), where $u \in \mathcal{U}$ is an auxiliary random variable, $\mathcal{U}$ is an arbitrary finite alphabet, and $\sum_{x,\tilde{x},k,u} d(\tilde{x}, x)\tilde{Q}(x, u|\tilde{x}, k)p(\tilde{x}, k) \leq D_1$. Denote by $\tilde{\mathcal{Q}}$ and $\mathcal{Q}$ the sets of admissible covert and attack channels, subject to respective distortion constraints (D_1, D_2).

The proof of Theorem 1 below relies on a proof of achievability and a converse for a fixed attack channel and is closely related to work by Gel'fand and Pinsker [3].

[1]P. Moulin was supported by NSF grant MIP-97-07633.

[1]X^N is often referred to as the *watermarked signal.*

Theorem 1 *Assume the attacker knows $\tilde{Q}$ and the decoder knows $\tilde{Q}$ and Q. For any attack subject to distortion D_2, a rate R is achievable iff $R < C$, where*

$$C = \max_{\tilde{Q}(x,u|\tilde{x},k)\in\tilde{\mathcal{Q}}} \min_{Q(y|x)\in\mathcal{Q}} J(\tilde{Q}, Q), \tag{1}$$

$(U, \tilde{X}, K) \to X \to Y$ is a Markov chain, and $J(\tilde{Q}, Q) \triangleq I(U;Y|K) - I(U;\tilde{X}|K)$.

If $K = \tilde{X}$ (host data available at the decoder), the solution becomes a saddlepoint of $I(X;Y|\tilde{X})$ [1].

III. Continuous Alphabets

The results above can be extended to the case of infinite alphabets $\mathcal{X}, \mathcal{U}, \mathcal{K}$. The case of Gaussian $\tilde{X}$ ($\sim \mathcal{N}(0, \sigma^2)$) and squared–error distortion measure $d(x, y) = (x - y)^2$ is of considerable interest. When $K = \tilde{X}$, the hiding capacity is given by $C = \frac{1}{2}\log\left(1 + \frac{D_1}{\beta D_2}\right)$ if $D_2 < \sigma^2 + D_1$, and 0 otherwise. Here $\beta = \left(1 - \frac{D_2}{\sigma^2 + D_1}\right)^{-1}$. The optimal covert channel $\tilde{Q}$ is given by $X = \tilde{X} + Z$, where $Z \sim \mathcal{N}(0, D_1)$ is independent of $\tilde{X}$. The optimal attack is the Gaussian test channel from R/D theory, with distortion level $\min(D_2, \sigma^2 + D_1)$.

For blind information hiding (no key), the optimal attack $Q(y|x)$ is again the Gaussian test channel, and the optimal $\tilde{Q}(x, u|\tilde{x})$ is the same distribution that achieves capacity in a problem studied by Costa [4]. The capacity is the same whether or not the host data are known at the decoder.

If $\tilde{X}$ is non–Gaussian with mean zero and variance σ^2, C above is an upper bound on hiding capacity. For small D_1 and D_2 (typical of many information–hiding problems), a remarkable result arises: the hiding capacity under the squared-error distortion metric is equal to $\frac{1}{2}\log\left(1 + \frac{D_1}{D_2}\right)$ *independently of the statistics of $\tilde{X}$, asymptotically as $D_1, D_2 \to 0$.*

IV. Further Extensions

The results above have been extended to the case of blockwise i.i.d. $(\tilde{X}_i, K_i)$ and blockwise i.i.d. attacks. If $(\tilde{X}_i, K_i)$ are i.i.d., then the optimal attack is memoryless. The framework developed in this paper can also be used to analyze the performance of a variety of information–hiding systems [2].

References

[1] J. A. O'Sullivan, P. Moulin, and J. M. Ettinger, "Information–Theoretic Analysis of Steganography," *Proc. IEEE Int. Symp. on Info. Thy*, Cambridge, MA, p. 297, Aug. 1998.

[2] P. Moulin and J. A. O'Sullivan, "Information-Theoretic Analysis of Information Hiding," preprint, Sep. 1999. Available from `www.ifp.uiuc.edu/ ~moulin/Papers/hiding.ps`.

[3] S. I. Gel'fand and M. S. Pinsker, "Coding for Channel with Random Parameters," *Problems of Control and Information Theory*, Vol. 9, No. 1, pp. 19—31, 1980.

[4] M. Costa, "Writing on Dirty Paper," *IEEE Trans. Info. Thy*, Vol. 29, No. 3, pp. 439—441, May 1983.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Information-Theoretically Secure Keyless Authentication

Valeri Korjik
IPN-Cinvestav, 2508, ESQ.Ticoman, C.P.07000,Mexico D.F.
Fax : (52)-5747-7088. E-mail: vkorjik@mail.cinvestav.mx
Maxim Bakin
State University of Telecommunications, St.Petersburg, Russia
Moika 65, C.P.191186, E-mail: maxusb@hotmail.com

We consider a cryptographic scenario of two honest parties A and B facing an active eavesdropper E. They share no secrete key initially but their final goal is to generate a shared information-theoretically secure key. We develop the special case represented in [1] where a random binary string is broadcasted by some center (like a satellite) over binary symmetric channels and received as X, Y, Z-strings with bit error probabilities ε_A, ε_B, ε_E ($\varepsilon_A<\varepsilon_E$, $\varepsilon_B<\varepsilon_E$) by legal parties and the intruder, respectively. The authentication protocol is a procedure to append some bit positions of X taken in line by certain rule to every message being transmitted from A to B. This rule can be chosen as some binary block code that compares messages and code words one-to-one. Party B accepts the message as original if and only if the fraction of bits in the received authenticator that agree with the corresponding bits of his string Y exceeds some fixed threshold. Otherwise B rejects the message considering it to be false. It was remarked in [1] that the distance property of a code used for such authentication differs from the Hamming distance and it should be changed to *semidistance.*

A simple construction of constant weight authentication codes based on linear binary codes which provide fixed *minimum code semidistance* was given in [1].

Using this construction we derive the formulas to estimate the probabiity that a modification of the message by an intruder is not detected by party B and the probability that B accepts the message if an intruder has not intervened at all. We propose several methods how to design authentication codes based on the use of nonlinear codes that can be more effective in some cases.

Unfortunately, the use of any authentication code as a part of key sharing procedure turns out to be inefficient because it requires so long authenticators that results in a very small key rate. The way out of this situation is to consider the so called *hybrid authentication* that based both on a *code authentication* and on a *hashing* in the *Almost Strong Universal*$_2$ class .We proof several statements and derive the formulas to estimate its efficiency.

References.

[1] U.M.Maurer, "Information-theoretically secure secrete-key agreement by NOT authenticated public discussion", *Lecture notes in computer science,Advances in Cryptology*, Eurocrypt'97,No.1233,pp.209-225.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On Point-to-Point Communication Networks

Lihua Song
Dept. of Information Engineering
The Chinese Univ. of Hong Kong
Shatin, New Territories
Hong Kong, China
e-mail: lhsong7@ie.cuhk.edu.hk

Raymond W. Yeung
Dept. of Information Engineering
The Chinese Univ. of Hong Kong
Shatin, New Territories
Hong Kong, China
e-mail: whyeung@ie.cuhk.edu.hk

Abstract — **A point-to-point communication network is represented by $(G, \mathbf{C})$, where $G = (\mathcal{V}, \mathcal{E})$ is a directed graph with vertex set $\mathcal{V}$ and edge set $\mathcal{E}$, and $\mathbf{C} = [C_{ij}, (i,j) \in \mathcal{E}]$ is a nonnegative-valued vector. A vertex in $\mathcal{V}$ represents a node in the communication network, and an edge (i,j) represents a point-to-point discrete memoryless channel (DMC) from node i to node j whose capacity is C_{ij}. We assume that the channels in the network are independent of each other. An information source with entropy rate h is generated at source node s and recovered at sink node t with arbitrarily small probability of error. We show that the value of a max-flow from node s to node t in $(G, \mathbf{C})$ must be greater than or equal to h. This results implies a separation theorem for network coding and channel coding in such a communication network.**

I. Introduction

A point-to-point communication network can be represented by $(G, \mathbf{C})$, where $G = (\mathcal{V}, \mathcal{E})$ is a directed graph with vertex set $\mathcal{V}$ and edge set $\mathcal{E}$, and $\mathbf{C} = [C_{ij}, (i,j) \in \mathcal{E}]$ is a nonnegative-valued vector. A vertex in $\mathcal{V}$ represents a node in the communication network, and an edge $(i,j) \in \mathcal{E}$ represents a point-to-point discrete memoryless channel (DMC) from node i to node j whose capacity is C_{ij}. All the channels in the network are independent of each other. We assume that there are a source node s and a sink node t in G such that the information source is generated at node s and recovered at node t. In the network, there is a dedicated encoder E_{ij} at node i ($i \neq t$) for each output channel $(i,j) \in \mathcal{E}$. Each encoder E_{ij} receives all the information sent to node i via the channels $(i',i) \in \mathcal{E}$. At the sink node t, there is a decoder which recovers the information source.

A code on a network of point-to-point channels can be very complicated in general, especially if the network is cyclic. In [1], we define a *realizable* code which covers almost all possible codes on a network. A triple $(G, \mathbf{C}, h)$ is *admissible* if there exists a realizable code on network $(G, \mathbf{C})$ such that information can be transmitted at rate h from node s to node t with arbitrarily small probability of error. Define the *capacity* of a network $(G, \mathbf{C})$ as the supremum of all h such that $(G, \mathbf{C}, h)$ is admissible.

II. Main results

Suppose there exists a realizable code on G such that an information source with entropy rate h generated at node s can be recovered at node t with arbitrarily small probability of error. A cut in G represents a collection of channels which separates node s and node t. A channel across a cut is called a *forward* channel if its direction is from node s to node t, otherwise it is called a *reverse* channel. If there is no reverse channel across the cut, the information source, the inputs of the channels across the cut, the outputs of the channels across the cut, and the reproduction of the information source by the decoder at node t form a Markov chain in this order. By the data processing theorem, the capacity of the cut (i.e., the total capacity of forward channels across the cut) must be greater than or equal to h.

However, a cut may contain reverse channels, even if G is acyclic. In this case, the Markov chain to which we applied the data processing theorem above does not always hold. The main result in [1] is that the capacity of any cut must be greater than or equal to h. The following theorem resembles the Max-flow Min-cut theorem [2] in network flow theory.

Theorem 1 *If $(G, \mathbf{C}, h)$ is admissible, then the value of a max-flow from the source to the sink is greater than or equal to h.*

Ahlswede et al [3] studied the problem in which for all edges $(i,j) \in \mathcal{E}$, information can be sent from node i to node j noiselessly, i.e., $C_{ij} = \infty$. This is the network coding problem associated with the problem we study in this work, except that they consider multicasting the information source from the source node to possibly more than one sink node in the network. Let R_{ij} be the coding rate of encoder E_{ij} for $(i,j) \in E$, and let $\mathbf{R} = [R_{ij}, (i,j) \in \mathcal{E}]$. They proved that it is possible to multicast information at rate h from the source node to each sink node if and only if the value of a max-flow from the source node to each sink node in $(G, \mathbf{R})$ is greater than or equal to h. From this result and Theorem 1, we can determine the capacity of a network.

Theorem 2 *The capacity of a network $(G, \mathbf{C})$ is equal to the value of a max-flow from node s to node t.*

It also follows from this theorem that in our problem, asymptotic optimality can always be achieved by separating network coding and channel coding. Generalization of our problem to multicasting the information source from the source node to a number of sink nodes is straightforward.

References

[1] L. H. Song and R.W. Yeung, "*On point-to-point communication networks*", in preparation.

[2] L. R. Ford and D. R. Fulkerson, *Flows in Networks,* Princeton University Press, Princeton, NJ, 1962.

[3] R. Ahlswede, N. Cai, S. Y. R. Li and R. W. Yeung, "*Network information flow: Single source,*" submitted to IEEE Transactions on Information Theory.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

The Gaussian Parallel Relay Network

Brett Schein
Laboratory for Information and Decision Systems
M.I.T.
e-mail: schein@mit.edu

Robert Gallager
Laboratory for Information and Decision Systems
M.I.T.
e-mail: gallager@lids.mit.edu

Abstract — **We introduce the real, discrete-time Gaussian parallel relay network. This simple network is theoretically important in the context of network information theory. We present upper and lower bounds to capacity and explain where they coincide.**

I. Introduction

In some contexts, cooperation between terminals in a multiple terminal system can enlarge the set of reliably achievable rates. For systems where power is of primary importance, such as in wireless or ad hoc networks, terminals can cooperate by sending signals with a common component. This common component coherently combines at a receiver, resulting in an increased effective power. Exploiting this requires common information at distributed points and synchronization of the carriers in a wireless system. Investigating how this can be accomplished is important for improving both real-world systems and theoretical understanding of networks.

To this end, we assume that carrier synchronization is feasible and introduce the real, discrete-time Gaussian parallel relay network, illustrated in Figure 1. We wish to find the capacity of the network when the only source of extrinsic information is encoded into the signal $\mathbf{X}$. The sole purpose of the relays is to get the information from $\mathbf{X}$ to a decoder observing $\mathbf{Y}$. We assume the noise processes are independent and are white with variances N_1, N_2, and N. Further, we assume the network input and relays have average power constraints P_x, P_1, and P_2. The network is thus parametrized by four signal to noise ratios (SNR's): $S_1 = \frac{P_x}{N_1}$, $S_2 = \frac{P_x}{N_2}$, $S_3 = \frac{P_1}{N}$, and $S_4 = \frac{P_2}{N}$. This network is similar to the relay channel introduced in [1] and studied in [2]. It differs via Relay 2, which provides an important separation between the source and destination.

II. Upper bounds to capacity

Due to the presence of the relays, it is not surprising that tight upper bounds to network capacity are difficult to determine. The first upper bound is a result of the data processing theorem applied to the broadcast side of the network.

$$R \le \frac{1}{n} I(\mathbf{X}^n; \mathbf{Y_1}^n, \mathbf{Y_2}^n) \le \frac{1}{2}\ln(1 + S_1 + S_2). \qquad (1)$$

The second upper bound is more involved and can be derived almost exactly as in [2] for the physically degraded Gaussian relay channel.

$$R \le \max_{\alpha\in[0,1]} \min[\frac{1}{2}\ln\left((1+S_1)(1+(1-\alpha)S_4)\right), \frac{1}{2}\ln\left(1 + S_3 + S_4 + 2\sqrt{\alpha S_3 S_4}\right)] \qquad (2)$$

A similar bound holds with S_2 in place of S_1 and the roles of S_3 and S_4 reversed. These bounds are in general tighter than the data processing bound applied to the multiple access side.

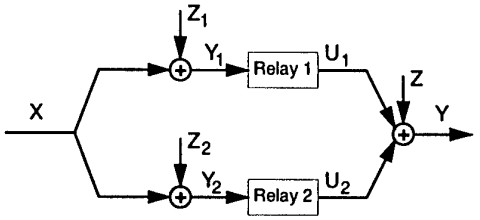


Figure 1: The Gaussian parallel relay network

III. Achievability results

We first present results for the symmetric case $S_1 = S_2$ and $S_3 = S_4$. We do this for two reasons. First, we reduce the parametrization from four SNR's to two, thus making presentation easier. Second, we highlight two fundamentally different approaches to communicating through this network.

We first consider a natural staggered block coding scheme. Both relays decode a block of observations and then transmit identical corresponding codewords (with high probability). The relays achieve perfect cooperation in this case, but the scheme is limited since each relay must decode reliably. This scheme results in reliably achievable rates up to

$$R = \frac{1}{2}\ln\left(1 + \min[S_1, 4S_3]\right). \qquad (3)$$

When $S_1 \ge 4S_3$, (3) and (2) coincide, determining capacity.

The second approach views the signals $\mathbf{Y_1}$ and $\mathbf{Y_2}$ as independent observations of the input $\mathbf{X}$. Each relay acts as a simple transponder, amplifying both signal and noise. If $\mathbf{X}$ is Gaussian, this combines the observations optimally (and the core signal component $\mathbf{X}$ coherently) before the multiaccess receiver noise $\mathbf{Z}$ is added. We can achieve rates up to

$$R = \frac{1}{2}\ln\left(1 + \frac{4S_1S_3}{1 + 2S_3 + S_1}\right). \qquad (4)$$

As the multiaccess noise power N becomes relatively small, i.e., as $\left(\frac{2S_3}{1+2S_3+S_1}\right) \to 1$, (4) and (1) coincide, and network capacity is $\frac{1}{2}\ln(1 + 2S_1)$.

Combining these approaches simultaneously is inferior to using the better of the two schemes. However, time-sharing between schemes at different values of S_1 and S_3 is beneficial. We present these results for a typical symmetric network. For an asymmetric network, coding schemes can be based on more general broadcast and multiple access approaches. We present a number of these generalizations.

IV. Conclusion

Intuition and study of the symmetric network suggest that the converses we have derived are not tight in general.

References

[1] E. Van der Meulen, "Three-terminal communication channels", *Adv. Appl. Prob.*, vol. 3, pp. 120-54, 1971.

[2] T. Cover and A. El Gamal, "Capacity theorems for the relay channel," *IEEE Trans. on Info. Th.*, vol. 25, pp. 572–84, 1979.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Static Broadcasting

Nadav Shulman and Meir Feder
Department of Electrical Engineering - Systems,
Tel-Aviv University, Tel-Aviv, 69978, ISRAEL
{shulman,meir}@eng.tau.ac.il

Abstract — **In this paper we present a different view on the broadcast channel that fits better an asynchronous setting, where each receiver can "listen" to the broadcasted data at different time intervals. In this scenario, there is a "static" fixed amount of data, that needs to be transmitted to all receivers. Each receiver wants to minimize the receiving time, and this way get the static data at the highest possible rate.**

I. Concept Definition

In this work we define and analyze *static broadcasting*. In this broadcasting scenario, the sender has only a fixed common information to transmit to all receivers. We suggest the following definition of the rate - the number of reliably received bits divided by the number of symbols the receiver has *used* to retrieve these bits (or, divided by the information gathering time). Under this definition, in principle, a receiver that listen through a better channel, may gather less channel symbols in order to estimate the transmitted message, and by this to increase its rate. In the saved time it can fetch more information from other transmitters. The term *static broadcasting* comes from the notion that the information the transmitter sends is fixed, static, and the same for all receivers.

In this work, a broadcast channel is composed of single transmitter and d memoryless channels W_i, $1 \le i \le d$, with common input alphabet through which the transmitter broadcasts to d receivers. The capacity region is defined as the closure of the set of all possible achievable rates. A rate $(R_1, R_2, \ldots, R_d)$ is said to be achievable if for any $\epsilon > 0$ there exists a code with M words such that for all i, the ith receiver can decode, with error probability smaller than ϵ, the codeword using the first $\lfloor \log M/R_i \rfloor$ channel symbols. The achievable rate region is given by the following theorem.

Theorem 1 *$(R_1, R_2, \ldots, R_d)$ is in the capacity region iff, for any $\delta \ge 0$ there exist input priors $P_1, P_2, \ldots$ and a number K such that $\frac{1}{n_i}\sum_{t=1}^{n_i} I(P_t; W_i) \ge R_i - \delta$ for all $1 \le i \le d$, where $n_i = \lfloor \frac{K}{R_i} \rfloor$.*

In defining the capacity region for static broadcasting we utilized the possibility of transmitting the information at a higher rate if the receivers are not forced to be synchronously and simultaneously connected to the transmitter. The fact that there are various possible definitions of the capacity for the broadcast channel, depending on the subset of time the data is received, has been pointed out in, e.g., [1]. However, the setting we propose is novel.

The proposed setting was further extended in [2]. For example, in [2] there is a setting where the receivers start receiving at different arbitrary times, which may fit an IP Multicast scenario. Another extension corresponds to data transmission over an unknown channel, using infinitely long codes (to allow a channel with unbounded small capacity). Finally, universal and sequential decoding schemes were investigated.

II. Examples of the Capacity Region

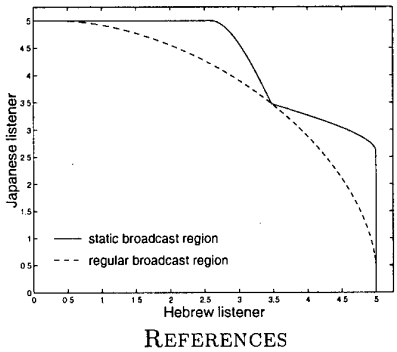
A general method to find the capacity region for static-broadcasting to 2 channels, is as follows. Assume the channels conditional probabilities are $W_1(y|x), W_2(y|x)$ and the corresponding capacities are C_1, C_2. Using the convexity of the mutual information, we may assume that the input prior to the channel is changed only at time points of the form $t = n_i + 1$. Hence, in the case of 2 receivers, we start with prior P and after one of the receivers got all the information, it will quit, and in order to maximize the rate to the second receiver, we shall change the input prior to the one that achieves its capacity. Assuming $I(P; W_1) \ge I(P; W_2)$. Then,

$$R_1 = I(P; W_1), \quad R_2 = \frac{I(P; W_1)C_2}{C_2 + I(P; W_1) - I(P; W_2)}.$$

Of course, any point $r_1 \le R_1, r_2 \le R_2$ is in the capacity region. To get the complete capacity region we should take the union of the region above over all possible values of the initial input prior, P.

In case where the capacity achieving prior is the same for all channels we can achieve simultaneously their point-to-point capacity. For example, two binary symmetric channels noisy and noiseless. In that case a simple code can be shown. Take any good systematic code for the noisy channel. The systematic part (the information bits are the prefix of each codeword) is sufficient, of course, for the noiseless channel and impose an effective rate of 1 for that channel. The noisy channel receives the information at a rate determined by the code.

In static broadcasting, unlike regular broadcasting, time sharing between two strategies is not a valid strategy. Hence, the capacity region is not necessarily convex. For example, suppose one communicates using 31 Japanese words and 31 Hebrew words. A Japanese listener can differentiate 32 different symbols (since all Hebrew words sound the same to him) and the same goes to a Hebrew listener. This broadcast channel leads to the capacity region in the figure below.



References

[1] Thomas M. Cover. Comment on broadcast channels. *IEEE Trans. on Inform. Theory*, IT-44:pp.2524–2530, October 1998.

[2] Nadav Shulman. *Communication in Unknown Channels*. PhD thesis, Tel-Aviv University, in preparation.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Achievable Distortion Regions of Gaussian Broadcast Systems

Udar Mittal
Human Interface Lab
Motorola Labs
Schaumburg, IL 60195
mittal@ccrl.mot.com

Nam Phamdo
Electrical & Computer Engineering
State University of New York
Stony Brook, NY 11794-2350
phamdo@ece.sunysb.edu

I. Introduction

We consider the problem of broadcasting a bandlimited white Gaussian source on an additive bandlimited white Gaussian noise channel with two receivers. Several hybrid digital-analog joint source-channel codes are proposed. The design principle is based on bandwidth/power splitting and matched tandem coding. The distortion regions of these codes are presented.

II. Problem Statement

Consider a memoryless Gaussian source, $\{x_i\}_{i=1}^{\infty}$, with zero mean and variance σ^2. The source is to be encoded and transmitted over a broadcast AWGN channel modeled by $Z_k = Y + V_k$, where Y is the channel input, Z_k and V_k are channel output and noise for the k-th user, $k = 1, 2$. We assume that Z_k, Y, and V_k are all m-dimensional, $E[||Y||^2] \leq mP$, the components of V_k are i.i.d. with zero mean and variance N_k, $k = 1, 2$, and $0 < N_1 < N_2$.

An n-dimensional encoder, α_n, is a mapping of an n-dimensional source vector X to an m-dimensional channel input vector Y. Here, $\rho = m/n$ is the bandwidth expansion factor (or the rate of the system in number of channel uses per source sample). We assume that ρ is fixed while m and n grow large. The decoder, $\beta_{n,k}$, for user k is a mapping of an m-dimensional vector Z_k to an n-dimensional vector $\hat{X}_k$. Let $D(N_k) \triangleq D(\alpha_n, \beta_{n,k}, N_k)$ be the mean-square distortion between X and $\hat{X}_k$. Shannon's capacity-rate-distortion limit dictates that

$$D(N_k) \geq \frac{\sigma^2}{(1 + P/N_k)^{\rho}}, \qquad k = 1, 2. \tag{1}$$

We are interested in the set of all possible pair $(D(N_1), D(N_2))$.

III. Achievable Distortion Region

A pair (d_1, d_2) is an *achievable distortion point* if there exists an encoder sequence $\{\alpha_n\}$ and decoder sequences $\{\beta_{n,1}, \beta_{n,2}\}$ such that α_n satisfies the power constraint and $\lim_{n\to\infty} D(\alpha_n, \beta_{n,k}, N_k) = d_k$ for $k = 1, 2$. The *achievable distortion region* is the collection of achievable distortion points [1].

IV. Main Results

Several hybrid-digital analog joint source-channel coding systems are proposed. Details of these systems can be found in [2]. Fig. 1 shows the encoder for one of these systems (Hybrid 3). This is valid for $\rho > 1$ (bandwidth expansion). For $\rho < 1$ (bandwidth compression), a dual of this system can be used [2]. In Fig. 1, the "Linear Encoder" corresponds to the analog part of the system. The performance of Hybrid 3 is shown in Fig. 2. Here, $\rho = 2$, $10\log_{10} P/N_1 = 20$ dB, and $10\log_{10} P/N_2 = 0$ dB. Points A and C correspond to traditional digital coding systems optimized for noise N_1 and N_2, respectively. The "Time-Sharing" dash-dot curve is the time-sharing between these two systems (in linear scale, it is a straight line between A and C). The "Digital" dash-dot curve is a purely digital system presented in [3]. Fig. 2 shows that Hybrid 3 is superior to both "Digital" and "Time-Sharing" systems. The result shows that the region above and to the right of the heavy solid line is achievable.

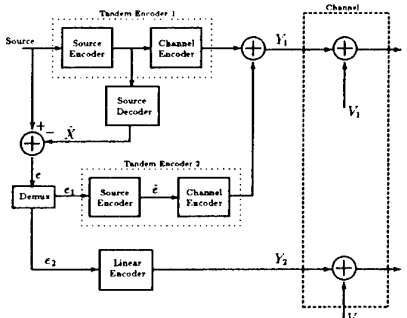


Figure 1: Encoder of Hybrid Digital-Analog System For $\rho > 1$ (Hybrid 3).

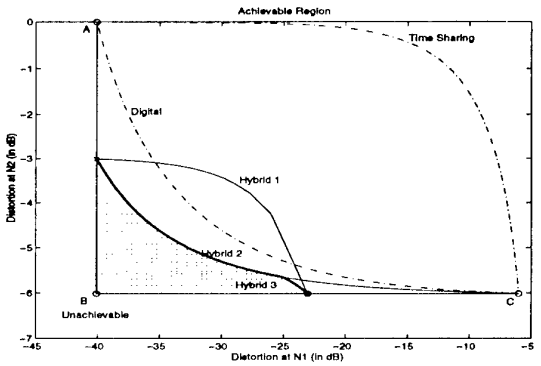


Figure 2: Distortion Performances of Hybrid Digital-Analog Systems.

References

[1] Z. Reznic, R. Zamir and M. Feder, "Joint source-channel coding of a Gaussian mixture source over the Gaussian broadcast channel," *Thirty-Sixth, Allerton Conference on Communication, Control, and Computing*, Oct. 1998.

[2] U. Mittal, "Broadcasting, robustness and duality in a joint source-channel coding system," *Ph.D. Dissertation*, Department of Electrical and Computer Engineering, SUNY at Stony Brook, 1999.

[3] M. Trott, "Unequal error protection codes: Theory and practice," *IEEE Information Theory Workshop*, Haifa, Israel, pp. 11, June 1996,

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Limits of Information, Markov Chains, and Projection

Andrew R. Barron
Yale University, Statistics Dept.
Box 208290, New Haven, CT 06520
e-mail: Andrew.Barron@yale.edu

Abstract — **The chain rule of information shows that log densities form Cauchy sequences, convergent in L_1, proving information limits, Markov chain convergence, and existence of information projections.**

Let $D(P||Q) = E_P \log p(X)/q(X)$, $A = E|\log p(X)/q(X)|$, and $V = \int |p-q|$ be the information divergence, absolute information divergence, and total variation distance between probability measures P and Q with density functions p, q with respect to a dominating measure on a measurable space. The chain rule and the Pinsker-type inequality $A \leq D + \sqrt{2D}$, deduced from $V \leq \sqrt{2D}$ (which implies that if D tends to zero then so does V and A) allow one to deduce in various settings that log densities provide Cauchy sequences convergent in L_1, thereby establishing information limits including Markov chain convergence and information projections.

I. Markov chains

Let $\{X_n\}$ be Markov with stationary transition probability on a general state space and let P_n be the distribution of X_n.

Theorem 1. *Markov Chain Convergence.* If $\{X_n\}$ is a reversible Markov chain with a unique invariant probability distribution P^*, then $\lim D(P_n||P^*) = 0$ if and only if the sequence $D(P_n||P^*)$ is eventually finite.

Proof: Let $D_n = D(P_n||P^*)$. The chain rule gives $D_m - D_n$, for $n > m$, as a divergence (between conditional distributions for X_m given X_n), establishing monotonicity and convergence of D_n, so that $D_m - D_n \to 0$ as $n, m \to \infty$, and thus via the Pinsker-type inequality $E|\log p_m(X_m)/p^*(X_m) - \log p_n(X_n)/p^*(X_n)| \to 0$, so that $\log p_n(X_n)/p^*(X_n)$ is a Cauchy sequence, convergent in L_1. Fritz [4] used information inequalities for reversible chains to show the total variation convergence of P_n to P^*, so that $p^*(X_n)/p_n(X_n)$ converges to 1 in probability. Thus $\log p_n(X_n)/p^*(X_n)$, which we have shown to be convergent in L_1, must have L_1 limit equal to 0.

II. Information Limits

Let $\mathcal{F}_n$ be a monotone sequence of sigma-fields with limit $\mathcal{F}_\infty$. Let P_n and Q_n denote the restrictions of P and Q to $\mathcal{F}_n$, let ρ_n be the density of P_n with respect to Q_n, and let $D_n = D(P_n||Q_n)$ for $n = 1, 2, \ldots, \infty$.

Theorem 2. *Information Limit.* If $\mathcal{F}_n$ is decreasing or if $\mathcal{F}_n$ is increasing and $D(P_n||Q_n)$ is bounded, then $\log \rho_n \to \log \rho_\infty$ in $L_1(P)$ and $\lim_n D(P_n||Q_n) = D(P_\infty||Q_\infty)$.

Proof: In the case that $\mathcal{F}_n$ is decreasing, for $n > m$ we have $D_m - D_n = \int \rho_m \log \rho_m/\rho_n dQ$ establishing monotonicity, convergence, and, hence, the Cauchy sequence property, so that, via the Pinsker-type inequalities, both $\int |\rho_m - \rho_n| dQ$ and $E|\log \rho_m - \log \rho_n|$ tend to 0 as $n, m \to \infty$. Hence ρ_n is convergent in $L_1(Q)$ (denote the limit ρ_∞) and $\log \rho_n$ is convergent in $L_1(P)$ with limit $\log \rho_\infty$. Sets A in $\mathcal{F}_\infty$ are in $\mathcal{F}_n$ for all n with $P(A) = \int_A \rho_n dQ$, so by $L_1(Q)$ convergence, $P(A) = \int_A \rho_\infty dQ$, that is, the limit ρ_∞ is indeed the density between the restrictions of P and Q to $\mathcal{F}_\infty$. For the increasing case one proceeds in the same manner using the chain rule to extract Cauchy convergence of ρ_n in $L_1(Q)$ and $\log \rho_n$ in $L_1(P)$ and to identify the limit.

Theorem 2 implies Theorem 1 using the decreasing $\mathcal{F}_n$ generated by $\{X_n, X_{n+1}, \ldots\}$. The conclusion for the limit of increasing information is classical, see [1] and the references cited therein. Our analysis shows the convergence directly from the chain rule, without appeal to a martingale convergence theorem. The results for the limit of decreasing information and the information limit of Markov chains are new.

III. Information Projection

Demonstrating existence of information projections for convex sets of distributions uses similar techniques. Let $D(C||p)$ and $D(p||C)$ denote the infimum of $D(q||p)$ and of $D(p||q)$, respectively, over choices of q in a convex set C. The set C might not admit a minimizer and one seeks a limit q^* obtained by sequences of q_n approaching the infimum. Topsoe [7], see also [3], resolves the $D(C||p)$ case. Here we state a result for the $D(p||C)$ case developed further in the Thesis of Li [6].

Theorem 3. *Information Projection.* Let C be convex and $D(p||C)$ finite. There exists a unique q^* (possibly outside of C) such that every sequence q_n with $D(p||q_n) \to D(p||C)$ has $\log q_n \to \log q^*$ in $L_1(p)$. Thus $D(p||q^*) = D(p||C)$. For all q in C, $c_q = E_p q(X)/q^*(X) \leq 1$ and, defining the density $r = (pq/q^*)/c_q$, we have the Pythagorean-like inequality $D(p||q) \geq D(p||q^*) + D(p||r)$, where via the Pinsker-type inequality $D(p||r)$ controls the $L_1(P)$ distance between $\log q$ and $\log q^*$. Furthermore, if $\int q = 1$ for all q in C, then $\int q^* \leq 1$.

Previously, Bell and Cover [2] show characterizing properties if q^* is in C. Kieffer [5] shows if $\{\log q : q \in C\}$ is closed in $L_1(P)$, then there exists q^* satisfying the key properties.

The proof identifies a sequence q_n in C such that $D(p||q_n) \downarrow D(p||C)$ and $c_{m,n} = E q_m(X)/q_n(X) \leq 1$ for all $n > m$. With $r_{m,n} = (pq_m/q_n)/c_{m,n}$, one finds $D_m - D_n$ equals $D(p||r_{m,n}) + \log 1/c_{m,n}$, so by the Cauchy sequence property, $\log 1/c_{m,n}$, $D(p||r_{m,n})$ and hence $E|\log q_m(X)/\log q_n(X)|$ converge to 0 as $n, m \to \infty$. Thus $\log q_n$ is a Cauchy sequence with limit denoted $\log q^*$ in $L_1(p)$. Further details are in [6].

References

[1] A. R. Barron. The strong ergodic theorem for densities: Generalized Shannon-McMillan-Breiman theorem. *Ann. Probab.*, vol. 13, pp. 1292-1303, 1985.

[2] R. Bell and T. M. Cover. Competitive optimality of logarithmic investment. *Math. of Oper. Res.* vol. 5, pp. 161-166, 1980.

[3] I. Csiszár. Sanov property, generalized I-projection and a conditional limit theorem. *Ann. Probab.* vol. 12, pp. 768-793, 1984.

[4] J. Fritz. An information-theoretical proof of limit theorems for reversible Markov processes. *Trans. Sixth Prague Conf. on Inform. Theory, Stat. Dec. Func., Rand. Proc.* Czech. Acad. 1973.

[5] J. Kieffer. An almost sure convergence theorem for sequences of random variables selected from log-convex sets. In *Almost everywhere convergence II*, pp. 151-166, Academic Press, 1991.

[6] J. Q. Li. Estimation of Mixture Models. Yale Thesis, 1999.

[7] F. Topsoe. Information theoretical optimization techniques. *Kybernetika* vol.15, pp. 8-27, 1979.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

The consistency of the BIC Markov order estimator

Imre Csiszár [1]
A. Rényi Insitute of Mathematics
Hung. Acad. Sci., P.O. Box 127
1364 Budapest, Hungary
e-mail: csiszar@math-inst.hu

Paul C. Shields [2]
Mathematics Department
The University of Toledo
Toledo OH 43606
paul.shields@utoledo.edu

Abstract — **We show that the BIC estimator of the order of a Markov chain (with finite alphabet) gives the correct order, eventually almost surely as the sample size goes to ∞, thereby strengthening earlier consistency results that assumed an apriori bound on the order. A key tool is a strong typicality result for Markov sample paths. We also show that the Bayesian or MDL estimator, of which the BIC estimator is regarded as an approximation, fails to be consistent for the uniformly distrubuted i.i.d. process.**

I. Main results

Given a set of cardinatlity $|A| < \infty$, denote by $\mathcal{M}_k$ the class of those probability mesures on A^∞ which are Markov of order at most k, with stationary transition probabilities. Set $\mathcal{M} = \cup_{k=0}^{\infty}\mathcal{M}_k$ where $\mathcal{M}_0$ is the i.i.d. class.

One popular approach to model selection is the so-called Bayesian Information Criterion (BIC). It suggests to estimate the Markov order by

$$\hat{k}_{\rm BIC}(x_1^n) = \arg\min_k \left(-\log \max_{P\in\mathcal{M}_k} P(x_1^n) + \frac{|A|^k(|A|-1)}{2}\log n \right) \tag{1}$$

if the observed sample is $x_1^n = (x_1, \ldots, x_n)$.

Our principal result is

Theorem 1 *For any stationary ergodic $Q \in \mathcal{M}$, $\hat{k}_{\rm BIC}(x_1^n)$ equals $k_0 = \min\{k: Q \in \mathcal{M}_k\}$, eventually almost surely.*

The hard part of the proof is to rule out "moderate overestimation" $\hat{k}_{\rm BIC}(x_1^n) \in (k^*, \alpha \log n)$, for suitable $k^* > k_0$ and $\alpha > 0$. A key tool to this is

Theorem 2 *Given a stationary ergodic $Q \in \mathcal{M}$, and $0 < \beta < 1/2$, there exists $\alpha > 0$ such that eventually almost surely, the k-block types of x_1^n, defined by*

$$\hat{P}(a_1^k \mid x_1^n) = \frac{1}{n-k+1}|\{i \in [0, n-k]: x_{i+1}^{i+k} = a_1^k\}|, \quad a_1^k \in A^k$$

satisfy for all $k \le \alpha \log n$

$$|\hat{P}(a_1^k \mid x_1^n) - Q(a_1^k)| \le n^{-\beta}Q(a_1^k), \quad a_1^k \in A^k. \tag{2}$$

Theorem 2 permits us to restrict attention to "typical sequences" satisfying (2); for these, the number of possible k-block types does not grow too fast as $n \to \infty$, and the method of types leads to suitable probability bounds.

We also consider the Bayesian order estimator

$$\hat{k}_{\rm KT}(x_1^n) = \arg\min_k\{-\log p_k - \log {\rm KT}_k(x_1^n)\} \tag{3}$$

which is also a minimum description length (MDL) estimator, see [1]. Here p_k is a prior probability assigned to the class $\mathcal{M}_k$, and ${\rm KT}_k$ is the Krichevsky-Trofimov distribution of order k, a Dirichlet mixture of measures in $\mathcal{M}_k$. The expression minimized in (1) is a good approximation to $-\log {\rm KT}_k(x_1^n)$ when k is fixed, but substantially overestimates the latter when k grows with n, a fact we use in the proof of Theorem 1 to rule out "gross overestimation" $\hat{k}_{\rm BIC}(x_1^n) \ge \alpha \log n$.

Theorem 3 *The estimator (3) is not consistent for the i.i.d. process with uniform distribution on A, if p_k decreases subexponentially as $k \to \infty$. Rather, in this case $\hat{k}_{\rm KT}(x_1^n) \to \infty$ almost surely.*

The proof depends on the fact that for large k it is likely that no k-block appears more than once in x_1^n, and then ${\rm KT}_k(x_1^n) = |A|^{-n}$.

II. Discussion

The key feature of our consistency result Theorem 1 is that the minimization for k in eq. (1) is unrestricted. When a prior bound k^* on the true order is known, and the minimization is retricted to $k \le k^*$, consistency has been proved by Finesso [2]. Kieffer [4] proved consistency without such restriction, for a modified estimator with a larger penalty term; he also raised the question whether the BIC estimator (1) was consistent.

Theorem 2 appears to be the first strong typicality result for non-i.i.d. processes that admits block size growth of order $\log n$; see, however, Flajolet et al. [3] for coin-tossing.

Bayesian inconsistency phenomena similar to Theorem 3 are well-known in Statistics though in less natural settings than ours. Theorem 3 gives a natural example when in the theorem about MDL consistency for almost every choice of the parameter, see [1], "almost" is non-vacuous. The contrast of Theorems 1 and 3 suggests a deficiency in the usual interpretation of the BIC estimator as an approximation to the Bayesian or MDL estimator.

We note that the (non-Bayesian) "normalized maximum likelihood" version of MDL, see [1], is also inconsistent for the uniformly distributed i.i.d. process.

References

[1] A. Barron, J. Rissanen, and B. Yu, "The minimum description length principle in coding and modeling", *IEEE Trans. Inform. Theory*, vol. 44, pp. 2743–2760, 1998.

[2] L. Finesso, "Estimation of the order of a Markov chain", in *Recent Advances in the Mathematical Theory of Systems, Control, and Network Signals, Proc. MTNS-91*, pp. 643–645, Mita Press, 1992.

[3] P. Flajolet, P. Kirschenhofer, and R. F. Tichy, "Deviations from uniformity in random strings", *Probab. Th. Rel. Fields*, vol. 80, pp. 139–150, 1988.

[4] J. Kieffer, "Strongly consistent code-based identification and order estimation for constrained finite-state model classes", *IEEE Trans. Inform. Theory*, vol. 39, pp. 803–902, 1993.

[1]Supported in part by a joint NSF-Hungarian Academy grant 92 and by the Hungarian National Foundation for Scientific Research, Grant T26041.

[2]Supported in part by a joint NSF-Hungarian Academy grant INT-9515485.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Large Deviations of Probability Rank

Erdal Arikan
Electrical Eng. Dept.
Bilkent University
06533 Ankara, Turkey
arikan@ee.bilkent.edu.tr

Abstract — **Consider a pair of random variables (X,Y) with distribution P. The probability rank function is defined so that $G(x|y)=1$ for the most probable outcome x conditional on $Y=y$, $G(x|y)=2$ for the second most probable outcome, and so on, resolving ties between elements with equal probabilities arbitrarily. The function G was considered in [1] in the context of finding the unknown outcome of a random experiment by asking questions of the form 'Is the outcome equal to x?' sequentially until the actual outcome is determined. The primary focus in [1], and the subsequent works [2], [3], was to find tight bounds on the moments $\mathbf{E}[G(X|Y)^\theta]$. The present work is closely related to these works but focuses more directly on the large deviations properties of the probability rank function.**

I. Results

The aim of this work is to determine the large deviation exponent of $\ln G$,

$$\lim_{n\to\infty} n^{-1}\ln P[\ln G(X^n|Y^n) > nL], \tag{1}$$

for a sequence of pairs of r.v.'s (X^n,Y^n) under various assumptions regarding their distribution. Special instances of this problem correspond to finding the error exponent in source and channel coding problems of information theory. E.g., if we regard X^n as an input of length n to a noisy channel and Y^n as the channel output, $P[\ln G(X^n|Y^n) > nL]$ is the probability of decoding error for a list decoder with list size e^{nL}. We begin by noting that the mean of $\ln G$ is closely related to the Shannon entropy.

Proposition 1 *For (X,Y) a pair of jointly distributed random variables,*

$$-\ln(1+\ln M) + H(X|Y) \le \mathbf{E}[\ln G(X|Y)] \le H(X|Y) \tag{2}$$

where M is the maximum over all y of the range of X conditioned on $Y=y$.

We study large-deviations of $\ln G(X^n|Y^n)$ under the assumption that the sequence of functions

$$\varphi_n(\theta) \triangleq \frac{1}{n}\ln \mathbf{E}[G(X^n|Y^n)^\theta] \tag{3}$$

converges to a limit $\varphi(\theta)$. We let $R_{\varphi'}$ denote the range of φ'. Now, the Gärtner-Ellis theorem [4, p.15] gives

Proposition 2 *For any $L \in R_{\varphi'}$,*

$$\lim_{n\to\infty} n_{-1}\ln P[\ln G(X^n|Y^n) > nL] = \varphi(\theta_L) - \theta_L\varphi'(\theta_L) \tag{4}$$

where $\theta_L = \inf\{\theta : \varphi'(\theta) = L\}$.

For the special case where (X^n,Y^n) is a pair of random vectors with i.i.d components, we recall from [1] that for any $\theta \ge 0$

$$\lim_{n\to\infty}\varphi_n(\theta) = \varphi(\theta) = \ln\sum_y\left[\sum_x P(x,y)^{1/(1+\theta)}\right]^{1+\theta} \tag{5}$$

This yields the source coding error exponent (with side information Y^n). The well-known source coding error exponent [5, p.37] is obtained by omitting the side information term.

Another special case of interest is when X^n represents a codeword from a block code with block length n and rate R. Then, $P(x^n) = e^{-nR}$ if x^n is a codeword and 0 otherwise. This distribution is called the code's empirical distribution and denoted Q_n below. The r.v. Y^n represents the channel output when X^n is transmitted. We recall from [1] that for $\theta \ge 0$,

$$\varphi_n(\theta) = \theta R - n^{-1}E_0(\theta, Q_n) + o(n) \tag{6}$$

where E_0 is is Gallager's function [6, p. 138] and $o(n)$ is a quantity that goes to zero as n goes to infinity. Proposition 2 now yields the well-known sphere-packing bound for list-decoding.

In the case of $L=0$, which corresponds to ordinary ML decoding, Proposition 2 may not apply since 0 may not belong in $R_{\varphi'}$. In this case, Gärtner-Ellis theorem yields only a lower-bound.

Proposition 3 *Let $\{(X^n,Y^n)\}$ be a sequence of input-output pairs for a noisy channel such that $\{\varphi_n\}$ converges to a limit φ. Then,*

$$\liminf_{n\to\infty} n^{-1}\ln P[\ln G(X^n|Y^n) > 0] \ge -\theta_0\varphi'_+(\theta_0) \tag{7}$$

where $\theta_0 = \inf\{\theta : \varphi(\theta) > 0\}$ and φ'_+ denotes right-derivative.

It can be shown that this bound is equivalent to the familiar sphere-packing lower bound [6, p. 157], except it is formulated in terms of code empirical distributions.

References

[1] E. Arikan, "An inequality on guessing and its application to sequential decoding," *IEEE Trans. Inform. Theory*, vol. IT-42, no. 1, pp. 99-105, January 1996.

[2] E. Arikan and N. Merhav, "Guessing subject to distortion," *IEEE Trans. Inform. Theory*, vol. IT–44, no. 3, pp. 1041–1056, May 1998.

[3] E. Arikan and N. Merhav, "Joint source-channel coding and guessing with application to sequential decoding," *IEEE Trans. Inform. Theory*, vol. IT-44, no. 5, pp. 1756–1769, September 1998.

[4] J. A. Bucklew, *Large Deviation Techniques in Decision, Simulation, and Estimation*. New York: Wiley, 1990.

[5] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. New York: Academic, 1981.

[6] R. G. Gallager, *Information Theory and Reliable Communication*. New York: Wiley, 1968.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Information–theoretic methods in testing the goodness of fit[1]

László Györfi
Dep. of Computer Science and Information Theory
Technical Univ. of Budapest
Stoczek u. 2
H-1521 Budapest, Hungary
e-mail: gyorfi@inf.bme.hu

G. Morvai
Dep. of Computer Science and Information Theory
Technical Univ. of Budapest
Stoczek u. 2
H-1521 Budapest, Hungary
e-mail: morvai@inf.bme.hu

Igor Vajda
Institute of Information Theory and Automation
Acad. of Sciences of the Czech Rep.
Pod vodárenskou věží
CZ-182 08 Prague, Czech Rep.
e-mail: vajda@utia.cas.cz

We present a new approach to evaluating the efficiency of information-divergence-type statistics for testing the goodness of fit. Since the Pitman approach is too weak to detect sufficiently sharply the differences in efficiency of these statistics, the attention is focused on the Bahadur efficiency.

We consider the classical statistical model of goodness of fit with independent data $(X_i : i \in N)$ where, under a hypothesis H, X_i is distributed by μ on an abstract space $(\mathcal{X}, \mathcal{A})$ and, under an alternative A, it is distributed by $\nu \neq \mu$. In addition to μ and ν, we consider the standard empirical distribution $\widehat{\mu}_n = (\delta_{X_1} + \cdots \delta_{X_n})/n$ on $(\mathcal{X}, \mathcal{A})$ and the infinite product distributions

$$P = \mu^N, \quad Q = \nu^N \quad \text{on } (\mathcal{X}^N, \mathcal{A}^N).$$

We also consider partitions $\mathcal{P}_n = \{A_{n1}, \ldots, A_{nm_n}\} \subset \mathcal{A}$ of $\mathcal{X}$ with $m_n \uparrow \infty$ and the discrete stochastic m_n-vectors $\boldsymbol{p}_n = (p_{nj})$, $\boldsymbol{q}_n = (q_{nj})$ and $\widehat{\boldsymbol{p}}_n = (\widehat{p}_{nj})$ generated by these partitions and the distributions μ, ν and $\widehat{\mu}_n$. We are interested in the statistics

$$T_{\phi,n} = D_\phi(\widehat{\boldsymbol{p}}_n; \boldsymbol{p}_n)$$

which are the ϕ-divergences of Csiszár for convex $\phi(t)$, $t \geq 0$. Particular attention is paid to the information divergence (ID) statistic $I(\widehat{\boldsymbol{p}}_n; \boldsymbol{p}_n)$ and the reversed ID statistic $I(\boldsymbol{p}_n; \widehat{\boldsymbol{p}}_n)$, and to the classical Pearson statistic $\chi^2(\widehat{\boldsymbol{p}}_n; \boldsymbol{p}_n)$ and the reversed Pearson (Neyman) statistic $\chi^2(\boldsymbol{p}_n; \widehat{\boldsymbol{p}}_n)$.

Our results are formulated for nonatomic μ and ν, under relatively milde restrictions on the partitions $\mathcal{P}_n$. These restrictions are fulfilled e. g. when $p_{nj} = 1/m_n$, the likelihood ratios p_{nj}/q_{nj} are bounded, and the partitions are nested in the sense $\mathcal{P}_1 \subset \mathcal{P}_2 \subset \ldots$ and generate the σ-algebra $\mathcal{A}$. Moreover, we consider restrictions on m_n of the type

$$\lim_{n\to\infty} \frac{m_n\, c_n}{n} = 0 \tag{1}$$

for nondecreasing sequences $c_n > 0$.

Our main result is the formula

$$B(\phi_1/\phi_2) = \frac{g_{\phi_1}(D_{\phi_1}(\nu;\mu))}{g_{\phi_2}(D_{\phi_2}(\nu;\mu))} \cdot \lim_{n\to\infty} \frac{s_{\phi_2,n}}{s_{\phi_1,n}} \tag{2}$$

for the *Bahadur relative efficiency* of the test rejecting H when $T_{\phi_1,n} > c_{\phi_1,n}$ with respect that rejecting when $T_{\phi_2,n} > c_{\phi_2,n}$. Here, for $\phi = \phi_1$ and $\phi = \phi_2$, $D_\phi(\nu;\mu)$ is the ϕ-divergence of distributions ν and μ and $g_\phi(\varepsilon)$ for $\varepsilon > 0$ is the exponent in the well known information-theoretic formula for large deviation of the "types" $\widehat{\boldsymbol{p}}_n$ in a discrete source of m_n letters distributed by $\boldsymbol{p}_n$, where

$$g_\phi(\varepsilon) = \lim_{n\to\infty} \left(s_{\phi,n} \left[\inf_{\widehat{\boldsymbol{p}}_n :\, T_{\phi,n} \geq \varepsilon} I(\widehat{\boldsymbol{p}}_n; \boldsymbol{p}_n) \right] \right), \tag{3}$$

cf. Problem 1.2.11 in [2]. In (3), $s_{\phi,n} > 0$ is an appropriate norming sequence leading to finite $g_\phi(\varepsilon)$.

The definition (2) exploits the approach developed in [3] and the formula (3) has been first proposed in [1]. Obviously, (2) is applicable only when the limits in (2) and (3) exist, but (2) also assumes that

$$\lim_{n\to\infty} \boldsymbol{E}_P\, T_{\phi,n} = 0 \quad \text{and} \quad \lim_{n\to\infty} T_{\phi,n} = D_\phi(\nu;\mu) \quad Q\text{-a. s.} \tag{4}$$

and that m_n satisfies (1) with $c_n = s_{\phi,n} \ln n$.

We have proved that (4) follows from (1) with $c_n = m_n^4 \ln n$ for $T_{\phi,n}$ equal to $I(\widehat{\boldsymbol{p}}_n; \boldsymbol{p}_n)$ and $\chi^2(\widehat{\boldsymbol{p}}_n; \boldsymbol{p}_n)$. On the other hand, the first of the conditions (4) cannot hold for $T_{\phi,n}$ equal to $I(\boldsymbol{p}_n; \widehat{\boldsymbol{p}}_n)$ and $\chi^2(\boldsymbol{p}_n; \widehat{\boldsymbol{p}}_n)$. We found that for their robustified versions $I(\boldsymbol{p}_n; \alpha_n \boldsymbol{p}_n + (1-\alpha_n)\widehat{\boldsymbol{p}}_n)$ and $\chi^2(\boldsymbol{p}_n; \alpha_n \boldsymbol{p}_n + (1-\alpha_n)\widehat{\boldsymbol{p}}_n)$ with $\alpha_n \downarrow 0$ both conditions (4) hold and the original nonrobustified function $g_\phi(\varepsilon)$ obtained from (3) remains valid. The sequences $s_{\phi,n}$ and the functions $g_\phi(\varepsilon)$ for the above mentioned statistics are presented in the Table, together with $B(\phi_1/\phi_2)$'s for the statistic T_{ϕ_2} in the line and T_{ϕ_1} in the preceeding line. From [3] it is known that $B(\phi_1/\phi_2) = 0$ for $T_{\phi_1,n} = \chi^2(\widehat{\boldsymbol{p}}_n; \boldsymbol{p}_n)$ and $T_{\phi_2} = I(\widehat{\boldsymbol{p}}_n; \boldsymbol{p}_n)$, i. e. that the ID test is infinitely more Bahadur efficient then the classical Pearson test. The remaining results of the Table seem to be new. They are negative for the reversed versions of the two formerly mentioned statistics.

$T_{\phi,n}$	$s_{\phi,n}$	$g_\phi(\varepsilon)$	$B(\phi_1/\phi_2)$
$\chi^2(\boldsymbol{p}_n; \alpha_n \boldsymbol{p}_n + (1-\alpha_n)\widehat{\boldsymbol{p}}_n)$	m_n	1	
$I(\boldsymbol{p}_n; \alpha_n \boldsymbol{p}_n + (1-\alpha_n)\widehat{\boldsymbol{p}}_n)$	m_n	1	1
$\chi^2(\widehat{\boldsymbol{p}}_n; \boldsymbol{p}_n)$	$\frac{\sqrt{m_n}}{\ln m_n}$	$\frac{\sqrt{\varepsilon}}{2}$	0
$I(\widehat{\boldsymbol{p}}_n; \boldsymbol{p}_n)$	1	ε	0

References

[1] J. Beirlant, L. Devroye, L. Györfi and I. Vajda, "Large deviations of divergence measures on partitions," *J. of Statist. Planning and Inference* (submitted 1999).

[2] I. Csiszár and J. Körner, "*Information Theory: Coding Theorems for Memoryless Systems*," Academic Press, New York 1981.

[3] D. Quine and J. Robinson, "Efficiencies of chi-square and likelihood ratio goodness–of–fit tests," *Annals of Statistics 13*, 727–742, 1985.

[1]Supported by the GA CR grant 102/99/1137.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Decomposable Codes Based on Two-Dimensional Array Codes

Xiao-Hong Peng
School of EEIE
South Bank University
London SE1 0AA, UK
pengx@sbu.ac.uk

P. G. Farrell
Communication Research Centre
Lancaster University
Lancaster LA1 4YR, UK
p.g.farrell@lancaster.ac.uk

Abstract: ***In this paper, we will present a construction method for obtaining the decomposable codes that are originated from two-dimensional array codes and of the form*** $|a_1+x|\cdots|a_m+x|a_1+\cdots+a_m+x+y|$ ***. Many best known codes can be constructed using this method.***

I. INTRODUCTION

Codes constructed by combining shorter or simpler codes are decomposable and can be decoded with reduced complexity. A new class of decomposable codes presented in this paper is created on the basis of two-dimensional array codes which themselves are decomposable. The construction of the codes, in a form of $|a_1+x|\cdots|a_m+x|a_1+\cdots+a_m+x+y|$, embraces many existing code structures. This is not just an extension of the existing code construction, but also an opportunity for finding more good codes or constructing the best known codes [3] in a simpler way. Also, because of the use of array codes, their trellis structure and efficient soft-decision decoding algorithm will play a major role in the trellis decoding of the decomposable codes created.

II. CODE CONSTRUCTION

A simple example of two-dimensional array codes is the product code. A product code C is formed by a direct product of two component codes $C_1=(n_1,k_1,d_1)$ and $C_2=(n_2,k_2,d_2)$, so it is a decomposable code. The generator matrix, G, of C is represented in the form of a *Kronecker product* of generator matrices of its component codes, G_1 and G_2,

i.e.: $G=G_1\otimes G_2=\left(g_{i,j}^{(1)}G_2\right)$ or $G=G_2\otimes G_1=\left(g_{i,j}^{(2)}G_1\right)$

where $G_1=\left(g_{i,j}^{(1)}\right), G_2=\left(g_{i,j}^{(2)}\right)$. The new decomposable code C' is constructed by using the generator matrix

$$G'=\begin{pmatrix} G_1 & & G_1 \\ & \ddots & \vdots \\ & G_1 & G_1 \\ G_A & \cdots\ \cdots & G_A \\ & & G_B \end{pmatrix} \qquad (1)$$

where G_A and G_B are the generator matrixes of component codes $C_A=(n_1,k_A,d_A)$ and $C_B=(n_1,k_B,d_B)$ respectively. Code C' is therefore referred as a $|a_1+x|\cdots|a_m+x|a_1+\cdots+a_m+x+y|$-construction code. with $a_1,\cdots,a_m\in C_1, x\in C_A$ and $y\in C_B$. This construction can be viewed as the squaring construction [1] when m=2, x=0 and y=0, and the Turyn [2] or cubing cons truction [1] when m=2and y=0, i.e. in a form of $|a+x|b+x|a+b+x|$.

To optimize a given code, we need to fix any two of the three code parameters, length n, dimension k and minimum distance d, and to improve the third one. In our case, for example, the two component codes G_A and G_B are used to augment the product code C in such a way where the length and minimum distance of the decomposable code C' are kept the same as code C, and the dimension of the code C' is greater than that of code C. This means that $n'=n$, $d'=d$ and $k'>k$. To this end, we set up criteria for selecting G_A and G_B, as follows:

The conditions for choosing G_A and G_B such that the augmented code, C', has the same minimum distance as C, i.e., $d'=d$, are set up for the following cases:

1. When $G_A\neq\mathbf{0}$, $G_B=\mathbf{0}$. $\begin{cases} d_A\geq d/n_2 \\ d_{\cup A}\geq d/n_2 \end{cases}$

2. When $G_A=\mathbf{0}$, $G_B\neq\mathbf{0}$. $d_B\geq d$

3. When $G_A\neq\mathbf{0}$, $G_B\neq\mathbf{0}$. $\begin{cases} d_A\geq d/n_2 \\ d_{\cup A}\geq d/n_2 \\ d_B\geq d \\ d_{\cup AB}\geq d/n_2 \end{cases}$

where $d_{\cup A}$ and $d_{\cup AB}$ are the minimum distances of the union codes $C_1\cup C_A$ and $C_1\cup C_A\cup C_B$, respectively.

An efficient search algorithm for optimum decomposable codes can be designed by setting the dimension-improving target according to the table of the best known codes [3], and letting C_1 be as small as possible. The use of small C_1 may require large number of component codes, but reduce the complexity of the search algorithm.

REFERENCES

[1] G.D. Forney Jr, Coset codes II: Binary lattices and related codes," IEEE Trans. Inform. Theory, vol. IT-34, pp.1152-1187, Sept. 1988.

[2] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, Amsterdam: North-Holland Mathematical Library, 1977.

[3] A.E. Brouwer and T. Erhoeff, "An update table of minimum-distance bounds for binary linear codes," IEEE Trans. Inform. Theory, vol. IT-39, pp.662-677, March 1993.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Bases of Rectangular Codes

Vladimir Sidorenko [1]
Institute for Information
Transmission Problems,
Russian Academy of Science
e-mail: sid@iitp.ru

Johannes Maucher
Ascom Systec AG
Applicaple Research & Technology
Switzerland
johannes.maucher@ascom.ch

Martin Bossert
Communication Eng. Dept.,
University of Ulm, Germany
e-mail:
boss@it.e-technik.uni-ulm.de

Abstract — **We investigate general properties of rectangular codes. The class of rectangular codes includes all linear, group, and many non-group codes. We define a basis of a rectangular code. This basis gives a universal description of a rectangular code. The rectangular algebra is defined. We show that all bases of a length-2 rectangular code have the same cardinality. Bounds on cardinality of a basis of a rectangular code are given. We present a simple procedure to get rectangular basis of a linear code from its generator matrix.**

A block code C is a set of words $c = (c_1, \dots c_n)$ of length n over an alphabet $Q = \{0, 1, \dots, q-1\}$. Given $t \in [1, n-1]$, split every codeword c into the *past* $p = (c_1, \dots c_t)$ and the *future* $f = (c_{t+1}, \dots, c_n)$, i.e., $c = pf$. A set $C \subset Q^n$ is called *t-rectangular* if the following implication is true [1] (in [2] such a set was called t-separable):

$$p_1 f_1, \quad p_1 f_2, \quad p_2 f_1 \in C \quad \rightarrow \quad p_2 f_2 \in C. \quad (1)$$

A set $C \subset Q^n$ is called *rectangular* if it is *t-rectangular* for each t.

All group, linear, and many famous nonlinear codes are rectangular. Rectangular codes have the following nice property. The minimal trellis of a rectangular code is unique, biproper, and minimizes a number of complexity measures including the Viterbi (or APP) decoding complexity. In addition, the minimal code trellis gives a universal compact representation of a rectangular code. We present another universal compact description of a rectangular code using a suggested idea of rectangular basis.

Given an arbitrary block code G, a rectangular set that includes G and has the minimum cardinality is called *a rectangular closure* of G and is denoted by $[G]$. A rectangular closure $[G]$ is unique. We say that a set G *generates* a rectangular set C (G is *a generating set* for C) if $[G] = C$. A set G is called *independent* if for any $g \in G$ $g \notin [G \setminus g]$. An independent set B generating a rectangular set C is called *a basis of the rectangular set* C. It is known [3] how to get a basis of a rectangular set and how to get the rectangular set from its basis.

1. *Rectangular Algebra.* We define over the set Q^n of words a ternary partial operation of *rectangular complement.* The set of words with this operation is called *rectangular algebra.* A rectangular code is a rectangular subalgebra. This allows us to use results of algebra. On the other hand the rectangular algebra is an interesting example of universal algebra.

The following theorem gives an upper bound on cardinality of the rectangular closure of the set G.

Theorem 1 $|[G]| \leq 2^{|G|-1}$.

An important question for any universal algebra is: "Have bases of a closed set the same cardinality?".

Conjecture 2 *All bases of a rectangular code have the same number of words.*

We show that Conjecture 2 is true for codes of length 2.

2. *Bounds on Cardinality of a Basis.* From Theorem 1 we get

Theorem 3 *Cardinality of a basis $B(C)$ of a binary rectangular code C is bounded by*

$$\log_2 |C| + 1 \leq |B(C)| \leq |C|.$$

4. *Rectangular basis of a linear code.* We present a simple procedure to get rectangular basis of a linear code from generator matrix of the code. This basis can be used as follows. Assume that a nonlinear rectangular code C is a union of cosets of a linear code L. Using the proposed procedure we obtain a basis $B(L)$ of the linear code L. A basis of a coset $L + a$ is $B(L) + a$. So, we can construct a generating set for C as union of bases of the cosets of L.

[1]The work was supported by Russian Fundamental Research Foundation (project No 99-01-00840) and by Deutsche Forschungs Gemeinschaft.

References

[1] F. R. Kschischang, "The trellis structure of maximal fixed-cost codes," *IEEE Trans. Inform. Theory,* vol. 42, pt. I, pp. 1828 - 1838, Nov. 1996.

[2] V. Sidorenko, "The Euler characteristic of the minimal code trellis is maximum," *Problems of Inform. Transm.* vol. 33, no. 1, pp. 87-93, January-March 1997.

[3] V. Sidorenko, J. Maucher, and M. Bossert, "On the theory of rectangular codes," in *Proc. of 6th Intern. Workshop on Algebraic and Combinatorial Coding theory,* Pskov, Russia, pp.207-210, Sept. 1998.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Cocyclic Hadamard Codes from Semifields

P. Udaya[1]
Department of Computer Science,
University of Melbourne,
Parkville, Vic., 3052
Melbourne, AUSTRALIA
e-mail: udaya@cs.mu.oz.au

K. Horadam
Department of Mathematics,
RMIT University,
GPO Box 2476V, VIC. 3001.
Melbourne, Australia.
e-mail: horadam@rmit.edu.au

Abstract — **We construct new cocyclic generalised Hadamard matrices using semifield multiplication. The matrices used are constructed from cocycles defined over elementary abelian groups. These constructions naturally yield generalised Hadamard codes meeting the Plotkin bound.**

I. Introduction

Non-binary Hadamard codes meeting the Plotkin bound can be constructed using generalized Hadamard matrices [1]. In this paper we construct families of cocyclic generalized Hadamard matrix codes meeting the Plotkin bound from cocycles defined from finite fields $\mathrm{GF}(p^m)$, commutative semifields such as Dickson semifields and non-commutative semifields of order 16.

II. Cocycles

Let G be a finite group of order v and C be a finite abelian group of order w where w divides v ($w|v$). A cocycle is a mapping $\psi : G \times G \to C$, satisfying the following cocycle equation $\psi(g,h)\psi(gh,k) = \psi(g,hk)\psi(h,k)$, for all $g,h,k \in G$. This implies $\psi(g,1) = \psi(1,h) = \psi(1,1)$, for all $g,h \in G$. We only consider normalized cocycles, for which $\psi(1,1) = 1$.

A cocycle associated with the groups G and C is naturally represented as a square matrix of order $v \times v$, whose rows and columns are indexed by the elements of the group G under some fixed ordering and whose entry in position (g,h) is $\psi(g,h)$. We call such matrices G-cocyclic matrices. We represent a G-cocyclic matrix as $M_\psi = [\psi(g,h)]_{g,h\in G}$. If the cocycle ψ is symmetric then M_ψ is a symmetric matrix.

Definition 1 *When $w|v$, the cocycle $\psi : G \times G \to C$ is orthogonal if the non-initial rows of M_ψ are uniformly distributed over the elements of C. That is, for each $g \neq 1 \in G$, $|\{h \in G : \psi(g,h) = a\}| = v/w$, for all $a \in C$.*

III. Generalized Hadamard matrices and related codes

A generalized Hadamard matrix $\mathrm{GH}(w, v/w)$ over a group C is a $v \times v$ matrix with entries from the group C of order w, $w|v$, such that the list of quotients $h_{ij}h_{kj}^{-1}, 1 \leq j \leq v$, contains each element of C exactly v/w times. Let H^* be a matrix with entries $h^*_{ij} = h_{ji}^{-1}$, then the defining matrix equation over $\mathbf{Z}C$ is

$$HH^* = vI_v + (v/w)(\sum_{u\in C} u)(J_v - I_v), \qquad (1)$$

where I_v and J_v are the $v \times v$ identity matrix and matrix with all entries 1, respectively. Generalized Hadamard matrices can be used directly to construct codes meeting the Plotkin bound. We have the following result.

[1]This work was supported by Australian Research Council Large Grant #A49701206

Theorem 1 *[1, 2] Let $\Psi : G \times G \to G$ be an orthogonal cocycle, where G is the additive group of $\mathrm{GF}(p^r)$. Let M_ψ be a G-cocyclic matrix of order $p^r \times p^r$ over G,*
1. the rows of M_ψ without the first column form a $(p^r - 1, p^r, p^r - 1)$ p^r-ary code meeting the Plotkin bound.
2. the rows of the translates of $a + M_\psi$, $a \in G$, of M_ψ form a $(p^r, p^{2r}, p^r - 1)$ p^r-ary code meeting the Plotkin bound.

IV. Orthogonal Linearized Polynomial (LP) Cocyclic matrices from Semifields

Throughout this section let G be an elementary abelian group of order p^a. Here we construct classes of orthogonal cocyclic matrices using using linearized permutation polynomials (LPP) over $\mathrm{GF}(p^r)$. Let $L(x) = \sum_{i=0}^{r-1} l_i x^{p^i}$ be a LPP over $\mathrm{GF}(p^r)$, then the linearized permutation cocycle (LP cocycle) is given by $\mu_L(g,h) = L(g) \cdot h$, where $\cdot$ represents multiplication in a semifield whose additive group is G. We have a lemma.

Lemma 1 *Let $(F,+,\cdot)$ be a finite semifield such that $G = (F,+) \cong (\mathrm{GF}(p^r),+)$. If $L(x) = \sum_{i=0}^{r-1} l_i x^{p^i}$ is a LPP of $\mathrm{GF}(p^r)$, then the LP cocycle defined by $\mu_L(g,h) = L(g) \cdot h$, is orthogonal.*

The above construction with $\cdot$ as the *field* multiplication in $\mathrm{GF}(p^r)$ accounts for all (symmetric and asymmetric) orthogonal cocycles for groups of order 4,8 and 9 [2].

The first order p^a for which there exist semifields which are not fields is 16. There are two such semifields, both non-commutative. These two semifields with the above construction leads to new classes of G-cocyclic generalised Hadamard matrices of order 16.

There is a class of finite commutative semifields called the Dickson semifields, defined when p is odd and the prime-power r is even. Let F be a two-dimensional vector space over $\mathrm{GF}(p^b)$, where p is odd and $b > 1$, so $(F,+) \cong (\mathbf{Z}_p)^{2b}$. Let z be any non-square in $\mathrm{GF}(p^b)$. Each field automorphism θ of $\mathrm{GF}(p^b)$ defines a multiplication $\cdot$ on F to be $(a,b)\cdot(c,d) = (ac + zb^\theta d^\theta, bc + ad)$, which makes F a commutative semifield. The only field property which does not hold is associativity of multiplication. But this implies that the rows of the matrix M_μ for the field multiplication in $\mathrm{GF}(p^{2b})$ cannot be permuted to give the rows for the Dickson semifields, and the corresponding Hadamard codes are distinct.

References

[1] C. Mackenzie and J. Seberry. Maximal q-ary codes and Plotkin's bound. *Ars Combin.B*, 26:37–50, 1988.

[2] K.J. Horadam and P. Udaya. Cocyclic Hadamard Codes. *To appear in IEEE, Trans. on Inform. Theory*, 2000.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

New DbEC-TbED Codes Better Than the Gilbert-Varshamov Bound

Gui-Liang Feng, Xin- Wen Wu, T.R.N.Rao[1]
CACS,University of Louisiana at Lafayette ,LA 70504,USA

Abstract — **A new class of DbEC-TbED codes over GF(q) is constructed. For the cases of q=3,4, the new codes are better than the Gilbert-Varshamov bound.**

Let $r(C) = n - \log_q|C|$ be the redundancy of a linear code over $GF(q)$, $\rho(q,n,d)$ be $\min\{r(D) \mid D$ is a q-ary code of length n and minimum distance $d\}$. It is well known that the *asymptotic Hamming bound* $\rho(q,n,d) \succeq t\log_q n$ holds as $n \to \infty$, where $t = \lfloor\frac{d-1}{2}\rfloor$. The *Gilbert-Varshamov bound* admits linear (q,n,d) codes which achieve the bound $r(q,n,d) \succeq (d-2)\log_q n$ as $n \to \infty$.

In coding theory, an important problem is finding the sequences of (q,n,d) codes, asymptotically exceeding the Gilbert-Varshamov bound, i.e.,

$$r(q,n,d) \prec (d-2)\log_q n.$$

It is well-known that the single-byte error-correcting and double-byte error-detecting (SbEC-DbED) codes, i.e., the codes with minimum distances ≥ 4, have been successfully used in computer memory subsystems. We are interested in designing some good DbEC codes and DbEC-TbED codes , such that the redundancies are less than Gilbert-Varshamov bound, and as small as possible. In a previous paper [1], we constructed a class of DbEC codes over $GF(2^i)$, which have the parameters: $n = q^m, r \leq 2m + \lceil\frac{m}{3}\rceil + 1$, $m = 3,4,\cdots$. Our constructions reduce the code redundancy of [2] by one symbol.

In [2, Corollary 6], a class of DbEC-TbED codes were obtained, which have the parameters:

$$n = q^{\lfloor 5(m-1)/6\rfloor}, \quad r \leq 2.5m, \quad m = 4,6,8,\cdots.$$

Another class of DbEC-TbED codes were constructed in [2, Theorem 5], which have the parameters:

$$n = q^m, \quad r \leq \frac{5(m+1)}{2} + \lceil\frac{m}{3}\rceil + \lceil\frac{m}{4}\rceil, \quad m = 3,5,7,\cdots.$$

In this paper, we will construct a new class of DbEC-TbED codes over $GF(q)$ which have the parameters:

$$n = q^m, \quad r \leq \begin{cases} \frac{5(m+1)}{2} + \lceil\frac{m}{3}\rceil + \lceil\frac{m}{4}\rceil, & \text{when } m = 3,5,7,\cdots, \\ \frac{5m}{2} + 1 + \lceil\frac{m}{3}\rceil + \lceil\frac{m}{4}\rceil, & \text{when } m = 4,6,8,\cdots. \end{cases}$$

It is clear that $\{\lfloor\frac{5(m-1)}{6}\rfloor \mid m = 4,6,8,\cdots\} = \{3,4,5,7,9,10,12,14,\cdots\}$, and it can be verified that the integers 6, 8, 11, 13, 16, 18, 21, 23, 26, 28, $\cdots$ are not in this set. Thus, we extend the well-known constructions for $m = 6,8,16,18,\cdots$.

Construction I: Let $m > 4$ and $1,\delta,\delta^2,\cdots,\delta^{m-1}$ be a basis of $GF(q^m)$, when m is even; $1,\delta,\delta^2,\cdots,\delta^m$ be a basis of $GF(q^{m+1})$, when m is odd, respectively. Consider the sequence $H = \{f_1, f_2, \cdots\}$ of polynomials in $\mathbf{F}_q[x_1, x_2, \cdots, x_m]$, where,

(1) if m is odd, $H = \{1, x_1, \cdots, x_m, (x_1 + x_2\delta + \cdots + x_m\delta^{m-1} + 0\delta^m)^{q^{\frac{m+1}{2}-1}+1}, (x_1 + x_2\delta + \cdots + x_m\delta^{m-1} + 0\delta^m)^{q^{\frac{m+1}{2}}+1}, (x_1+x_2\beta+x_3\beta^2)^{q^2+q+1}, \cdots, (x_{3k-2}+x_{3k-1}\beta+x_{3k}\beta^2)^{q^2+q+1}, (x_1+x_2\gamma+x_3\gamma^2+x_4\gamma^3)^{q^3+q^2+q+1}, \cdots, (x_{4l-3}+x_{4l-2}\gamma+x_{4l-1}\gamma^2+x_{4l}\gamma^3)^{q^3+q^2+q+1}\}$, where $m \leq 3k$ and $m \leq 4l$, and when $i \geq m$, let $x_i = 0$;

(2) if m is even, $H = \{1, x_1, \cdots, x_m, (x_1 + x_2\delta + \cdots + x_m\delta^{m-1})^{q^{\frac{m}{2}-1}+1}, (x_1 + x_2\delta + \cdots + x_m\delta^{m-1})^{q^{\frac{m}{2}}+1}, (x_1 + x_2\beta + x_3\beta^2)^{q^2+q+1}, \cdots, (x_{3k-2} + x_{3k-1}\beta + x_{3k}\beta^2)^{q^2+q+1}, (x_1 + x_2\gamma + x_3\gamma^2 + x_4\gamma^3)^{q^3+q^2+q+1}, \cdots, (x_{4l-3} + x_{4l-2}\gamma + x_{4l-1}\gamma^2 + x_{4l}\gamma^3)^{q^3+q^2+q+1}\}$, where $m \leq 3k$ and $m \leq 4l$, and when $i \geq m$, let $x_i = 0$.

Let $LS = \mathbf{F}_q^m$ and let $\mathbf{H} = (\mathbf{f}_1, \mathbf{f}_2, \cdots)^T$ be a parity check matrix, we have a code C over $GF(q)$.

Theorem 1 *The code C in Construction I has the parameters:*

$$n = q^m, \qquad d \geq 6,$$
$$r \leq \begin{cases} \frac{5(m+1)}{2} + \lceil\frac{m}{3}\rceil + \lceil\frac{m}{4}\rceil, & \textit{when } m = 5,7,9,\cdots, \\ \frac{5m}{2} + 1 + \lceil\frac{m}{3}\rceil + \lceil\frac{m}{4}\rceil, & \textit{when } m = 6,8,10,\cdots. \end{cases}$$

For $q = 3$ and 4, these codes are better than Gilbert-Varshamov bound.

Construction II: Consider $q = 3$. Let H' be the sequences of all of the polynomials of degree ≤ 2 in H. It is clear that

$$|H'| = \begin{cases} 2.5(m+1), & \text{when } m = 3,5,7,\cdots, \\ 2.5m + 1, & \text{when } m = 4,6,8,\cdots. \end{cases}$$

Let $\mathbf{H}'$ be parity check matrices, we obtain a class of codes over $GF(3)$.

Theorem 2 *The codes in Construction II have the parameters:*

$$n = 3^m, \qquad d \geq 6,$$
$$r \leq \begin{cases} 2.5(m+1), & \textit{when } m = 3,5,7,\cdots, \\ 2.5m + 1, & \textit{when } m = 4,6,8,\cdots. \end{cases}$$

Construction III: Consider $q = 4$. Let H'' be the sequences of all of the polynomials of degree ≤ 3 in H and $\mathbf{H}''$ be parity check matrices, we obtain a class of codes over $GF(4)$.

Theorem 3 *The codes in Construction III have the parameters:*

$$n = 4^m, \qquad d \geq 6,$$
$$r \leq \begin{cases} \frac{5(m+1)}{2} + \lceil\frac{m}{3}\rceil, & \text{when } m = 3,5,7,\cdots, \\ \frac{5m}{2} + 1 + \lceil\frac{m}{3}\rceil, & \text{when } m = 4,6,8,\cdots. \end{cases}$$

[1]This work was supported in part by the National Science Foundation under Grant NCR-9804973.

References

[1] G. L. Feng, X.-W. Wu, T. R. N. Rao, "New Double-Byte Error-Correcting Codes for Memory Systems", *IEEE Trans. on Infor. Theory*, vol. IT-44, no. 3(1998), pp.1152-1163.

[2] I. I. Dumer, "Nonbinary double-error-correcting codes designed by means of algebraic varieties", *IEEE Trans. on Infor. Theory*, vol. IT-41, no. 6(1995), pp. 1657-1666.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Minimal and systematic convolutional codes over finite Abelian groups

Fabio Fagnani
Dipartimento di Matematica
Politecnico di Torino
C.so Duca degli Abruzzi, 24
I-10129 Torino, Italy
e-mail:
fagnani@calvino.polito.it

Sandro Zampieri
Dipartimento di Elettronica ed Informatica
Università di Padova
via Gradenigo, 6/a
I-35131 Padova, Italy
e-mail: zampi@dei.unipd.it

Abstract — **The classes of convolutional codes over finite Abelian groups which admit minimal encoders or systematic encoders are first characterized and then compared.**

I. Introduction

Codes over rings and groups have attracted much attention in recent years for their potential use in the phase modulation coding [1]. Here we study convolutional codes over finite Abelian groups presenting necessary and sufficient conditions under which they admit minimal or systematic encoders.

II. Convolutional codes and encoders

Given a finite Abelian group V, $\mathcal{L}_V$ is the group of Laurent sequences over V (sequences definitely equal to 0 in the past). If V and W are finite Abelian groups, any element $N(D) = \sum_{i=0}^{+\infty} N_i D^i \in \hom(W,V)[[D]]$ induces a homomorphism (*shift operator*) $N(D) : \mathcal{L}_W \to \mathcal{L}_V$ by letting act D as the forward translation. $N(D)$ is called *rational* if there exists $p(D) \in \mathbb{Z}[D]$ such that $p(D)N(D) \in \hom(W,V)[D]$. Rational shift operators are exactly those which admit a state realization with finite state space [2].

A *convolutional code* (c.c. from now on) over V is any subgroup $\mathcal{C} \subseteq \mathcal{L}_V$ for which there exists another finite Abelian group W and a rational and injective shift operator $N(D) : \mathcal{L}_W \to \mathcal{L}_V$ such that $\mathcal{C}$ coincides with the image of $N(D)$. The shift operator $N(D)$ is said to be an *encoder* for $\mathcal{C}$. A c.c. admits infinitely many encoders, but they all have, up to isomorphism, the same domain W which will be denoted by $W(\mathcal{C})$ and called the *encoding group* of $\mathcal{C}$ [2].

Let $\mathcal{C} \subseteq \mathcal{L}_V$ be a c.c and let $\mathcal{C}_-$ (resp. $\mathcal{C}_+$) be the subgroup of $\mathcal{C}$ consisting of the sequences which are 0 at $t \geq 0$ (resp. $t < 0$). Define the *input group* of $\mathcal{C}$ as $U(\mathcal{C}) := \{x \in V : \exists v \in \mathcal{C}_+,\ v(0) = x\}$, and the *state group* of $\mathcal{C}$ as the quotient group $X(\mathcal{C}) := \mathcal{C}/(\mathcal{C}_- \oplus \mathcal{C}_+)$. Let $N(D) : \mathcal{L}_{W(\mathcal{C})} \to \mathcal{L}_V$ be an encoder for $\mathcal{C}$. It can be shown [2] that $W(\mathcal{C})$ and $U(\mathcal{C})$ have the same cardinality. Moreover, $N(D)$ admits a state space realization with minimal state space $X(N)$ whose size represents the amount of memory needed to implement $N(D)$ on-line. It is a standard result that $X(N)$ cannot be smaller than $X(\mathcal{C})$.

With no loss of generality we will assume in the sequel that for any $x \in V$ there exists $v \in \mathcal{C}$ such that $v(0) = x$.

III. Minimal and systematic group behaviors

We now introduce two important classes of c.c. A c.c. $\mathcal{C} \subseteq \mathcal{L}_V$ is said to be *minimal* if it admits an encoder (called minimal) $N(D)$ such that $X(N)$ is isomorphic to $X(\mathcal{C})$. A c.c. $\mathcal{C} \subseteq \mathcal{L}_V$ is said to be *systematic* if it admits an encoder (called systematic) $N(D) : \mathcal{L}_W \to \mathcal{L}_V$ of the following type: V can be split as $V = W \oplus \tilde{V}$ and there exists $\tilde{N}(D) : \mathcal{L}_W \to \mathcal{L}_{\tilde{V}}$ such that $N(D)w = (w, \tilde{N}(D)w)$.

In the field case it is well known that any c.c. is systematic and minimal. In the group case there are examples of c.c. which are not minimal. On the other hand, it can be shown that systematic encoders are always minimal so that a systematic c.c. is always minimal. The following theorem provides a characterization of systematic c.c. which extends a result given in [1].

Theorem 1 *Let $\mathcal{C} \subseteq \mathcal{L}_V$ be a c.c.. The following conditions are equivalent.*

1. *$\mathcal{C}$ is systematic.*
2. *There exists a subgroup $\tilde{V}$ of V such that $V = U(\mathcal{C}) \oplus \tilde{V}$.*

Condition 2. can be checked in a very efficient way once we have the c.c. represented as the image of an encoder.

The relation existing between minimal and systematic c.c. is clarified by the following result. First we introduce a transformation which can be performed on a code. Fix $N \in \mathbb{N}$ and consider the map $P^N : \mathcal{L}_V \to \mathcal{L}_{V^N}$ defined by $P^N(v)(t) := v_{|[tN, tN+N-1]}$. If $\mathcal{C} \subseteq \mathcal{L}_V$ is a c.c., $\mathcal{C}^N := P^N(\mathcal{C}) \subseteq \mathcal{L}_{V^N}$ is a c.c, too.

Theorem 2 *Let $\mathcal{C} \subseteq \mathcal{L}_V$ be a c.c.. The following conditions are equivalent.*

1. *$\mathcal{C}$ is minimal.*
2. *There exists $N \in \mathbb{N}$ such that $\mathcal{C}^N$ is systematic.*

In certain situations the classes of minimal and systematic codes do coincide.

Theorem 3 *Let $\mathcal{C} \subseteq \mathcal{L}_V$ be a code and assume that $W(\mathcal{C})$ is a $\mathbb{Z}_n$-free module for some integer n. Then, the following conditions are equivalent*

1. *$\mathcal{C}$ is minimal.*
2. *$\mathcal{C}$ is systematic.*
3. *$U(\mathcal{C})$ is $\mathbb{Z}_n$-free.*

On the other hand, through computer search, we have found a minimal c.c. with $W(\mathcal{C}) = \mathbb{Z}_4 \oplus \mathbb{Z}_2$ and $V = \mathbb{Z}_4^3$, which is not systematic.

References

[1] J.L. Massey and T. Mittelholzer, "Systematicity and rotational invariance of convolutional codes over rings," *Proc. Int. Workshop on Alg. and Comb. Coding Theory*, pp. 154–158, 1990.

[2] F. Fagnani and S. Zampieri, "Convolutional codes over finite Abelian groups: some basic results," *Proc. of 1999 IMA Summer Program: Codes, Systems and Graphical Models*, Submitted for publication, 2000.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On the Design of Convolutional Codes over Block Fading Channels

Marco Chiani
CSITE, DEIS Univ. of Bologna
V.le Risorgimento, 2
I-40136 Bologna, Italy
e-mail: mchiani@deis.unibo.it

Andrea Conti
CSITE, DEIS Univ. of Bologna
V.le Risorgimento, 2
I-40136 Bologna, Italy
e-mail: aconti@deis.unibo.it

Velio Tralli
CSITE, DIF Univ. of Ferrara
Via Saragat, 1
I-44100 Ferrara, Italy
e-mail: vtralli@ing.unife.it

Abstract — **A general methodology to analyze convolutional codes over block fading channels is presented. Starting from this approach some good generator polynomials for different block fading channels are obtained.**

I. Methodology and Assumptions

We assume a block fading channel [1, 2], where the fading level is constant over B encoded bits. The number of blocks L is the available amount of diversity provided by the channel. The achievable diversity per dimension depends on the code-rate [1]. The codeword error probability (CEP) for terminated-trellis convolutional codes over block fading channel is obtained from a suitably defined matrix $\tilde{\mathbf{A}}$ that take into account the trellis structure and the interleaving function.
Let us consider, as in [3], the mxm matrix $\mathbf{A}(D)$ (where m is the number of trellis states), whose elements are $A_{ij} = D^h$ if a transition from the state i to the state j exists and produces an output with Hamming-weight h, and 0 otherwise. Assume for the sake of simplicity a rate $1/n$ code, if the fading level were constant along the codeword of $N \cdot n$ encoded bits, we would observe that:

Obs. 1 The matrix $\tilde{\mathbf{A}}(D) = \mathbf{A}^N(D)$ has elements A_{ij}^N that take into account all the transitions from state i to state j with N input bits. **Obs. 2** For zero tailing the element A_{11}^N is sufficient to obtain the code weight distribution.

For block fading channel matrix $\tilde{\mathbf{A}}$ can be generalized as a combination of matrices $\mathbf{A}(D_1, .., D_n)$ with elements $A_{ij} = D_1^{h_1} \cdot .. \cdot D_n^{h_n}$, with $h_l = 0, 1$, which means that the transition from state i to j produces the output $(h_1, ..., h_n)$. A_{ij} is equal to 0 if no transition exists from i to j.

For uninterleaved convolutional codes over block fading channel we have

$$\tilde{\mathbf{A}} = \prod_{i=1}^{L} \mathbf{A}^{N/L}(D_i, .., D_i) \tag{1}$$

where N/L is the number of transitions per block. In the case of branch-interleaving, the expression for the matrix $\tilde{\mathbf{A}}$ is

$$\tilde{\mathbf{A}} = \Big[\prod_{i=1}^{L} \mathbf{A}(D_i, .., D_i) \Big]^{N/L}. \tag{2}$$

For the bit-interleaved case the expression becomes

$$\tilde{\mathbf{A}} = \Big[\prod_{i=1}^{L/n} \mathbf{A}(D_{(i-1)n+1}, .., D_{in}) \Big]^{B}. \tag{3}$$

The element $\tilde{A}_{11}$ gives information about all sequences starting from and ending in state 0; D_l is related to the $l-th$ fading level. So,

$$\tilde{A}_{11} - 1 = T(D_1, D_2, .., D_L) = \sum_{i_1} .. \sum_{i_L} w(i_1..i_L) \cdot D_1^{i_1} \cdot .. \cdot D_L^{i_L} \tag{4}$$

where $T(D_1, D_2, .., D_L)$ is the generalized transfer function.

Upper-bounding the complementary error function as $erfc\sqrt{x+y} \leq erfc\sqrt{x} \cdot e^{-y} \leq e^{-(x+y)}$ and averaging over fading gives the bound on CEP:

$$\overline{CEP} \leq \sum_{i_1} .. \sum_{i_L} w(i_1..i_L) \cdot \frac{1}{2}\Big(1 - \sqrt{\frac{i_1\bar{\gamma}}{1+i_1\bar{\gamma}}}\Big) \prod_{l=2}^{L} \frac{1}{1+i_l\bar{\gamma}} \tag{5}$$

$$\overrightarrow{\bar{\gamma} \to +\infty} \sum_{(i_1,..,i_L) \in I_\alpha} \frac{w(i_1, .., i_L)}{4\,\bar{\gamma}^{\alpha}} \Big(\prod_{l=1,\ I_l \neq 0}^{N} i_l \Big)^{-1} \tag{6}$$

where the sums in (5) are for $(i_1, .., i_L) \neq (0, .., 0)$, $\bar{\gamma}$ is the average signal to noise ratio and I_α is the set of $(i_1, .., i_L)$ with α non zero elements. This bound can be also derived from $\frac{1}{2}(\tilde{A}_{11} - 1)$, which is half the generalized transfer function $T(D_1, .., D_L)$, substituing 1 with 1; a term D_i^h with $1 - \sqrt{\frac{h\bar{\gamma}}{1+h\bar{\gamma}}}$; and the other $L-1$ terms D_i^h with $\frac{1}{1+h\cdot\bar{\gamma}}$.

It is worth noting that the low degree terms in (4) give the diversity order, α, achievable by a given coding scheme over the block fading channel. Moreover, these allow an asymptotical evaluation of the average CEP. As these terms can be directly derived from matrix $\tilde{\mathbf{A}}$, a comparison among different convolutional codes is possible in order to design good codes. So we can find the best codes given L, the interleaving strategy and the codeword length. To perform an efficient search a suitable decomposition of $\tilde{\mathbf{A}}$ has been developed. As an example, for a rate 1/2, 64 states code with bit interleaving and $N = 194$, the optimum generator polynomials for $L = 8$ are $(127, 155)_8$. An asymptotic gain of $0.3dB$ in terms of signal to noise ratio with respect to the optimum generator polynomials for AWGN has been verified by simulations. These generators are optimum for any N larger than 40. Numerical results will be presented at the conference.

References

[1] E.Malkamaki, H.leib, "Coded Diversity on Block-Fading Channels", IEEE Trans. on Information Theory, vol.45, march 1999.

[2] M.Chiani, "Error Probability for Block Codes over Channels with Block Interference", IEEE Trans. on Information Theory, vol.44, nov.1998.

[3] J.K.Wolf, A.J.Viterbi, "On the Weight Distribution of Linear Block Codes Formed From Convolutional Codes", IEEE Trans. on Communications, vol.44, sept.1996.

[4] Y.S.Leung, S.G.Wilson, J.W.Ketchum, "Multifrequency Trellis Coding with Low Delay for Fading Channels", IEEE Trans. on Communications, vol.41, oct.1993.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Further Results on Unequal Error Protection of Convolutional Codes*

Chung-Hsuan Wang and Chi-chao Chao
Dept. of Electrical Engineering, National Tsing Hua University
Hsinchu, Taiwan 30013, R.O.C.
e-mail: ccc@ee.nthu.edu.tw

Abstract — **In this paper, we concentrate on the study of combining the optimality with respect to unequal error protection and canonicity of generator matrices for convolutional codes. The transformation which can keep the optimality of generator matrices is constructed, based on which a procedure for obtaining a basic and optimal generator matrix with the smallest external degree is also proposed. Moreover, necessary and sufficient conditions for a canonical generator matrix whose separation vector is the greatest among all canonical generator matrices are given. Finally, the existence of the greatest separation vector among all canonical generator matrices is proved for some convolutional codes.**

In a previous paper [1], we showed that every convolutional code has at least one optimal generator matrix with respect to unequal error protection. A procedure for converting an arbitrary optimal generator matrix to a basic [2] polynomial generator matrix (PGM) without affecting its optimality was also proposed. However, by a counter-example, we showed that not every convolutional code can have an optimal generator matrix which is also canonical [2]. Since the external degree [2] of a PGM corresponds to the number of memory elements in direct-form realization of this PGM, to reduce the hardware complexity, it is desirable to generate a basic and optimal generator matrix of the smallest external degree.

To obtain the transformation between optimal generator matrices, we first define an effectively lower-triangular matrix.

Definition 1 *Let G(D) be a generator matrix of an (n,k) convolutional code. Assume the components of the separation vector [1] $s(G(D))$ are nondecreasingly ordered and have α distinct values, each with β_i repetitions for all $1 \le i \le \alpha$. For a $k \times k$ matrix $T(D)$ over $F(D)$, where $F(D)$ is the rational field over a field F, let $t_{u,v}(D)$ be the entry in position (u,v) of $T(D)$ for all $1 \le u, v \le k$. $T(D)$ is called effectively lower-triangular with respect to $G(D)$ if and only if*

$$t_{u,v}(D) = 0$$

for all $\sum_{l=1}^{i-1} \beta_l < u \le \sum_{l=1}^{i} \beta_l$, $v > \sum_{l=1}^{i} \beta_l$, and $1 \le i \le \alpha$.

Based on effectively lower-triangular matrices, necessary and sufficient conditions for the transformation between all optimal and basic generator matrices are given as follows.

Theorem 1 *Given an (n,k) convolutional code C, let $G(D)$ be an optimal and basic generator matrix of nondecreasing separation vector. For any $k \times k$ nonsingular matrix $T(D)$ over $F(D)$, $T(D) \cdot G(D)$ is optimal and basic if and only if $T(D)$ is unimodular and effectively lower-triangular with respect to $G(D)$.*

Based on Theorem 1, a procedure for obtaining a basic and optimal generator matrix which has the smallest external degree is proposed.

In addition, some properties of canonical PGM's for UEP are discussed below. If there exists a canonical PGM of the greatest separation vector, the corresponding necessary and sufficient conditions are given in Theorem 2.

Theorem 2 *Consider an (n,k) convolutional code C. Define $w(C) = \{w(c(D)) : \forall\ c(D) \in C\}$ and $C^\rho = \{c(D) : \forall\ c(D) \in C$ and $w(c(D)) < \rho\}$. Without loss of generality, assume the components of the separation vectors corresponding to the following generator matrices are nondecreasingly ordered. A generator matrix $G(D)$ has the greatest separation vector among all canonical generator matrices if and only if $\forall\ \rho \in w(C)$, for any canonical generator matrix $A(D)$ of C satisfying*

$$\langle C^\rho \rangle \subseteq \langle \boldsymbol{a}_1(D), \boldsymbol{a}_2(D), \cdots, \boldsymbol{a}_i(D) \rangle$$

we have

$$\langle C^\rho \rangle \subseteq \langle \boldsymbol{g}_1(D), \boldsymbol{g}_2(D), \cdots, \boldsymbol{g}_i(D) \rangle$$

where $G(D)$ and $A(D)$ have rows $\boldsymbol{g}_i(D)$'s and $\boldsymbol{a}_i(D)$'s for all $1 \le i \le k$, respectively.

Although we have shown that every convolutional code has an optimal matrix, however, the existence of a canonical PGM whose separation vector is the greatest among all canonical PGM's is still doubtful. Instead of a general proof, in Theorem 3, we show the existence of a canonical PGM with the greatest separation vector for the convolutional codes of $k \le 3$.

Theorem 3 *Let $G(D)$ and $G'(D)$ be canonical generator matrices of an (n,k) convolutional code C with $k \le 3$. If $s(G(D))$ and $s(G'(D))$ are not comparable, there exists another canonical generator matrix $G^*(D)$ and two permutations ϕ and ϕ' of vector components such that*

$$s(G^*(D)) \ge \phi(s(G(D))) \quad \text{and} \quad s(G^*(D)) \ge \phi'(s(G'(D))).$$

Finally, following a similar proof, the result of Theorem 3 can be directly extended to the convolutional codes whose optimal generator matrix has distinct components in the separation vector.

*This work was supported by the National Science Council of the Republic of China under Grant NSC-88 -2213-E-007-081.

References

[1] M.-C. Chiu, C.-C. Chao, and C.-H. Wang, "Convolutional codes for unequal error protection," in *Proc. 1997 IEEE Int. Symp. Inform. Theory*, Ulm, Germany, June 1995, p. 290.

[2] R. J. McEliece, "The algebraic theory of convolutional codes," in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman eds. Amsterdam, The Netherlands: Elsevier, 1998, pp. 1065–1138.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On the Computation of Weight Enumerators for Convolutional Codes

Cecilio Pimentel [1]
Dept. of Electronics and Systems, Fed. Univ. Pernambuco, P.O. Box 7800
50711-970 Recife - Brazil e.mail: cecilio@npd.ufpe.br

Abstract — **Performance bounds for maximum likelihood decoding of convolutional codes over memoryless channels are commonly measured using the first few terms of the series expansion of the *transfer function* $T(x,y)$. In this paper we present an efficient algebraic method to obtain this truncated series without first computing the complete $T(x,y)$.**

I. The Path Weight Enumerators

Let $\mathcal{S}$ be the set of all paths of an $1/n$-rate convolutional code with constraint length K, that diverge from the all-zero path at $t=0$ and remerge into the all-zero path at some time later. Let w_1 and w_2 be weight functions such that $w_1(\boldsymbol{\sigma})$ and $w_2(\boldsymbol{\sigma})$ are the number of 1's in the input and output sequence, respectively, corresponding to a state sequence $\boldsymbol{\sigma} \in \mathcal{S}$. $T(x,y)$ is the generating series for the set $\mathcal{S}$ with respect to w_1 and w_2, that is, $T(x,y) = \sum_{\boldsymbol{\sigma} \in \mathcal{S}} x^{w_1(\boldsymbol{\sigma})} y^{w_2(\boldsymbol{\sigma})}$. The number of paths in $\mathcal{S}$ of Hamming weight d is the coefficient of y^d in $T(1,y)$, and the total number of nonzero information bits in all paths of Hamming weight d in $\mathcal{S}$ is the coefficient of y^d in $\left\{\frac{\partial T(x,y)}{\partial x}\right\}_{x=1}$.

The first step to compute $T(x,y)$ is to generate the adjacent matrix $\mathbf{A}$ as follows. The $(i,j)^{th}$ entry of $\mathbf{A}$ is either $[\mathbf{A}]_{i,j} = x^{w_1(i\to j)} y^{w_2(i\to j)}$, where $w_1(i \to j)$ and $w_2(i \to j)$ are the Hamming weights of the input and output strings on the branch that connects the states i and j, respectively, or zero, if i and j are not connected. All state sequences in $\mathcal{S}$ have the following structure: The first symbol is 0, the second is 1, the third is either 2 or 3, and so on, the second last symbol is 2^{K-2}, and the last symbol is 0. Define a non-zero path as a path which does not enter or leave the zero state. Let $T_1(x,y)$ be the generating series that enumerates non-zero paths from the initial state 1 to the terminal state 2^{K-2} with respect to w_1 and w_2. Thus

$$T(x,y) = [\mathbf{A}]_{0,1}\, T_1(x,y)\, [\mathbf{A}]_{2^{K-2},0}. \qquad (1)$$

Let $\mathbf{A}(0)$ be a matrix identical to its counterpart $\mathbf{A}$, except that the first row and the first column are set to zero. Then

$$T_1(x,y) = \left[(\mathbf{I} - \mathbf{A}(0))^{-1}\right]_{1,2^{K-2}}. \qquad (2)$$

The $(1,2^{K-2})^{th}$-entry of the k^{th} power of $\mathbf{A}(0)$ is a bivariate polynomial whose exponents are Hamming weights $w_1(\boldsymbol{\sigma})$ and $w_2(\boldsymbol{\sigma})$ of all non-zero paths originating in state 1 and terminating in state 2^{K-2}, and the coefficients are the multiplicity of the weights. It is necessary to invert a $2^{K-1} \times 2^{K-1}$ symbolic matrix in order to find a closed form expression for $T_1(x,y)$. We propose next an iterative procedure for calculating $T_1(x,y)$, called state reduction algorithm, that discards, at each step, all paths with Hamming weight higher than a given order. We need the following definitions:

[1]This work was supported by CNPq under Grant 300987/96-0.

Definition 1: Two finite state machines (FSM) are said to be equivalent if and only if their transfer functions are identical.
Definition 2: Two FSM are said to be equivalent of order L_m if and only if the series expansion of $T(x,y)$ and $\{\partial T(1,y)/\partial x\}_{x=1}$ of order L_m and lower are the same for the two FSM.

II. State Reduction Algorithm

The algorithm creates a sequence of adjacent matrices representing equivalent FSM of order L_m with one state less. It should be observed that each non-zero path is formed by concatenating paths that start from state 1 and reach state 2^{K-2} for the first time some time later. Call the set of all such paths $\mathcal{S}_2$. For example, the path $\boldsymbol{\sigma} = 124|124|1364$ is the concatenation of 3 paths belonging to $\mathcal{S}_2$. If $T_2(x,y)$ is the generating series for the set $\mathcal{S}_2$, we have:

$$T_1(x,y) = T_2(x,y)(1 - [\mathbf{A}]_{2^K-2,1}\, T_2(x,y))^{-1}.$$

To calculate $T_2(x,y)$ we may form a sequence of equivalent FSM where at each step we eliminate transitions from and into the r^{th} state. The $2^{K-1} \times 2^{K-1}$ adjacent matrix for this equivalent FSM, denoted by $\mathbf{A}(r)$, is calculated from the adjacent matrix of the previous step $\mathbf{A}(s)$ (obtained from the elimination of the s^{th} state) as shown in the following lemma.

Lemma 1 Let $\mathcal{R}$ and $\mathcal{C}$ be sets of indexes l, $l = 1, \cdots, 2^{K-1}$, $l \neq r$, such that $[\mathbf{A}(s)]_{l,r}$ and $[\mathbf{A}(s)]_{r,l}$ are different from zero, respectively. The $(i,j)^{th}$ entries of the matrix $\mathbf{A}(r)$ are:

$[\mathbf{A}(s)]_{i,j} + [\mathbf{A}(s)]_{i,r}(1 - [\mathbf{A}(s)]_{r,r})^{-1}[\mathbf{A}(s)]_{r,j}$, if $i \in \mathcal{R}$, $j \in \mathcal{C}$;
0, if $i = r, j = 1, \cdots, 2^{K-1}$;
0, if $j = r, i = 1, \cdots, 2^{K-1}$;
$[\mathbf{A}(s)]_{i,j}$, otherwise,

where on the first row, $[\mathbf{A}(s)]_{i,j}$ is due to parallel transitions, and $(1-[\mathbf{A}(s)]_{r,r})^{-1}$ stands for the circulation loop on the r^{th} state. The state reduction algorithm is summarized below:

- Set $s = 0$. Find $\mathbf{A}(0)$.
- Form the sequence of equivalent FSM $\mathbf{A}(r)$, $r = 2^{K-1} - 1, \cdots, 2^{K-2} - 1, 2^{K-2} + 1, \cdots, 2$, according to Lemma 1.
- $T_2(x,y) = [\mathbf{A}(2)]_{1,2^{K-2}}$.

We propose next a modification of the algorithm which is significant in practice. We will create a sequence of *equivalent FSM of order* L_m by performing the following operation: After calculating $[\mathbf{A}(r)]_{i,j}$, $i \in \mathcal{R}, j \in \mathcal{C}$, according Lemma 1, we compute symbolically its series expansion with respect to the variable y, up to order L_m. The algorithm has two new features. First, we defined combinatorial identities to work with equivalent FSM at the level of the adjacent matrix which is convenient for symbolic computation. Second, no matter the number of states, the entries of $\mathbf{A}(r)$ are bivariate polynomials whose powers of y are of order at most L_m, resulting in a truncated transfer function with considerable less storage requirements.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

The binary multiplying channel without feedback: new rate pairs in the zero-error capacity region

Ludo Tolhuizen
Philips Research Laboratories, WY 61
Prof. Holstlaan 4
5656 AA Eindhoven
The Netherlands
e-mail: ludo.tolhuizen@philips.com

Two terminals, T1 and T2, wish to communicate over the binary multiplying channel (BMC). To this end, they choose sets X and Y, respectively, of (input) vectors in $\{0,1\}^n$. If $\mathbf{x}\in X$ and $\mathbf{y}\in Y$ are fed to the BMC, it gives as output the vector $\mathbf{x}\cdot\mathbf{y}$, defined by $(\mathbf{x}\cdot\mathbf{y})_i = x_i y_i$ for all $i\in\{1,2,\ldots,n\}$. Each terminal should be able to determine *unambiguously* the vector transmitted by the other one, using its own transmitted vector and the observed channel output. We call a pair (X,Y) satisfying this requirement *uniquely decodable*, or UD for short. Moreover, we call a UD pair (X,Y) *symmetric* if $X = Y$. Note that unlike [1], we do *not* allow feedback, that is, encoding of a message does not depend on the output bits observed so far.

If (X,Y) is a UD pair of length n, we define the rate pair $(R(X),R(Y)) = (\frac{1}{n}\log|X|, \frac{1}{n}\log|Y|)$. As usual, all logarithms have base 2. A rate pair (x,y) will be called *achievable* if for each $\epsilon > 0$, there exists a UD pair (X,Y) such that $R(X) > x-\epsilon$ and $R(Y) > y-\epsilon$. The set of achievable rate pairs will be called the zero-error capacity region of the BMC without feedback, and it will be denoted by Z.

In [2], we construct UD codepairs from cosets of binary linear codes with many information sets and obtain the following theorem, in which h denotes the binary entropy function.

Theorem
$\{(h(R_2)+R_1-1, h(R_1)+R_2-1) \mid \frac{1}{2} \le R_1, R_2 < 1\} \subset Z$.
For $\frac{1}{2} \le R < 1$, *the rate pair* $(h(R)+R-1, h(R)+R-1)$ *can be achieved with symmetric UD pairs.*

Specializing the theorem to the case R=2/3, we find

Corollary *The rate pair* $(\log(3/2),\log(3/2)) \approx (0.585, 0.585)$ *can be achieved with symmetric UD pairs.*

The rate pair of the corollary yields the largest known sum of the rates of pairs in Z, and clearly improves on the largest known sum rate so far attained by a UD pair with rate pair (0.548,0.548) [3]. It follows from [4, Thm. 3] that the rate pair (log(3/2),log(3/2)) is the largest possible that can be achieved with symmetric UD pairs. Stated differently, asymptotically our construction yields cancellative families of sets [4] [5, Sec. VII] of largest possible rate.

The results are represented graphically in Figure 1. The rate pairs from the theorem lie on and below the curve N, labelled by "new rate pairs". As ({1},{0,1}) is a UD pair, (0,1)$\in Z$; similarly, (1,0)$\in Z$. With a time sharing argument [1, Sec. 8], it can be shown that Z is convex. Consequently, all rate pairs on and below the tangents to N through (1,0) and (0,1) are in Z. The relevant segments of these tangents are drawn as well.
The line segment "upper bound" represents the upper bound of [6], according to which $x+y \le 1.2181$ for any $(x,y) \in Z$. As remarked by Erik Meeuwissen in [7, Stellling 2], combination of this upper bound with Shannon's lower bound [1, Sec. 13] shows that the zero-error capacity region of the BMC without feedback is strictly smaller than its ϵ-error capacity region.

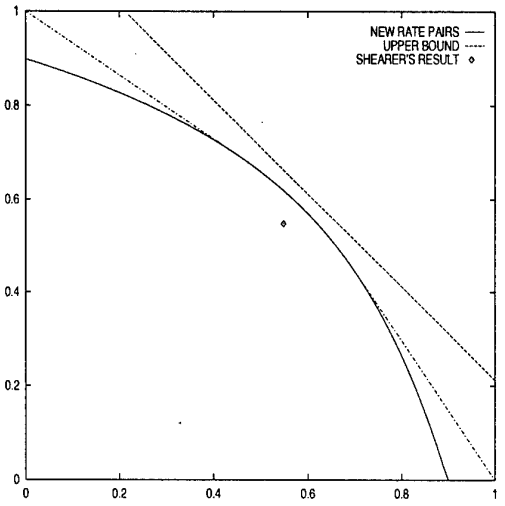


Fig. 1: Graphical representation of the results. All points below the solid curve or its two tangents are in Z.

References

[1] C.E. Shannon, "Two-way communication channels", Proc. 4th Berkeley Symp. Math. Stat. and Prob., 1961, pp. 611–644. Reprinted in *Key Papers in the Development of Information Theory*, D. Slepian(ed), IEEE Press, 1974, pp. 339–372.

[2] L.M.G.M. Tolhuizen, "New rate pairs in the zero-error capacity region of the binary multiplying channel without feedback", accepted for publication in *IEEE Trans. Inform. Th.*, May 2000.

[3] J.B. Shearer, "On Cancellative Families of Sets", *Electr. J. Combinatorics*, Vol. 1, No. 4, 1996.

[4] P. Frankl and Z. Füredi, "Union-free Hypergraphs and Probability Theory", *Europ. J. Combinatorics*, Vol. 5, 1984, pp. 127–131.

[5] J. Körner and A. Orlitsky, "Zero-Error Information Theory", *IEEE Trans. Inform. Th.*, **IT**-44, 6, Oct. 1998, pp. 2207–2229.

[6] R. Holzman and J. Körner, "Cancellative Pairs of Families of Sets", *Europ. J. Combinatorics*, Vol. 16, 1995, pp. 263–266.

[7] H.B. Meeuwissen, *Information Theoretical Aspects of Two-way Communication*, Ph.D. thesis, Eindhoven Univ. Techn., May 1998.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Error exponents for the two-user Poisson multiple-access channel

Shraga I. Bross
Dept. of Electrical Engineering
Technion, Haifa 32000, ISRAEL
e-mail:
shraga@ee.technion.ac.il

Marat V. Burnashev
Institute for Problems of
Information Transmission
Russian Academy of Sciences
101447 Moscow, Russia
e-mail: burn@iitp.ru

Shlomo Shamai (shitz)
Dept. of Electrical Engineering
Technion, Haifa 32000, ISRAEL
e-mail:
sshlomo@ee.technion.ac.il

Abstract — **The error exponent of the two-user Poisson multiple-access channel under peak and average power constraints, but unlimited in bandwidth, is considered. First, a random coding lower bound on the error exponent is obtained, and an extension of Wyner's single-user codes [1] is shown to be exponentially optimum for this case as well. Second, the sphere packing bounding technique suggested in [2] is generalized to the case at hand and an upper bound on the error exponent, which coincides with the lower bound, is derived.**

The model studied here assumes two independent users that generate the inputs $\lambda_{m_i}(t)$, $i = 1, 2$, $0 \le t \le \infty$, which determine the rates of two corresponding doubly stochastic Poisson processes $d_i(t)$. The observation is

$$\nu(t) = \sum_{i=1}^{2} d_i(t) + D(t) \ ,$$

which is also a Poisson process with instantaneous rate $\lambda_0 + \sum_{i=1}^{2} \lambda_{m_i}(t)$. The dark current represented by $D(t)$ is a homogeneous Poisson process of rate λ_0. It is further assumed that the waveforms are subject to peak and average power constraints - i.e. $0 \le \lambda_{m_i}(t) \le A$, $1/T \int_0^T \lambda_{m_i}(t)dt \le q_i A$..

Using a DMC decomposition for our continouos-time model the two-user capacity region of [3] is obtained. Furthermore, applying the rate-splitting technique of [4] to our discrete time model we conclude that in the non band limited case rate-splitting extends to the continuous-time Poisson channel.

Next assuming maximum-likelihood decoding, a lower bound on the error exponent is computed via the random coding error exponent of this DMC decomposition. The exponent consists of two terms; the successive decoding and joint decoding exponents defined respectively by ($s = \lambda_0/A$)

$$\begin{aligned} E_{11}(\rho, q_1, q_2) &= s + q_1 + q_2 - (1 - q_2)s[1 + \tau_0 q_1]^{1+\rho} \\ &\quad -q_2(1 + s)[1 + \tau_1 q_1]^{1+\rho} \end{aligned} \qquad (1)$$

with

$$\tau_0 = (1 + 1/s)^{\frac{1}{1+\rho}} - 1 \ , \quad \tau_1 = [1 + 1/(s + 1)]^{\frac{1}{1+\rho}} - 1$$

and

$$\begin{aligned} &E_{12}(\rho, q_1, q_2) = \\ &\quad s + q_1 + q_2 - \Big[(1 - q_1)(1 - q_2)s^{\frac{1}{1+\rho}} \\ &\quad +(q_1 + q_2 - 2q_1q_2)(1 + s)^{\frac{1}{1+\rho}} + q_1q_2(2 + s)^{\frac{1}{1+\rho}}\Big]^{1+\rho} \end{aligned} \qquad (2)$$

An extension of the code construction of [1, part I] to the case at hand is presented wherein a two-user code with non-equal ($q_1 < q_2$) average-power cnstraint is constructed. This is acomplished by constructing first a $(q_2, M_1 + M_2, T)$ Wyner code and then modifying a (q_2, M_1, T) subcode to conform with the q_1 constraint. The resulting code exhibits the statistical properties of a two-user "random-code" hence the corresponding upper bounds on the successive decoding and joint decoding error probabilities are shown to yield the exponents (1) and (2).

We extend the approach outlined in [2] to the two-user case thereby obtaining a sphere-packing lower bound on the error probability. Specifically, we associate a "volume" with the set of all sequences representing a realization of n arrivals on $[0, T]$. Given a specific realization of n arrivals, each hypothesis of transmitted two-user message determines a configuration triple (n_1, n_2, n_0) consisting of the number of photon arrivals on the time slot where only one of the users is active, both of them are active and none of them is active, respectively. Now, each such configuration is also associated with a corresponding volume. Using these definitions we derive a lower bound on the error probability.

We prove that in the non band limited regime binary signaling incurrs but a negligible loss in the error probability. Furthermore, it is shown that equi-energy signaling for each of the users is optimal from the error probability aspect. These conclusions lead to a sphere-packing exponent which coincides with the random coding lower bound.

Using similar arguments as in [1, part II] we show that the straight line bound is tight for rates below the cutoff rate.

Consequently, the two-user Poisson MAC joins its single-user partner as one of very few for which the reliability function is known.

References

[1] A. D. Wyner, "Capacity and error exponent for the direct detection photon channel - parts I-II," *IEEE Trans. Inform. Theory,* vol. IT-34, pp. 1449-1471, November 1988.

[2] M. V. Burnashev and Y. A. Kutoyants, "On sphere-packing bound, capacity and related results for the Poisson channel," *Probl. Inform. Transm.*, vol. 35, pp. 3-22 (1999).

[3] A. Lapidoth and S. Shamai (Shitz), "The Poisson multiple-access channel," *IEEE Trans. Inform. Theory,* vol. IT-44, pp. 488-502, March 1998.

[4] A. Grant, B. Rimoldi, R. Urbanke and P. Whiting, "Rate splitting multiple-access for discrete memoryless channels," to appear in *IEEE Trans. Inform. Theory,*.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On the capacity of some uncoordinated multiple-access channels

Peter Gober
Digital Communications Group
University of Essen
Ellernstr. 29
45326 Essen, Germany
e-mail: peter.gober@ieee.org

Abstract — **We consider *uncoordinated* multiple-access. Here, a number of transmitter-receiver pairs operate independently over a common channel and regard the transmissions of the remaining users as random noise. It is shown, that for the uncoordinated binary adder channel, the capacity is upper bounded by $1/\ln 2$ bits/transmission and does not grow logarithmically with the number of users as it does in the coordinated case. An asymptotic lower bound for the capacity is given. Further examples of uncoordinated channels are studied.**

I. Introduction

Here, we are interested in *uncoordinated* multiple-access. Each transmitter has a dedicated receiver, that only decodes the messages intended for him and regards the remaining transmissions as random noise (*single-user detection*).

The following approach to uncoordinated multiple-access has been introduced by Cohen, et al. [2]: The individual transmissions are treated as identical single-user channels with identical outputs. The activity of the other users stimulates channel transitions. As a result, transition probabilities are functions of the input distribution.

The (total) capacity of an uncoordinated multiple-access channel is defined by

$$C_{\text{uncoord.}} = T \cdot \left[\max_{p(x)} \left(H(Y) - H(Y|X_i) \right) \right]. \qquad (1)$$

The maximum is taken over the input distribution (which is common to all users).

II. Binary adder channel

The binary adder multiple-access channel accepts binary input $x_i \in \{0, 1\}$ from each of T transmitters. The channel output $y \in \{0, \ldots, T\}$ is the algebraic sum of the inputs, $y = x_1 + x_2 + \cdots + x_T$.

For the *coordinated* binary adder multiple-access channel, Chang and Wolf [1] found that the capacity is achieved by $P(X_i = 0) = P(X_i = 1) = \frac{1}{2}$. It increases with the logarithm of T.

Figure 1 shows one of the equivalent single-user channels for the binary adder channel. The input probabilities are $P(X = 1) = p$ and $P(X = 0) = 1 - p$.

We can show, that the mutual information of the single-user channels can be written as

$$I(X;Y) = \sum_{i=0}^{T-1} \binom{T-1}{i} p^i (1-p)^{T-1-i} \left[(1-p) \log_2 \frac{T-i}{T(1-p)} + p \log_2 \frac{i+1}{Tp} \right]. \qquad (2)$$

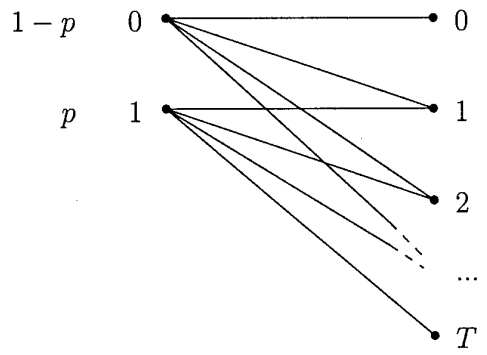


Fig. 1: Binary adder channel as seen by an individual transmitter-receiver pair

It can then be shown:

Theorem 1 *The capacity of the uncoordinated T user multiple-access binary adder channel is upper bounded by $C \leq \frac{1}{\ln 2}$ bits/transmission.*

The capacity does not grow with the number of users as it does in the coordinated case.

Theorem 2 *As $T \to \infty$, for the capacity of the uncoordinated T-user multiple-access binary adder channel, it holds $C_{T\to\infty} \geq .8371$ bits/transmission.*

III. Further channels

In addition the uncoordinated XOR channel and an uncoordinated continous-time channel are studied.

References

[1] S.-C. Chang, J. K. Wolf, "On the T-user M-frequency noiseless multiple-access channel with and without intensity information," *IEEE Trans. Inform. Theory*, vol. IT-27, pp. 41–48, Jan. 1981.

[2] A. R. Cohen, J. A. Heller, A. J. Viterbi, "A new coding technique for asynchronous multiple access communication," *IEEE Trans. Communication Technology*, vol. COM-19, pp. 849–855, Oct. 1971.

[3] P. Gober, "Aspects of uncoordinated multiple-access," Ph. D. thesis, University of Essen, 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On the White Gaussian Multiple-Access Relay Channel

Gerhard Kramer[1] and Adriaan J. van Wijngaarden
Bell Laboratories, Lucent Technologies
600 Mountain Ave, Murray Hill NJ 07974, U.S.A.
e-mail: {gkr,alw}@research.bell-labs.com

Abstract — **The multiple-access relay channel (MARC) is introduced and capacity outer and inner bounds for it are derived.**

I. Introduction

The spectral efficiency of mobile radio networks can be improved by allowing each mobile station to act as a relay for one other mobile station. One can expect further performance improvement if each relay aids not just a single mobile station, but many simultaneously. We attempt to quantify this improvement by introducing the multiple-access relay channel (MARC) and deriving capacity results for it. Most of the discussion is restricted to the white Gaussian MARC.

II. Model

A white Gaussian MARC is a $K+2$ terminal channel with $K+1$ inputs X_1, X_2, ..., X_K, X_R and two outputs Y_D and Y_R such that

$$Y_D = \left(\sum_{k=1}^{K} X_k\right) + X_R + Z_D, \quad Y_R = \left(\sum_{k=1}^{K} X_k\right) + Z_R, \quad (1)$$

where Z_D and Z_R are zero-mean Gaussian random variables with variances N_D and N_R, respectively. The terminal transmitting X_k sends a B_k bit message to the destination terminal receiving Y_D, $k = 1, \ldots, K$. A relay terminal observes Y_R and transmits X_R. There are block energy constraints on the N transmissions: $\sum_{n=1}^{N} \mathrm{E}[|X_{kn}|^2]/N \le P_k$, $k = 1, \ldots, K$, and $\sum_{n=1}^{N} \mathrm{E}[|X_{Rn}|^2]/N \le P_R$. The *capacity region* $\mathcal{R}_{\mathrm{MARC}}$ is the closure of the set of rate-tuples $(R_1, \ldots, R_K)$, where $R_k = B_k/N$ bits per use, at which the destination terminal can decode the K messages with arbitrarily small positive error probability.

III. An Outer Bound

One can derive the following outer bound to $\mathcal{R}_{\mathrm{MARC}}$ by following similar steps as in the proof of Theorem 4 in [1]. This outer bound applies to both discrete memoryless and white Gaussian MARCs. We write $X_{(S)} = \{X_k : k \in S\}$ for a set S.

Theorem 1 *$\mathcal{R}_{\mathrm{MARC}}$ is contained within the convex hull of the set of rate-tuples $(R_1, \ldots, R_K)$ satisfying*

$$0 \le \sum_{k\in S} R_k \le \min\left[I(X_{(S)}; Y_R Y_D | X_{(S^C)} X_R), \; I(X_{(S)} X_R; Y_D | X_{(S^C)})\right], \quad (2)$$

where S is any subset of $\{1, 2, \ldots, K\}$, S^C is the complement of S in $\{1, 2, \ldots, K\}$, and $P(x_1, x_2, \ldots, x_K, x_R)$ factors as

$$\left[\prod_{k=1}^{K} P(x_k)\right] \cdot P(x_R | x_1, \ldots, x_K). \quad (3)$$

[1]This work was performed while this author was with Endora Tech AG, Hirschgässlein 40, 4051 Basel, Switzerland.

IV. Information Rates

We extend the coding technique of [1, Sec. IV]. Consider the independent, zero mean, unit variance, Gaussian random variables V_k and W_k, $k = 1, \ldots, K$, and set

$$\begin{aligned} X_k &= \sqrt{P_k} \cdot (\sqrt{\alpha_k}\, V_k + \sqrt{1-\alpha_k}\, W_k), \\ X_R &= \sqrt{P_R} \cdot \textstyle\sum_{k=1}^{K} \sqrt{\beta_k}\, V_k, \end{aligned} \quad (4)$$

where $0 \le \alpha_k \le 1$, $\beta_k \ge 0$ and $\sum_{k=1}^{K} \beta_k = 1$. Terminal k randomly generates a certain number $2^{NR_{k_o}}$ of codewords $\underline{v}_k(i)$ of length N by using P_{V_k} in the usual memoryless fashion. For each $\underline{v}_k(i)$, terminal k generates 2^{NR_k} codewords $\underline{w}_k$ by using P_{W_k} and forms

$$\underline{x}_k(i) = \sqrt{P_k} \cdot (\sqrt{\alpha_k}\, \underline{v}_k(i) + \sqrt{1-\alpha_k}\, \underline{w}_k).$$

Each $\underline{x}_k(i)$ is then associated with a $\underline{v}_k(j)$, where j may not be i, by using the random partitioning technique of [1, p. 575].

The transmission is in blocks of length N. Terminal k chooses that $\underline{v}_k(i)$ associated with the $\underline{x}_k$ of the previous block and lets the current block's message choose one of the 2^{NR_k} $\underline{x}_k(i)$. The relay terminal is assumed to have decoded all $\underline{x}_k$ of the previous block and hence knows the $\underline{v}_k(i)$. He transmits $\underline{x}_R = \sqrt{P_R} \cdot \sum_{k=1}^{K} \sqrt{\beta_k}\, \underline{v}_k(i)$. The resulting information rates suggest that the rate-tuple $(R_1, \ldots, R_K)$ is approachable if, for all $S \subseteq \{1, \ldots, K\}$,

$$0 \le \textstyle\sum_{k\in S} R_k \le \min\left[I(X_{(S)}; Y_R | X_{(S^C)} V_{(\{1,\ldots,K\})}), \; I(X_{(S)} V_{(S)}; Y_D | X_{(S^C)} V_{(S^C)})\right]. \quad (5)$$

The region of (5) can enlarge the basic K-user multiple-access capacity region, and for $K = 1$ it is the same region as that in [1]. However, (5) is generally smaller than the anticipated

$$0 \le \textstyle\sum_{k\in S} R_k \le \min\left[I(X_{(S)}; Y_R | X_{(S^C)} X_R), \; I(X_{(S)} X_R; Y_D | X_{(S^C)})\right], \quad (6)$$

whose only difference to (2) is that Y_D is missing in the first information inside the square brackets. Note that the same probability distribution (3) is used for (2), (5) and (6).

As a simple example, consider the case where the relay aids terminal $k = 1$ only, i.e., $\beta_1 = 1$. We can then set $\alpha_k = 0$ for $k = 2, \ldots, K$ and can achieve the region (6). However, the probability distribution $P(x_1, x_2, \ldots, x_K, x_R)$ factors as $\left[\prod_{k=1}^{K} P(x_k)\right] \cdot P(x_R | x_1)$ rather than as in (3).

It is unclear whether the region of (6) is achievable with (3). In any case, we show that the region of (6) differs from that of (2) for any sum-of-rates by at most a factor of $1 + N_R/N_D$ in terms of signal-to-noise ratio. This factor is at most 2 for the usual case where $N_R \le N_D$. For $K = 1$ this gives a simple outer bound to any eventual rate increase over (6).

References

[1] T. M. Cover and A. El Gamal, "Capacity theorems for the relay channel," *IEEE Trans. Inform. Theory*, vol. 25, pp. 572–584, Sept. 1979.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Compressing as well as the best tiling of an image

Wee Sun Lee[1]
Department of Computer Science
National University of Singapore
Singapore 117543
Republic of Singapore
e-mail: leews@comp.nus.edu.sg

Abstract — **We investigate the task of compressing an image by using different probability models for compressing different regions of the image. We introduce a class of probability models for images, the *k-rectangular tilings* of an image, that is formed by partitioning the image into k rectangular regions and generating the coefficients within each region by using a probability model selected from a finite class of N probability models. For an image of size $n \times n$, we give a sequential probability assignment algorithm that codes the image with a code length which is within $O(k \log \frac{Nn}{k})$ of the code length produced by the *best* probability model in the class. The algorithm has a computational complexity of $O(Nn^3)$. An interesting subclass of the class of k-rectangular tilings is the class of tilings using rectangles whose widths are powers of two. This class is far more flexible than quadtrees and yet has a sequential probability assignment algorithm that produces a code length that is within $O(k \log \frac{Nn}{k})$ of the best model in the class with a computational complexity of $O(Nn^2 \log n)$ (similar to the computational complexity of sequential probability assignment using quadtrees).**

I. Introduction

Consider the task of compressing a wavelet subband comprising $n \times n$ wavelet coefficients that have been quantized using a scalar quantizer. For natural images, it is well known that the wavelet coefficients are small in smooth areas and large in the neighbourhood of edges. Because of that, we would like to use different probability models for coding different parts of the subband in order to obtain good compression. We will restrict ourselves to a finite number N of different probability models to choose from.

We introduce a class of probability models formed by partitioning the image into k rectangular regions and generating the coefficients within each region by using a probability model from the finite class of N probability models. We call the class of probability models that is generated in this way the class of *k-rectangular tilings* of the image. Our algorithm aims to compress as well as the best model in this class.

II. Related Work

The class of k-rectangular tilings can be considered as a natural extension to two dimensions of the class of piecewise-identically-distributed source for sequences studied in information theory [6, 4]. Similar methods have also been studied in computational learning theory [2, 5, 1]. In fact, the method described in this abstract is an extension of the specialist method in [1] to two dimensions.

III. Main Results

In this paper, we provide a sequential probability assignment algorithm that codes the image with a code length that is within $O(k \log \frac{Nn}{k})$ bits of the code length produced by the best model in the class of k-rectangular tilings of the image, where k does not need to be known in advance. The computational complexity of the algorithm is $O(Nn^3)$. If we restrict the class of probability models to those generated using rectangular partitions of D discrete widths, the computational complexity can be improved to $O(Nn^2 D)$. This means that we can have a fast algorithm of computational complexity $O(Nn^2 W)$ for a probability assignment that is competitive with the best assignment provided by the class of k-rectangular tilings using rectangles of widths less than W. Another interesting class of models under the restriction to D discrete widths is the class of k-rectangular tilings with rectangles whose widths are powers of two. Restriction of the probability models to this class allows us to have an algorithm with a computational complexity of $O(Nn^2 \log n)$. This class is similar to the class of quadtrees but is more powerful since only one dimension is restricted to the $\log_2 n$ discrete sizes and arbitrary shifts are allowed.

Experiments on compressing wavelet transform of images reported elsewhere [3] show that the method is practically effective.

IV. Open Problem

The method described in this abstract is a sequential probability assignment method. We do not know how to obtain *efficient* two stage coding methods with good bounds on the redundancy for the class of k-rectangular tilings of an image. Such forward adaptation methods may allow the use of sophisticated quantization methods in conjunction with this class of models.

Acknowledgments

The author would like to thank Phil Long for helpful discussions on this work.

References

[1] Yoav Freund, Robert E. Schapire, Yoram Singer, and Manfred Warmuth. Using and combining predictors that specialize. In *Proceedings of the Twenty-Ninth Annual ACM Symposium on the Theory of Computing*, El Paso, Texas, 1997.

[2] M. Herbster and M. Warmuth. Tracking the best expert. *Machine Learning*, 32(2), August 1998.

[3] Wee Sun Lee. Trees, windows and tiles for wavelet image compression. In *Data Compression Conference*, Snowbird, Utah, 2000.

[4] N. Merhav. On the minimum description length principle for sources with piecewise constant parameters. *IEEE Transactions on Information Theory*, 39(6):1962–1967, November 1993.

[5] V. Vovk. Derandomizing stochastic prediction strategies. In *Proceedings of the Tenth Annual Conference on Computational Learning Theory*, pages 32–43, Nashville, Tennessee, 1997.

[6] Frans M. J. Willems. Coding for a binary independent piecewise-identically-distributed source. *IEEE Transactions on Information Theory*, 42(6):2210–2217, November 1996.

[1]This work was supported in part by the National University of Singapore Academic Research Fund grant RP3992710.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

The Optimal Overflow and Underflow Probabilities with Variable-Length Coding for the General Source

Osamu Uchida[1] and Te Sun Han
Graduate School of Information Systems
University of Electro-Communications
Chofugaoka 1-5-1, Chofu, Tokyo 182-8585, Japan
e-mail: o-uchida@hn.is.uec.ac.jp, han@is.uec.ac.jp

Abstract — **In variable-length coding, the probability of codeword length per source letter being above (resp. below) a prescribed threshold is called the overflow (resp. the underflow) probability. In this study, we show that the infimum achievable threshold given the overflow probability exponent r always coincides with the infimum achievable fixed-length coding rate given the error exponent r, without any assumptions on the source. In the case of underflow probability, we also show the similar results. From these results, we can utilize various theorems and results on the fixed-length coding established by Han for the analysis of overflow and underflow probabilities.**

I. General Sources

Let us define a *general source* as an infinite sequence $\mathbf{X} = \{X^n = (X_1^{(n)}, \cdots, X_n^{(n)})\}_{n=1}^{\infty}$ of n-dimensional random variables X^n where each component random variable $X_i^{(n)}$ $(1 \le i \le n)$ takes values in a *countably infinite* set $\mathcal{X}$ which is called the *source alphabet*. It should be noted here that each component of X^n may change depending on block length n. This implies that the sequence $\mathbf{X}$ is quite general in the sense that it may not satisfy even the consistency condition as usual processes. The class of sources thus defined covers a very wide range of sources including all nonstationary and/or nonergodic sources.

II. Overflow and Underflow Probabilities

Let $\varphi_n^{\mathrm{v}} : \mathcal{X}^n \to \mathcal{U}^*$, $\psi_n^{\mathrm{v}} : \mathcal{U}^* \to \mathcal{X}^n$ be a prefix *variable-length encoder* (a one-to-one mapping) and the *decoder* (the inverse mapping of the encoder), respectively, where $\mathcal{U} \equiv \{1, 2, \cdots, K\}$ is called the *code alphabet* and $\mathcal{U}^*$ is the set of all (non-null) finite-length strings from $\mathcal{U}$. Then, let us define the *overflow probability* of the prefix variable-length encoder φ_n^{v} with threshold R by

$$\epsilon_n(\varphi_n^{\mathrm{v}}, R) \equiv \Pr\left\{\frac{1}{n} l\left(\varphi_n^{\mathrm{v}}(X^n)\right) > R\right\},$$

where $l(\mathbf{u})$ denotes the length of $\mathbf{u} \in \mathcal{U}^*$. We also define the *underflow probability* of the prefix variable-length encoder φ_n^{v} with threshold R by

$$\epsilon_n^*(\varphi_n^{\mathrm{v}}, R) \equiv \Pr\left\{\frac{1}{n} l\left(\varphi_n^{\mathrm{v}}(X^n)\right) < R\right\}.$$

For unifilar finite-state sources, Merhav [1] has shown that the optimal exponential decay rate of the overflow probability is equal to the optimal error exponent for fixed length coding, and this optimal decay rate can be universally achieved by using Lempel-Ziv code.

[1]O. Uchida is now with the Dept. of Network Engineering, Kanagawa Institute of Technology, Atsugi, Kanagawa, 243-0292 Japan.

III. Main Results

Definition 1 : R is called an *r-achievable overflow threshold* if there exists a prefix variable-length encoder φ_n^{v} such that

$$\liminf_{n\to\infty} \frac{1}{n} \log \frac{1}{\epsilon_n(\varphi_n^{\mathrm{v}}, R)} \ge r.$$

Moreover, we define the *infimum r-achievable overflow threshold* by

$$L_e(r|\mathbf{X}) \equiv \inf\{R \mid R \text{ is an } r\text{-achievable overflow threshold}\}.$$

Theorem 1 : For *any* general source $\mathbf{X}$ with *countably infinite* alphabet $\mathcal{X}$ and all $r > 0$, we have

$$L_e(r|\mathbf{X}) = R_e(r|\mathbf{X}),$$

where $R_e(r|\mathbf{X})$ is the *infimum r-achievable fixed-length coding rate* [2], and it has been shown by Han [2] that $R_e(r|\mathbf{X}) = \sup_{R\ge 0}\{R - \sigma(R) \mid \sigma(R) < r\}$, where $\sigma(R) \equiv \liminf_{n\to\infty} \frac{1}{n} \log \frac{1}{\Pr\left\{\frac{1}{n}\log \frac{1}{P_{X^n}(X^n)} \ge R\right\}}$.

Definition 2 : R is called an *r-achievable underflow threshold* if there exists a prefix variable-length encoder φ_n^{v} such that

$$\limsup_{n\to\infty} \frac{1}{n} \log \frac{1}{\epsilon_n^*(\varphi_n^{\mathrm{v}}, R)} \le r.$$

Moreover, we define the *infimum r-achievable underflow threshold* by

$$L_e^*(r|\mathbf{X}) \equiv \inf\{R \mid R \text{ is an } r\text{-achievable underflow threshold}\}.$$

Theorem 2 : For *any* general source $\mathbf{X}$ with *countably infinite* alphabet $\mathcal{X}$ and all $r > 0$, we have

$$L_e^*(r|\mathbf{X}) = R_e^*(r|\mathbf{X}),$$

where $R_e^*(r|\mathbf{X})$ is the *infimum r-achievable fixed-length coding rate* [2], and it has been shown by Han [2] that $R_e^*(r|\mathbf{X}) = \inf\left\{h \ge 0 \,\middle|\, \inf_{R\ge 0}\left\{\sigma^*(R) + [R - \sigma^*(R) - h]^+\right\} \le r\right\}$, where $\sigma^*(R) \equiv \limsup_{n\to\infty} \frac{1}{n} \log \frac{1}{\Pr\left\{\frac{1}{n}\log \frac{1}{P_{X^n}(X^n)} \le R\right\}}$, and $[x]^+ \equiv \max(x, 0)$.

Remark : In [2], Han has shown examples of the computation for $R_e(r|\mathbf{X})$ and $R_e^*(r|\mathbf{X})$ for many kinds of sources $\mathbf{X}$. These examples include *countably infinite* alphabet cases that can not be treated by the traditional method of *types*. From Theorems 1 and 2, we can use all of these results to derive the values of $L_e(r|\mathbf{X})$ and $L_e^*(r|\mathbf{X})$.

References

[1] N. Merhav, "Universal coding with minimum probability of codeword length overflow," *IEEE Trans. Inform. Theory*, vol. 37, pp.556–563, May 1991.

[2] T. S. Han, "The reliability functions of the general source with fixed-length coding," *IEEE Trans. Inform. Theory*, to appear.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Minimum Conditional Entropy Context Quantization

Xiaolin Wu[1] Philip A. Chou[2] Xiaohui Xue[3]

Abstract — **We consider the problem of finding the quantizer Q that quantizes the K-dimensional causal context $C_i = (X_{i-t_i}, X_{i-t_2}, \ldots, X_{i-t_K})$ of a source symbol X_i into one of M conditioning states such that the conditional entropy $H(X_i|Q(C_i))$ is minimized. The resulting minimum conditional entropy context quantizer can be used for sequential coding of the sequence $X_0, X_1, X_2, \ldots$.**

A key problem in sequential source coding of a discrete random sequence $X_0, X_1, X_2, \cdots$ is modeling the underlying conditional distribution of the source $P(X_i|X^{i-1})$, Because of model estimation considerations, it is not possible to directly use all of X^{i-1} as the model's context. Many practical source coders choose *a priori* a model with fixed complexity, based on domain knowledge such as correlation structure and typical data length, and estimate only the model parameters. To avoid context dilution problem, we quantize the modeling context into a relatively small number of conditioning states, and estimate $P(X_i|Q(C_i))$ instead, where Q is a context quantizer. This approach has produced some of the best performing signal compression algorithms such as CALIC and JPEG 2000, despite the fact that they are not strictly universal. A pivotal issue for these source coders, which impacts their rate-distortion performance, is the design of the context quantizer Q. The problem is one of optimal vector quantization design with respect to the Kullback-Leibler distance.

Let Y be a discrete random variable, and let C be a jointly distributed random vector, possibly real. Given a positive integer M, we wish to find the quantizer $Q : C \to \{1, 2, \ldots, M\}$ such that $H(Y|Q(C))$ is minimized. Clearly, $H(Y|Q(C)) \geq H(Y|C)$ by the convexity of H. However, we wish to make $H(Y|Q(C))$ as close to $H(Y|C)$ as possible. Equivalently, we wish to minimize the non-negative "distortion" of Q

$$\begin{aligned} D(Q) &= H(Y|Q(C)) - H(Y|C) \\ &= \int dP(\mathbf{c}) D(P_{Y|C=\mathbf{c}} || P_{Y|Q(C)=Q(\mathbf{c})}), \end{aligned} \quad (1)$$

which is the average, over all context vectors $\mathbf{c}$, of the Kullback-Leibler distances between the probability mass functions (pmfs) $P_{Y|C}(\cdot|\mathbf{c})$ and their "reproduction" pmfs $P_{Y|Q(C)}(\cdot|Q(\mathbf{c}))$.

Let $\beta_m(y) = P_{Y|Q(C)}(y|m)$ denote the mth reproduction pmf. Then an optimal Q must map almost all context vectors $\mathbf{c}$ to the conditioning state m that minimizes the Kullback-Leibler distance $D(P_{Y|C=\mathbf{c}}||\beta_m)$, i.e.,

$$Q(\mathbf{c}) = \arg\min_m D(P_{Y|C=\mathbf{c}}||\beta_m). \quad (2)$$

The quantization regions $A_m = \{\mathbf{c} : Q(\mathbf{c}) = m\}$, $m = 1, \ldots, M$, of a minimum conditional entropy context quantizer are generally quite complex in shape, and may not even be convex or connected. However, their associated sets of pmfs $B_m = \{P_{Y|C}(\cdot|\mathbf{c}) : \mathbf{c} \in A_m\}$ are simple convex sets in the probability simplex for Y, owing to the above necessary condition for optimal Q. Let $\beta_m(y) = P(y|C \in A_m)$ be the conditional distribution of Y given $C \in A_m$. Then by (2), for each $\mathbf{c} \in B_m$, the Kullback-Leibler distance from $P_{Y|C}(y|\mathbf{c})$ to $\beta_m(y)$ must be less than (or equal to) the Kullback-Leibler distance to $\beta_{m'}(y)$, $m' \neq m$. Hence

$$\sum_y P(y|\mathbf{c}) \log \frac{1}{\beta_m(y)} \leq \sum_y P(y|\mathbf{c}) \log \frac{1}{\beta_{m'}(y)}, \quad (3)$$

for all $m' \neq m$. In other words, if $\mathbf{c} \in B_m$, then $P(y|\mathbf{c})$ lies in an intersection of halfspaces.

If Y is a binary random variable, then its probability simplex is one-dimensional. In this case, the quantization regions B_m are simple intervals. If the random variable Z is defined as $P_{Y|C}(1|C)$ (the posterior probability that $Y = 1$ as a function of C), then the conditional entropy $H(Y|Q(C))$ of the optimal context quantizer can be expressed

$$H(Y|Q(C)) = \sum_{m=1}^{K} P\{Z \in [q_{m-1}, q_m)\} H(Y|Z \in [q_{m-1}, q_m)) \quad (4)$$

for some set of thresholds $\{q_m\}$. Therefore, the optimal context quantizer can be found by searching over $\{q_m\}$. This is a scalar quantization problem, which can be solved exactly using dynamic programming, regardless of the dimensionality of the context space. Once the scalar problem is solved, the optimal context quantizer cells A_m are given by

$$A_m = \{\mathbf{c} : P_{Y|C}(1|\mathbf{c}) \in [q_{m-1}, q_m)\}. \quad (5)$$

In particular, the boundaries between these cells are determined by those vectors $\mathbf{c}$ for which the posterior probability $P_{Y|C}(1|\mathbf{c})$ is a constant: For example, $P_{Y|C}(1|\mathbf{c}) = q_m$ for $\mathbf{c}$ along the boundary between A_m and A_{m+1}. Equivalently, A_m can be expressed in terms of the likelihood ratio

$$L(\mathbf{c}) = \frac{P_{C|Y}(\mathbf{c}|1)}{P_{C|Y}(\mathbf{c}|0)} = \frac{P_Y(0)}{P_Y(1)} \frac{P_{Y|C}(1|\mathbf{c})}{1 - P_{Y|C}(1|\mathbf{c})}. \quad (6)$$

If both $P_{C|Y}(\mathbf{c}|0)$ and $P_{C|Y}(\mathbf{c}|1)$ are d-dimensional Gaussians, then optimal context quantizer cells are bounded by d-dimensional quadratic surfaces.

The significance of this research is in that it offers a constructive means of designing optimal source codes for minimum code length via high-order context modeling. The problem of controlling model cost in high-order context modeling is addressed by designing optimal context quantizer, which collapses high-order contexts into any given number of coding states in a way to minimize the actual code length. Once the context quantizer Q is designed, on-line estimation of $P(\cdot|Q(C))$ by count statistics and adaptive entropy coding can be done very efficiently, much faster than by context tree methods. We observe that our techniques often outperform the universal source codes of proven optimality by appreciable margins on real data in image, video, and audio compression.

[1]Dept. of Computer Science, Univ. of Western Ontario, London, Ontario, Canada N6A 5B7, wu@csd.uwo.ca.

[2]Microsoft Research, One Microsoft Way, Redmond, WA 98005, USA, pachou@microsoft.com.

[3]Dept. of Computer Science, Harbin Institute of Technology, Harbin, China, xue@csd.uwo.ca.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On the variance and the probability of length overflow of lossless codes

Ryo NOMURA[1]
Waseda University
Shinjuku-ku, Tokyo, Japan.
ryochan@matsu.mgmt.waseda.ac.jp

Toshiyasu MATSUSHIMA
Waseda University
Shinjuku-ku, Tokyo, Japan.

Shigeichi HIRASAWA
Waseda University
Shinjuku-ku, Tokyo, Japan.

Abstract — **In this paper, we show the probability of length overflow of several codes by using the variance and the asymptotic normality of the codelength.**

I. Introduction

Lossless source coding schemes are examined under several criterions. The most representative criterion is redundancy. Recently, Merhav[1] proposed the probability of length overflow.

In this paper we redefine the probability of length overflow. We consider a finite alphabet source $A = \{i : 0 \le i \le k-1\}$. Let $x^n = x_1 x_2 x_3 \cdots x_n \in X^n$ denotes a source sequence. And let $p(x^n)$ denotes the probability distribution of a source. Let $L(\cdot)$ be a codelength and ϵ_n be a function of n.

Definition I. 1 *The probability of length overflow is defined by*

$$Pr\{L(x^n) > \epsilon_n\}. \tag{1}$$

We shall evaluate a code by using the probability of length overflow instead of the expected codelength.

Next we define the two quantities, that have very important role in this paper. First we generalize the minimal coding variance, which is inherent value of a source, proposed by Kontoyiannis[2].

Definition I. 2 *The rth moment of self-information is defined by*

$$M(X)^r = \lim_{n\to\infty} E\left[\left\{-\frac{1}{n}\log p(x^n) - E[-\frac{1}{n}\log p(X^n)]\right\}^r\right].$$

Especially, the 2nd moment of self-information coincides with the minimal coding variance.

Second we define the moment of codelength.

Definition I. 3 *Let $L_c(x^n)$ denotes the codelength for sequence x^n when we use a code c. Then the rth moment of a code c is denoted by*

$$\sigma_c^r = \lim_{n\to\infty} E\left[\left\{\frac{1}{n}L_c(x^n) - E[\frac{1}{n}L_c(X^n)]\right\}^r\right]. \tag{2}$$

Especially, when $r = 2$ we call this the variance of codelength of a code c.

II. The probability of length overflow

We show the probability of length overflow of a code c. Let $L_c(x^n)$ denote the codelength of a code c for x^n.

Lemma II. 1 *If the codelength of a code c satisfies asymptotic normality with respect to a source, the probability of length overflow of a code c is given by*

$$\lim_{n\to\infty} Pr\{L_c(x^n) \ge \epsilon_n\} \tag{3}$$
$$= \int_{Z_n^*}^{\infty} \frac{1}{\sqrt{2\pi}} \exp\left[-\frac{y^2}{2}\right] dy,$$

where, $Z_n^* = \frac{\epsilon_n - E[L_c(x^n)]}{\sqrt{n\sigma_c^2}}$, σ_c^2 is the variance of a code c.

[1]This work was supported by in part of Waseda University under Grant 99A-551 for Special Research Projects.

When a source distribution is known, it is well known that a codelength $-\log p(x^n)$ minimize the expected codelength. We call this code Shannon code and let σ_S^2 be the variance of Shannon code. Obviously, the variance of Shannon codelength coincides with 2nd moment of self-information. Here we define a condition of a source as follows.

Condition II. 1 *The codelength of Shannon code with respect to a source satisfies the asymptotic normality.*

Then we have the following lemma.

Lemma II. 2 *Under ConditionII. 1 , if $\lim \epsilon_n > nH(X) + \sqrt{nM(X)^2}$, then we have*

$$\lim_{n\to\infty} Pr\{-\log p(x^n) > \epsilon_n\} = 0. \tag{4}$$

III. The probability of length overflow of Bayes code

We consider a parameterized source distribution. Let $\theta \in \Theta$ is a k-dimensional parameter of a source. If θ is unknown, it is known that Bayes code minimize the redundancy with respect to Bayes criterion. The coding probability of Bayes code is given by $m(x^n) = \int_{\theta\in\Theta} p(x^n|\theta)p(\theta)d\theta$, where $p(\theta)$ is a prior distribution of θ. We define a condition of a source.

Condition III. 1 *The codelength of Bayes code with respect to a source satisfies the asymptotic normality.*

Then we have the following theorem.

Theorem III. 1 *Let the variance of Bayes code denoted by σ_B^2, we have*

$$M(X)^2 + \frac{k}{n} \ge \sigma_B^2 \ge M(X)^2 + \frac{k}{n} - \sqrt{\frac{2kM(X)^2}{n}}. \tag{5}$$

From above theorem, we have the following lemma.

Lemma III. 1 *Under ConditionIII. 1 , if $\lim_{n\to\infty} \epsilon_n > nH(X) + \sqrt{nM(X)^2}$, then we have*

$$\lim_{n\to\infty} Pr\{-\log m(x^n) > \epsilon_n\} = 0. \tag{6}$$

IV. Consideration

We obtained the probability of length overflow of codes, that minimize the expected codelength. From above lemmas neither source distribution is known or unknown, under ConditionII. 1 ,III. 1 , if we wish the probability of length overflow goes to 0 then it is necessary that ,$\lim_{n\to\infty} \epsilon_n > nH(X) + \sqrt{nM(X)^2}$.

We introduce the moment of self-information and the moment of codelength, that play very important role to analyse the probability of length overflow.

References

[1] N. Merhav, "Universal Coding with Minimum Probability of Codeword Length Overflow," *IEEE Trans. Inf. Theory*,37(3):556-563,1991.

[2] I. Kontoyiannis, "Second-Order Noiseless Source Coding Theorems." *IEEE Trans. Inf. Theory*,43(4):1339-1341,1997.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Identification in the Presence of Side Information with Application to Watermarking

Y. Steinberg and N. Merhav
EE Dpt., Technion, Haifa, Israel
[ysteinbe,merhav]@ee.technion.ac.il

Abstract — **Watermarking (WM) codes are analyzed from an information–theoretic viewpoint as identification (ID) codes with side information that is available either at both transmitter and receiver or at the transmitter only. For the former case, formulas are provided for the ID capacity and for achievable error exponents. For the latter case, upper and lower bounds to the ID capacity are derived.**

WM techniques are about embedding a message into a covertext dataset (say, an image) such that on the one hand, quality is maintained, and on the other hand, this message cannot be removed without access to some secret key or without rendering the data useless. The main application is for proving ownership of the data and for protection against forgers.

In contrast to the vast amount of research work reported in the signal/image processing literature, relatively little attention has been devoted to this problem from the information-theoretic perspective. A few exceptions are, e.g., [2],[3],[5],[6], where attempts were made to characterize capacity and/or error exponents of WM systems by viewing them as coded communication systems, where the covertext data plays the role of side information available at the encoder only or at both ends (depending on the application).

More precisely, consider the following system: A rate- R block code of length n, fed by an (nR)-bit message m, and a n-block of a memoryless covertext source V, generates an n-block of the watermarked version X, within small degradation of quality, symbolized by distortion $Ed(V,X) \leq D_1$. An active attacker, modeled as a memoryless channel $W : X \to Y$ may introduce additional distortion $Ed(X,Y) \leq D_2$ in attempt to disrupt the watermark. Finally, Y is decoded at the receiving end, with or without access to the covertext V, in order to extract the watermark.

In all the above–mentioned papers, WM systems were viewed as ordinary communication systems, where the decoder carries out *full* decoding, i.e., decides which one of 2^{nR} possible messages was embedded. In most of the applications, however, full decoding is not really necessary, as one needs only to detect whether or not a *particular* watermark resides in the covertext. Performance, in this case, is measured by the tradeoffs between rate, false–alarm probability and misdetection probability. This observation guides us to view WM codes as ID codes [1] rather than ordinary transmission codes.

Since in the ID setting, both false–alarm and misdetection probabilities (of each individual message) can be kept arbitrarily small for large n even for a doubly exponential number of messages (when randomized encoders are allowed), the ID WM capacity is defined as limsup of the normalized iterated logarithm of the maximum achievable number of messages defined by an encoder that satisfies the distortion constraint.

Our main results are as follows (for proofs, see [7]):

Theorem 1 *For a discrete memoryless covertext source V, available at both transmitter and receiver, and a given DMC W, the ID WM capacity C_1 is given by*

$$C_1 = H(V) + \sup I(X;Y|V), \tag{1}$$

where the supremum is over all triples (V,X,Y) distributed according to $P(V,X,Y) = P(V)P(X|V)W(Y|X)$ with $Ed(V,X) \leq D_1$.

Theorem 2 *For a discrete memoryless covertext source V, available at the transmitter only, and a given DMC W, the ID WM capacity C_2 is bounded by*

$$\sup_B I(U;Y) \leq C_2 \leq \sup_A I(U;Y), \tag{2}$$

where A is the set of all quadruples (U,V,X,Y) distributed according to $P(U,V,X,Y) = P(V)P(X,U|V)W(Y|X)$ with $Ed(V,X) \leq D_1$, and B is the same as A but with the additional constraint that $I(U;V) < I(U;Y)$.

Two comments: (i) The direct part of Theorem 1 includes a more refined analysis (see [7]) that characterizes a set of achievable triples (R, E_1, E_2), where E_1 and E_2 are exponential rates of the error probabilities of the two kinds. As E_1 and E_2 tend to zero, the maximum achievable rate is $R = C_1$. (ii) It is known that in ID problems, if both transmitter and receiver have access to a common information source (common experiment) Z, then the ID capacity is increased by the entropy of Z. In Theorem 1, obviously $Z = V$. In Theorem 2, the receiver can partially guess V with a common information rate of $I(U;V)$, which when added to $I(U;Y) - I(U;V)$ (corresponding to the transmission capacity with side information at the transmitter only [4]), gives $I(U;Y)$. Accordingly, the additional constraint of set B in Theorem 2 means that the transmission capacity is positive.

References

[1] R. Ahlswede and G. Dueck, "Identification via channels," *IEEE Trans. Inform. Theory*, vol. 35, pp. 15-29, January 1989.

[2] I. J. Cox, M. L. Miller, and A. L. McKellips, "Watermarking as communications with side information," *Proc. of the IEEE*, vol. 87, no. 7, pp. 1127–1141, July 1999.

[3] A. Cohen and A. Lapidoth, "On the Gaussian watermarking game," *Proc. ISIT 2000*, Sorrento, Italy, June 2000.

[4] S. I. Gel'fand and M. S. Pinsker, "Coding for channel with random parameters," *Problems of information and Control*, pp. 19-31, 1980.

[5] N. Merhav, "On random coding error exponents of watermarking systems," *IEEE Trans. Inform. Theory*, March 2000.

[6] J. A. O'Sullivan, P. Moulin, and J. M. Ettinger, "Information theoretic analysis of steganography," *Proc. ISIT '98*, p. 297, 1998.

[7] Y. Steinberg and N. Merhav, "Identification in the presence of side information with application to watermarking," submitted to *IEEE Trans. Inform. Theory* (available at: http://www-ee.technion.ac.il/~merhav).

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding

Brian Chen and Gregory W. Wornell
Research Laboratory of Electronics and Department of Electrical Engineering and Computer Science
Massachusetts Institute of Technology, Room 36-631
Cambridge, MA 02139
Email: bchen@alum.mit.edu and gww@allegro.mit.edu

Abstract — **We consider the problem of embedding one signal (*e.g.*, a digital watermark), within another "host" signal to form a third, "composite" signal. The goal is to achieve efficient rate-distortion-robustness trade-offs. We introduce a new class of embedding methods called distortion-compensated quantization index modulation. In several different contexts involving both intentional and unintentional attacks, capacity-achieving methods exist within this class, while in other contexts these methods achieve provably better rate-distortion-robustness performance than previously proposed spread-spectrum and generalized low-bit(s) modulation methods.**

I. Introduction

Digital watermarking and information embedding systems embed information in a host signal, which is typically an image, audio signal, or video signal. The host signal is not degraded unacceptably in the process, and one can recover the watermark even if the composite host and watermark signal undergo a variety of attacks as long as these corruptions do not unacceptably degrade the host signal. These systems play an important role at least three major application areas: (1) copyright protection of multimedia content, (2) authentication and tamper-detection, and (3) backwards-compatible upgrading of existing legacy communication networks [1].

II. Problem Model

We wish to embed a message $m \in \{1, 2, \ldots, 2^{NR_m}\}$, sometimes called a digital watermark, in some host signal vector $\mathbf{x} \in \Re^N$, where R_m is the embedding *rate* in bits per host signal sample. Specifically, m and $\mathbf{x}$ are mapped onto a composite signal vector $\mathbf{s} \in \Re^N$ using some embedding function $\mathbf{s}(\mathbf{x}, m)$, and we define a *distortion* measure between $\mathbf{x}$ and $\mathbf{s}$. Equivalently, we can define a host-dependent distortion signal $\mathbf{e}(\mathbf{x}, m)$ that is added to $\mathbf{x}$ to obtain $\mathbf{s}$. The composite signal $\mathbf{s}$ is subjected to unintentional attacks and possibly to intentional attacks inside some channel, which produces an output vector $\mathbf{y} \in \Re^N$. A decoder generates an estimate $\hat{m}$ of m after observing $\mathbf{y}$, *i.e.*, we consider the "host-blind" case, where $\mathbf{x}$ is not available to the decoder. Ideally, the decoder can reliably recover the embedded information as long as the channel degradations are not too severe. Thus, the tolerable severity of the degradations is a measure of the *robustness* of the system. The goodness of $\mathbf{s}(\mathbf{x}, m)$ and its corresponding decoder is measured by the achievable rate-distortion-robustness trade-offs.

This work has been supported in part by the Office of Naval Research under Grant No. N00014-96-1-0930, by the Air Force Office of Scientific Research under Grant No. F49620-96-1-0072, by the MIT Lincoln Laboratory Advanced Concepts Committee, and by a National Defense Science and Engineering Graduate Fellowship.

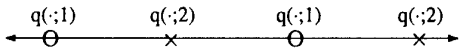


Fig. 1: Quantization index modulation information embedding.

III. Distortion-Compensated Quantization Index Modulation

Quantization index modulation (QIM) embedding functions arise by defining an ensemble of quantizers $\mathbf{q}(\cdot; m)$, one quantizer in the ensemble for each possible value of m. Then, $\mathbf{s}(\mathbf{x}, m) = \mathbf{q}(\mathbf{x}; m)$. An example is shown in Fig. 1 for the case where $N = 1$, $R_m = 1$, and the quantizers are uniform, scalar quantizers. One can decode, for example, by determining whether $\mathbf{y}$ is closer to a o point ($\hat{m} = 1$) or to a $\times$ point ($\hat{m} = 2$). Thus, the $\times$ and o points represent both source codewords for representing $\mathbf{x}$ and channel codewords for communicating m. QIM systems reject interference from the host signal since $\mathbf{x}$ determines which o or $\times$ point is chosen but does not deflect $\mathbf{s}$ or $\mathbf{y}$ away from these points. Distortion-compensated QIM (DC-QIM) systems add back some fraction $1 - \alpha$ of the quantization error, $\mathbf{s}(\mathbf{x}, m) = \mathbf{q}(\mathbf{x}; m) + (1 - \alpha)[\mathbf{x} - \mathbf{q}(\mathbf{x}; m)]$, which can be shown [1] to improve rate-distortion-robustness performance with the proper choice of α.

IV. Performance Against Attacks

In fact, one can derive sufficient conditions under which capacity-achieving DC-QIM systems exist [1]. These conditions are satisfied in at least three cases: (1) the additive Gaussian noise channel and Gaussian host signal scenario of [2], (2) the case of squared error distortion-constrained attacks and a Gaussian host signal described in [3], and (3) the case of squared error distortion-constrained attacks, a non-Gaussian host signal, asymptotically small embedding-induced distortion, and asymptotically small attacker's distortion described in [3].

In a number of other contexts where the capacity is unknown, DC-QIM methods achieve provably better performance than previously proposed additive spread-spectrum methods, which do not reject interference from the host signal, and generalized low-bit(s) modulation methods. These cases are discussed in [1], along with practical implementations of DC-QIM and QIM systems.

References

[1] B. Chen, *Design and Analysis of Digital Watermarking, Information Embedding, and Data Hiding Systems.* PhD thesis, MIT, Cambridge, MA, June 2000.

[2] M. H. M. Costa, "Writing on dirty paper," *IEEE Trans. on Info. Thy.*, vol. 29, pp. 439–441, May 1983.

[3] P. Moulin and J. A. O'Sullivan, "Information-theoretic analysis of information hiding," Preprint, Oct. 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Relationship between Quantization and Distribution Rates of Digitally Watermarked Data

Damianos Karakos
Department of Electrical and Computer Engineering
University of Maryland
College Park, MD 20742, USA
e-mail: karakos@eng.umd.edu

Adrian Papamarcou
Department of Electrical and Computer Engineering
University of Maryland
College Park, MD 20742, USA
e-mail: adrian@eng.umd.edu

Abstract — **We consider a watermarking system where 2^{nR_W} distinct Gaussian watermarks are embedded in respective copies of an n-dimensional i.i.d. Gaussian image. Copies are distributed to customers in digital form, using R_Q bits per image dimension. We establish the rate region for the pair (R_Q, R_W) such that (i) the average quadratic distortion between the original image and each distributed copy is no more than a specified level; and (ii) the error probability in decoding the embedded watermark in the distributed copy approaches zero asymptotically in n.**

I. Problem Formulation

Recently, there have been some information-theoretic approaches to the analysis of watermarking systems. Of particular interest is [1], which gives a general expression for the maximum rate of the set of messages that can be hidden within a host data set subject to a distortion constraint, as well as the requirement that the message withstand a deliberate attack aimed to destroy it.

In this paper, we study a related problem that combines source and channel coding in a watermarking framework. This problem is motivated by the following scenario. A data distributor (e.g., a news agency) has to deliver an information sequence I^n (e.g., a digital image) to $M_n = 2^{nR_W}$ customers, such that each customer receives a different watermarked version of I^n. To that end, the agent creates M_n watermarks $X^n(1), \ldots, X^n(M_n)$ independently of I^n, and uses them to generate the watermarked copies $Y^n(k) = I^n + X^n(k)$, $k = 1, \ldots, M_n$. Due to bandwidth limitations, the agent compresses the watermarked data at a rate of R_Q bits per image dimension subject to a fidelity criterion prior to distribution.

For security purposes as well as for maximum usability, we assume that both the quantization and the reconstruction of the image are *independent* of the choice of the watermark set. In addition, the agent who generated the image should be able to discern which watermark is present in a digital image with a low probability of error P_e (e.g., in case an authenticator needs to track down the initial owner of an illegally distributed image). Therefore, watermarks and source codewords have to be designed in such a way that knowledge of the watermark set and the original data is enough for detecting reliably the watermark in a compressed, watermarked image.

The main result of this paper is the determination of the allowable rates R_Q and R_W for the above system, under the following assumptions: (i) I^n is i.i.d. $\mathcal{N}(0, P_I)$, (ii) the watermarks $X^n(1), \ldots, X^n(M_n)$ are generated i.i.d. $\mathcal{N}(0, P_X)$ with $P_X < P_I$, and (iii) the distortion constraint $n^{-1}E[\|I^n - \hat{Y}^n\|^2] \leq D$ is met ($\hat{Y}^n$ is the quantized version of Y^n). Unlike the case in [1], here we consider a single fidelity criterion, namely the resultant distortion between the original data sequence and the watermarked/quantized data. Also, while quantization degrades the original image, it cannot be construed as a malicious attack of the type modeled in [1]. In our case, data compression and watermarking are cooperative (not competing) schemes, and must be optimized jointly.

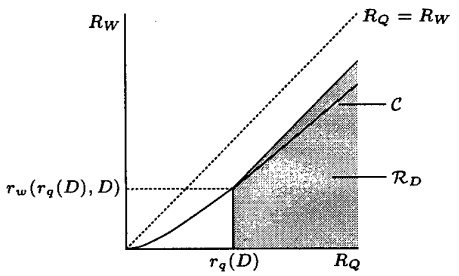


Fig. 1: For any distortion constraint D, the shaded area represents the region $\mathcal{R}_D$ of achievable pairs (R_Q, R_W). As D varies, the minimum source coding rate $r_q(D)$ and the maximum corresponding watermarking rate $r_w(r_q(D), D)$ parametrically define curve $\mathcal{C}$.

II. Results

The coding theorem that establishes the bounds on R_Q and R_W consists of two parts. The forward theorem demonstrates the existence of a source code for $\hat{Y}^n$ and an i.i.d. Gaussian random code for the watermark set such that the distortion constraint is satisfied and the probability of error P_e is arbitrarily small, as long as (R_Q, R_W) belongs to some region $\mathcal{R}_D$. The converse theorem shows that if an arbitrary source code and an i.i.d. Gaussian watermark code jointly satisfy the distortion constraint and yield an asymptotically vanishing P_e, then (R_Q, R_W) must lie in $\mathcal{R}_D$. We proved that $\mathcal{R}_D$ is characterized as follows:

$$R_Q \geq r_q(D) \triangleq \frac{1}{2}\log\left(\frac{P_I^2}{(P_I + P_X)D - P_I P_X}\right)$$

$$R_W \leq r_w(R_Q, D) \triangleq R_Q - \frac{1}{2}\log\left(\frac{P_I}{D}\right)$$

where $\frac{P_I P_X}{P_I + P_X} < D \leq P_I$ (all distortion values of interest). The graphical representation of these results is given in Figure 1.

References

[1] J. O'Sullivan, P. Moulin and J. M. Ettinger, "Information Theoretic Analysis of Steganography", in *Proc. IEEE Int. Symp. on Information Theory*, Cambridge, MA, p. 297, Aug. 1998.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On the Gaussian Watermarking Game

Aaron Cohen[1]
Massachusetts Inst. of Technology
77 Mass. Ave., 35-303
Cambridge, MA 02139
e-mail: acohen@mit.edu

Amos Lapidoth
Swiss Federal Inst. of Technology
ETH-Zentrum
CH-8092, Zurich, Switzerland
e-mail: lapidoth@isi.ee.ethz.ch

Abstract — **We compute the value of the watermarking game for a Gaussian covertext and squared-error distortions. Both the public version of the game (covertext known to neither attacker nor decoder) and the private version of the game (covertext unknown to attacker but known to decoder) are treated. Surprisingly, the two versions yield identical values.**

I. Introduction

The watermarking game [1, 2] can model a situation where an original source sequence ("covertext") needs to be copyright-protected before it is distributed to the public. The copyright ("message") needs to be embedded in the distributed version ("stegotext") so that no "attacker" with access to the stegotext will be able produce a "forgery" that resembles the covertext and yet does not contain the embedded copyright message. The watermarking process ("encoding") should, of course, introduce little distortion so as to guarantee that the stegotext closely resembles the original covertext.

Different messages may correspond to different possible owners, versions, dates, etc. of the covertext, and it is thus of interest to study the number of distinct messages that can be embedded if reliable decoding is required from any reasonable forgery. The highest exponential rate at which this number can grow in relation to the covertext size is the coding value of the game. A precise statement of this problem and some proofs can be found in [3].

II. Watermarking model

The watermarking game can be described as follows. A source emits the zero-mean variance-σ_u^2 IID length-n *covertext* sequence $\mathbf{U}$. Independently of $\mathbf{U}$, a copyright *message* W is drawn uniformly over the set $\mathcal{W}_n = \{1, \ldots, \lfloor 2^{nR} \rfloor\}$, where R is the *rate* of the system.

Using a secret key Θ_1, which is independent of $\mathbf{U}$ and W, the *encoder* produces the *stegotext* $\mathbf{X} = \mathbf{X}(\mathbf{U}, W, \Theta_1) \in \mathbb{R}^n$. We require the encoder to satisfy $\frac{1}{n}\|\mathbf{X}-\mathbf{U}\|^2 \leq D_1$, a.s., where $D_1 > 0$ is a given constant called the *encoder distortion level*, and a.s. stands for "almost surely".

The *attacker*, which is assumed to be ignorant of $\mathbf{U}$ and Θ_1, produces a *forgery* $\mathbf{Y} = \mathbf{Y}(\mathbf{X}, \Theta_2) \in \mathbb{R}^n$ based on $\mathbf{X}$ and its own attack key Θ_2. We similarly require the attacker to satisfy $\frac{1}{n}\|\mathbf{Y} - \mathbf{X}\|^2 \leq D_2$, a.s., where $D_2 > 0$ is a given constant called the *attacker distortion level.*

The *decoder* produces an estimate of the message $\hat{W}$. In the *public version* of the game, the decoder only uses the encoder's secret key and the forgery, so that $\hat{W} = \hat{W}(\mathbf{Y}, \Theta_1)$. In the *private version* of the game, the decoder also uses the covertext, so that $\hat{W} = \hat{W}(\mathbf{Y}, \Theta_1, \mathbf{U})$. We consider the probability of error averaged over the covertext, message and both sources of randomness, which is written $\bar{P}_e(n) = \Pr(\hat{W} \neq W)$.

We adopt a conservative approach to the watermarking game and assume that once the watermarking system is employed, its details are made available to the attacker. The attacker can thus optimize for the encoder and decoder. This precludes the decoder from using the maximum-likelihood decoding rule. We thus say that rate R is *achievable* if there exists a sequence of allowable rate-R encoder and decoder pairs such that for any sequence of allowable attackers, $\bar{P}_e(n)$ tends to zero as n tends to infinity.

The value of the game is called the *coding capacity*, and it is the supremum of all achievable rates. We write the coding capacity as $C_{\text{priv}}(D_1, D_2, \sigma_u^2)$ and $C_{\text{pub}}(D_1, D_2, \sigma_u^2)$ for the private and public versions of the game, respectively.

Theorem 1. *For the Gaussian watermarking game,*

$$C_{\text{pub}}(D_1, D_2, \sigma_u^2) = C_{\text{priv}}(D_1, D_2, \sigma_u^2).$$

If the interval

$$\mathcal{A}(D_1, D_2, \sigma_u^2) = \left[\max\left\{D_2, (\sigma_u - \sqrt{D_1})^2\right\}, (\sigma_u + \sqrt{D_1})^2\right],$$

is empty, then $C_{\text{priv}}(D_1, D_2, \sigma_u^2)$ is zero. Otherwise,

$$C_{\text{priv}}(D_1, D_2, \sigma_u^2) = \max_{A \in \mathcal{A}(D_1, D_2, \sigma_u^2)} \frac{1}{2}\log\left(1 + \left(\frac{1}{D_2} - \frac{1}{A}\right)\left(D_1 - \frac{(A - (\sigma_u^2 + D_1))^2}{4\sigma_u^2}\right)\right).$$

If expected rather than a.s. distortion constraints are used, then the coding capacity for both versions is zero.

Note that the optimal A is a root of a cubic equation and hence a closed form solution for the capacity exists. Different capacity results for yet another version of this game with expected distortion constraints and a decoder that knows the attack strategy (ML decoder) have been recently reported in [1].

[1]This research was supported in part by a NSF Graduate Fellowship (A. Cohen) and by the NSF Faculty Early Career Development (CAREER) Program (A. Lapidoth) at MIT. It was conducted in part at the Institute for Signal and Information Processing, ETH.

References

[1] J. A. O'Sullivan, P. Moulin, and J. M. Ettinger, "Information theoretic analysis of steganography," In *Proc. of ISIT*, 1998. See also P. Moulin and J. A. O'Sullivan, "Information-theoretic analysis of information hiding," preprint, 1999, available at http://www.ifp.uiuc.edu/~moulin/paper.html.

[2] N. Merhav, "On random coding error exponents of watermarking systems," *IEEE Trans. on Inform. Theory*, 46(2):420–430, Mar. 2000.

[3] A. Cohen and A. Lapidoth, "On the Gaussian watermarking game," Laboratory for Information and Decision Systems report, LIDS-P-2464, Nov. 1999. See also "On the Gaussian watermarking game," in *Proc. of CISS*, TA4-21–TA4-27, Mar. 2000.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

An Information Theoretic Approach to Metering Schemes

Annalisa De Bonis and Barbara Masucci
Dipartimento di Informatica ed Applicazioni – Università di Salerno
84081 Baronissi (SA), Italy
e-mail: {debonis, masucci}@dia.unisa.it

Abstract — **A *metering scheme* is a method to count the number of clients which visit each server. Naor and Pinkas [1] presented metering schemes which allow to identify servers which are visited by at least a certain number h of clients and is secure against attempts by servers of inflating the count of their visits. In this paper we consider secure metering schemes for *ramp access structures*. We provide lower bounds on the size of the information given to clients and to servers and present a scheme achieving these bounds.**

I. Introduction

We consider a scenario where there are n clients, m servers and an audit agency A whose task is to measure the interaction between the n clients and the m servers in order to count the number of client visits that any server receives. Our scenario contemplates the existence of *corrupt servers* and *corrupt clients* which could cooperate in order to inflate the count of the visits that a corrupt server receives. Naor and Pinkas [1] proposed metering schemes as a mean to prevent servers from inflating the count of their visits. In their schemes any server which is visited by a number of clients larger than or equal to some *threshold* h provides A with a short *proof*. The metering scheme operates for at most τ time frames and during these time frames is supposed to be *secure*. A metering scheme is secure at a certain time frame t if any server visited by less than h clients at that time frame has no information about its proof. In our model the clients receive a certain amount of information from the audit agency and give part of this information to the servers when visiting them. Given the high complexity of such a distribution mechanism, a natural step is to trade complexity for security. Hence, we consider a more flexible situation where a server which receives less than h visits is able to gain some partial information about its proof.

II. Metering Schemes for Ramp Structures

An (n, m, τ, c, s) *metering system* Σ consists of n clients $\mathcal{C}_1, \ldots, \mathcal{C}_n$ and m servers $\mathcal{S}_1, \ldots, \mathcal{S}_m$, which are active for a number τ of time frames and in which c clients and s servers can be corrupt. A *corrupt* server can be assisted by corrupt clients and other corrupt servers in order to inflate the count of its visits. A corrupt client can donate to a corrupt server the whole information it has received from A. A corrupt server can donate to another corrupt server the information that it has so far received from clients. A *ramp structure* indicates a pair of thresholds (ℓ, h), where $1 \leq c \leq \ell < h < n$.

For $i = 1, \ldots, n$, $j = 1, \ldots, m$, $t = 1, \ldots, \tau$, $\mathbf{C}_i$ is the random variable associated with the information given by A to $\mathcal{C}_i$, $\mathbf{C}^t_{i,j}$ is that associated with the information given by $\mathcal{C}_i$ to $\mathcal{S}_j$ during a visit at time frame t, $\mathbf{X}^t_{j,(d_j)}$ is that associated with the information received by $\mathcal{S}_j$ at time frame t assuming it is visited by d_j clients at that time frame, and $\mathbf{P}^t_j$ is that associated with the proof generated by $\mathcal{S}_j$ when it is visited by at least h clients during time frame t and $\mathbf{V}^{[t]}_j$ is that associated with the information received by $\mathcal{S}_j$ in time frames $1, \ldots, t$.

Definition II.1 *Let Σ be an (n, m, τ, c, s) metering system. An (n, m, τ, c, s)* metering scheme *for an (ℓ, h) ramp structure is a distribution protocol of the proofs for the m servers in Σ in such a way that the following properties are satisfied:*

1. $H(\mathbf{C}^t_{i,j}|\mathbf{C}_i) = 0$, $i = 1, \ldots, n$, $j = 1, \ldots, m$, $t = 1, \ldots, \tau$.
2. $H(\mathbf{P}^t_j|\mathbf{X}^t_{j,(d_j)}) = 0$, $d_j \geq h$, $j = 1, \ldots, m$, $t = 1, \ldots, \tau$.
3. $H(\mathbf{P}^t_1, \ldots, \mathbf{P}^t_\beta|\mathbf{C}_1 \ldots \mathbf{C}_c\mathbf{X}^t_{1,(d_1)} \ldots \mathbf{X}^t_{\beta,(d_\beta)}\mathbf{V}^{[t-1]}_1 \ldots \mathbf{V}^{[t-1]}_\beta)$
   $= H(\mathbf{P}^t_1, \ldots, \mathbf{P}^t_\beta)$, $d_j \leq \ell - c$, $j = 1, \ldots, \beta$, $t = 1, \ldots, \tau$.
4. $H(\mathbf{P}^t_1, \ldots, \mathbf{P}^t_\beta|\mathbf{C}_1 \ldots \mathbf{C}_c\mathbf{X}^t_{1,(d_1)} \ldots \mathbf{X}^t_{\beta,(d_\beta)}\mathbf{V}^{[t-1]}_1 \ldots \mathbf{V}^{[t-1]}_\beta)$
   $= \frac{1}{h-\ell}\sum_{j=1}^{\beta}[h - (c + d_j)]H(\mathbf{P}^t_j|\mathbf{P}^t_1 \ldots \mathbf{P}^t_{j-1})$, *where $\mathbf{X}^t_{j,(d_j)}$ is associated with a set of visits to $\mathcal{S}_j$ from d_j clients other than $\mathcal{C}_1, \ldots, \mathcal{C}_c$, $\ell < d_j + c < h$, $j = 1, \ldots, \beta$ and $t = 1, \ldots, \tau$.*

Lower Bounds

Theorem II.2 *Let Σ be an (n, m, τ, c, s) metering system. Let $\mathcal{S}_1, \ldots, \mathcal{S}_s$ denote the corrupt servers. In any metering scheme for the ramp structure (ℓ, h) for Σ, it holds that $H(\mathbf{C}_i) \geq \frac{1}{h-\ell}\sum_{t=1}^{\tau} H(\mathbf{P}^t_1, \ldots, \mathbf{P}^t_s)$, for $i = 1, \ldots, n$.*

Theorem II.3 *Let Σ be an (n, m, τ, c, s) metering system. In any metering scheme for the ramp structure (ℓ, h) for Σ it holds that $H(\mathbf{C}^t_{i,j}) \geq \frac{1}{h-\ell}H(\mathbf{P}^t_j)$, for any $i = 1, \ldots, n$, $j = 1, \ldots, m$, and $t = 1, \ldots, \tau$.*

A Scheme Achieving our Lower Bounds

Our scheme is a generalization of Shamir's scheme [2].

Initialization: The audit agency A chooses $h-\ell$ polynomials $P_1(y), \ldots, P_{h-\ell}(y)$ over $GF(q)$, where q is a prime number larger than $n+h-\ell$. For $r = 1, \ldots, h-\ell$, $P_r(y)$ has degree $s\tau - 1$. Let $f_1, \ldots, f_{h-\ell}$ be preselected elements of $GF(q)$ distinct from $1, \ldots, n$. Let $Q(x, y)$ be a random bivariate polynomial over $GF(q)$ of degree $h-1$ in x and degree $s\tau-1$ in y, such that $Q(f_r, y) = P_r(y)$, for $r = 1, \ldots, h - \ell$ (It is easy to construct such a random polynomial by using Langrange polynomials.). Hence, A sends to each client $\mathcal{C}_i$ the univariate polynomial $Q(i, y)$, which is of degree $s\tau - 1$.

Regular Operation: When the client $\mathcal{C}_i$ visits the server $\mathcal{S}_j$ in time frame t, it sends to $\mathcal{S}_j$ the value $Q(i, j \circ t)$. The argument $j \circ t$ denotes the concatenation of j and t, and we assume that $j \circ t$ is in $GF(q)$ and that no distinct two pairs (j, t) and (j', t') are mapped to the same element.

Proof Generation: If the server $\mathcal{S}_j$ has been visited by at least h different clients in time frame t, then it can perform a Lagrange interpolation and reconstruct the polynomial $Q(x, j \circ t)$. Then, it computes $Q(f_r, j \circ t)$ for $r = 1, \ldots, h - \ell$. The resulting $(h - \ell)$-tuple $(P_1(j \circ t), \ldots, P_{h-\ell}(j \circ t))$ constitutes the proof that the server sends to the audit agency.

References

[1] M. Naor and B. Pinkas, "Secure and Efficient Metering", *Eurocrypt '98.*

[2] A. Shamir, "How to Share a Secret", *Commun. of the ACM*, 22, pp. 612–613, 1979.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Point Process Channel and Capacity of The Exponential Server Queue

Rajesh Sundaresan[1]
Qualcomm Inc., 385 Reed St.,
Santa Clara, CA 95051 USA
e-mail: rajeshs@qualcomm.com

Abstract — **We give a conceptually simple proof for the capacity of the exponential server queue. Our proof links the timing channel to the point-process channel with complete feedback. This point-process approach enables us to bound capacities of timing channels that arise in multiserver queues, queues in tandem, and other simple configurations.**

The capacity of the exponential server queue with service rate μ packets per second is $e^{-1}\mu$ nats per second [1]. The capacity of the point-process channel with maximum input intensity μ points per second, and no background intensity, is also $e^{-1}\mu$ nats per second (cf.[2],[3]). Furthermore, in both channels, the capacity does not increase in the presence of complete feedback. In [1], the connection between both channels in the presence of complete feedback was discussed briefly. In [4], this connection was further explored. It was shown that any strategy on the exponential server channel can be mapped to an equivalent strategy that uses feedback on the point-process channel. This observation implies that the capacity of the exponential server channel is upperbounded by the capacity of the point-process channel with complete feedback, i.e., $e^{-1}\mu$ nats per second.

From [1], we know that $e^{-1}\mu$ nats per second is indeed achievable on the exponential server queue. In other words, although the exponential server queue is only a particular case of a point-process channel with feedback, it attains the point-process channel capacity. In this paper, we provide insight on why there is no loss in capacity.

To see the connection between the queue and the point-process channel, fix a sequence of arrivals denoted by the counting process $x = (x_t : t \in [0,T])$. Let $(Y_t : t \in [0,T])$ be the corresponding counting process of departures from the single-server queue of service rate μ packets per second. Then the state process $(Q_t = x_t - Y_t : t \in [0,T])$ indicates the number of packets in the queue as a function of time. Furthermore, the departure process $(Y_t : t \in [0,T])$ is a self-exciting Poisson process with rate $\lambda = (\lambda_t = \mu 1\{Q_{t-} > 0\} : t \in (0,T])$. Indeed, if $Q_{t-} = 0$, no packet can depart at time t $(\in (0,T])$ and the instantaneous rate of the departure process is 0. If $Q_{t-} > 0$, at least one packet is in the system at $t-$. Due to the memoryless property of exponential service times, the residual time for the next departure is exponentially distributed with mean $1/\mu$ seconds, independent of the past, i.e., the instantaneous rate of the departure process is μ at time t.

It is well-known that the sample function density (which plays the role of probability density) given input x, is $p(x,y)$, where

$$p(x,y) \triangleq \exp\left\{\int_0^T [\log(\lambda_t)\, dy_t - \lambda_t\, dt]\right\}. \qquad (1)$$

Furthermore, for a given probability measure on the input space, the normalized mutual information is

$$\frac{1}{T} I_T(X;Y) = \frac{1}{T} E \int_0^T dt\ \left[\phi(\lambda_t) - \phi\left(\hat{\lambda}_t\right)\right], \qquad (2)$$

where $\hat{\lambda}_t = E[\lambda_t | (Y_s : s \in [0,t))]$, for each $t \in [0,T]$, and $\phi(u) = u \log u$, (see [2], [3], [5]). We take $\phi(0) = 0$. Note that $\hat{\lambda}_t$ is an estimate of the rate of the departure process given prior departures.

We can show the existence of codes that have vanishing probability of error (as the observation interval T increases without bound) at rate $e^{-1}\mu$ nats per second. Here, for brevity, we only argue that there is an input probability measure such that the normalized mutual information equals the upperbound $e^{-1}\mu$ nats per second. The input measure should induce the following properties to attain the upperbound.

(a) $\lambda_t = 0$ or μ.

(b) $(1/T)\int_0^T dt\ E[\lambda_t] = e^{-1}\mu$.

(c) λ_t should be independent of prior departures $(Y_s : s \in [0,t))$, and $E[\lambda_t]$ should be a constant over time, i.e., $\hat{\lambda}_t = e^{-1}\mu$.

Let the input probability measure be a Poisson process with rate $e^{-1}\mu$ packets per second. Let the queue be in equilibrium at $t = 0$. We then have an $M/M/1$ queueing system. Property (a) holds because λ_t is μ times an indicator function. Property (b) follows from ergodicity of the state process and the fact that the queue is nonempty with probability e^{-1}. Property (c) holds by Burke's theorem (for e.g., [5, V.T1]); the state of the queue Q_t is independent of prior departures $(Y_s : s \in [0,t))$ and therefore so is λ_t.

The point-process approach via (1), (2) and the filtering techniques of [5] (to provide estimates of queue size) can be used to find achievable rates of some simple networks of exponential servers. In [6], lower bounds on the capacities of multiserver queues and two queues connected in tandem are provided.

[1] This work was supported in part by the National Science Foundation under Grant NCR-9523805 002

References

[1] V. Anantharam and S. Verdú, "Bits through queues", *IEEE Trans. Inform. Theory*, vol. IT-42, pp.4-18, Jan. 1996.

[2] Y.M. Kabanov, "The capacity of a channel of the Poisson type, *Theory Prob. Appl.*, vol. 23, pp.143-147, 1978.

[3] M.H.A. Davis, "Capacity and cutoff rate for Poisson-type channels", *IEEE Trans. Inform. Theory*, vol. IT-26, pp.710-715, Nov. 1980.

[4] R. Sundaresan and S. Verdú, "Robust decoding for timing channels", *IEEE Trans. Inform. Theory*, col. IT-46, pp.405-419, Mar. 2000.

[5] P. Brémaud, *Point Processes and Queues: Martingale Dynamics*, Springer-Verlag, New York, 1981.

[6] R. Sundaresan, *Coded Communication over Timing Channels*, Doctoral dissertation, Princeton University, Princeton, NJ, Sept. 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

The Jamming Game for Packet Timing Channels

James Giles and Bruce Hajek[1]
Department of Electrical and
Computer Engineering and the
Coordinated Sciences Laboratory
University of Illinois at
Urbana-Champaign
Urbana, Illinois, 61801 USA
e-mail:
{j-giles,b-hajek}@uiuc.edu

Abstract — **This work focuses on covert timing channels, in which information is conveyed in the timing of packets. Jamming strategies and coding strategies are developed for various timing channel models.**

I. Introduction

Information can be conveyed covertly using the timing of packet transmissions, where the usage is covert because by design and common usage, information in packet communication networks is conveyed only by the bits within the packets. While there is no apparent way to completely eliminate covert timing channels in a reliable communications system (e.g. [1]), a delay device can be added to the channel to jam covert timing communication. With an appropriate coding and decoding scheme, a timing channel coder can still reliably communicate in the presence of a jammer. For various channel models and delay constraints on the jammer, the game between the jammer and the coder is explored.

II. Assumptions

We assume that the mean number of packets per unit time transmitted by the coder is constrained such that for a large fixed time, T, the total number of arrivals is at most λT with probability one. We take $T \to \infty$ and write $\bar{I}$ for mutual information per unit time. The coder is aware of the delay constraints placed on the jammer, but is not aware of the actual strategy employed by the jammer. We assume that no feedback is given to the coder.

The jammer can choose any delay strategy, including strategies that change the packet ordering, subject to constraints on the delay. However, the jammer cannot insert duplicate or additional packets since this might impact the underlying packet communication system. The delay constraints that we consider for jammers include a Maximum-Delay-Less-than-D (MDLD) constraint, an Average-Delay-D (ADD) constraint, and a Maximum-Buffer-Size-B (MBB) constraint.

III. Channel Models

A continuous time packet model and a discrete time packet model are considered.

In the continuous time packet model, there are no lower bounds on the spacing between initiations of packet transmissions so the coder or the jammer can send multiple packets in a single instant. The only restriction on the continuous time packet model is that neither the coder nor the jammer can split a packet.

In the discrete time packet model, time is slotted and both the coder and the jammer can transmit zero or one packets in each time slot. The discrete time packet model is a tractable way to introduce a lower bound on the interpacket spacing.

Two more models are introduced to facilitate analysis. These models have fluid flows rather than packet streams.

IV. Results

We look for jamming strategies, $\tilde{Q}$, that satisfy $\max_X \bar{I}(X,\tilde{Q}) = \min_Q \max_X \bar{I}(X,Q)$, and coding strategies $\tilde{X}$, that satisfy $\min_Q \bar{I}(\tilde{X},Q) = \max_X \min_Q \bar{I}(X,Q)$ where $\bar{I}(X,Q)$ represents the mutual information per unit time between X and the output of jammer Q when X is the input.

For the set of MDLD jammers in the continuous time packet model, we have found a saddlepoint coding and jamming strategy, with mutual information rate $\frac{1}{D}H(\text{Geo}_0(\lambda D))$. For an ADD jammer in the continuous time fluid model, we have shown that the mutual information rate for a saddlepoint is between $0.55/D$ bits per unit delay and $4/D$ bits per unit delay, if a saddlepoint exists. For a MBB jammer in the discrete time packet model, we have upper and lower bounds on the mutual information rate for a saddlepoint that are within a factor of 2. The min-max and max-min capacities of the fluid models are shown to dominate those of the packet models for several scenarios.

For many of our results we assume that the coder and decoder have access to a source of common randomness (they choose a code without the jammer's knowledge), and that the coder and decoder have access to a common clock. However, for particular constraints and models, such as a MDLD constraint in the continuous time packet model, we have coding schemes that do not depend on these assumptions.

V. More Information

For more information and a complete paper see: http://www.comm.csl.uiuc.edu/~hajek.

References

[1] I. S. Moskowitz and M. H. Kang. Covert channels-here to stay? In *Proceedings of COMPASS '94*, pages 235–243, June 1994.

[1]James Giles is supported by a Department of Defense NDSEG Fellowship. This work was also supported by the National Science Foundation under Grant ANR-99-80544.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Information transmission over a finite buffer channel

Suhas N. Diggavi Matthias Grossglauser
AT&T Shannon Laboratories,
180 Park Avenue, Bldg 103,
Florham Park NJ 07932, USA.
{suhas,mgross}@research.att.com

Abstract — **We study information transmission through a finite buffer channel modeled as a concatenation of a discrete memoryless channel and a finite state erasure channel. The state of the erasure channel is determined by the buffer occupancy upon arrival of the transmission symbol; an erasure occurs when an input arrives to a full buffer. We show that the capacity of the channel depends on the long-term loss probability of the buffer and the capacity of the DMC. Thus, even though the channel itself has memory, the capacity apparently depends only on the stationary loss probability of the buffer. We also show that delayed feedback does not help in this channel. We also study the channel as a deletion channel where we do not know where the erasures have occurred.**

I. Summary

We propose a channel abstraction for the finite-buffer channel and study its capacity. This model is motivated by packet-switched networks, where a packet is queued in a finite buffer on each router along its path through the network. A packet can be dropped because of buffer overflow, or corrupted due to transmission errors. We *do not* consider coding in inter-arrival times in this abstraction[1]. Note that the sender may have control over the long-term packet arrival rate, which affects the loss process at the buffer; however, there is no side information transmitted using the arrival process.

We formulate this problem as transmission over a finite state channel where the transitions of the finite state channel occur due to arrivals and departures of packets to the buffer. The model considered resembles the problem of transmission through finite state channels studied extensively [2]. But one of the differences is that the state process need not be Markovian (see Figure I). In this paper we consider only a single user's packets arriving at the buffer and the buffer state is affected by the arrivals of that user.

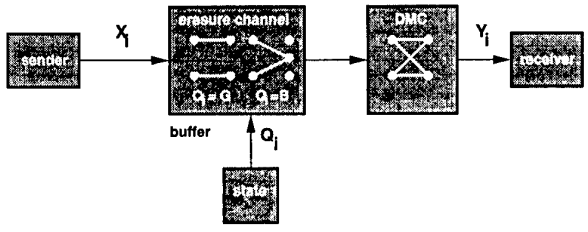


Figure 1: Finite-state channel model.

We first consider the problem where the receiver knows when a packet is dropped. In practice, this is done using a sequence number associated with packets. Later we study the channel where this is not known and model it as a deletion channel. Under regularity conditions on the state transition process we can prove a coding theorem for the proposed channel model [3]. We show that though this channel has memory, the capacity is determined by the long term stationary loss probability of the buffer. That is, the capacity is the product of the capacity of the DMC and that of the long term probability of a packet getting through. This shows that even though the finite buffer channel has complicated memory, its capacity behavior is akin to a simple erasure channel.

Proposition I.1 *Under mixing and asymptotic mean stationarity conditions on the state process $\{Q_i\}$, the capacity of the finite buffer channel is given by,*

$$C = \lim_{n\to\infty} C_n = C_0 \lim_{n\to\infty} \frac{1}{n}\sum_{i=1}^{n} \mathbb{P}\{Q_i \neq B\}, \qquad (1)$$

where B denotes the full buffer state and C_0 is the capacity of the DMC. Furthermore, capacity can be achieved by an i.i.d. input process $\{X_i\}$.

This capacity is expressed in bits per packet. This can be translated to a transmission rate (bits/second) by taking into account the packet arrival process, based on some ergodic conditions on the arrival process. Note that the average packet arrival rate can be chosen to maximize this transmission rate.

We also studied the case where there is feedback available from the channel output to the transmitter, delayed by at least one symbol. We showed that feedback in this case does not improve the channel capacity even though the channel could have complicated memory[2].

Finally we study a model of transmission in the absence of sequence numbers on the packets. This can be studied as a deletion channel. Similar problems have arisen in the context of transmission in the presence of synchronization errors, studied in [4] among others. This is a difficult problem in general and we study specific deletion models and develop some bounds for achievable performance.

References

[1] Venkat Anantharam and Sergio Verdú, "Bits through Queues," *IEEE Transactions on Information Theory*, vol. 42, number 1, pp. 4–18, January 1996.

[2] Robert G. Gallager, *Information theory and reliable communications*, John Wiley and Sons, New York, 1968.

[3] Robert M. Gray, *Entropy and Information Theory*, Springer-Verlag, New York, 1990.

[4] V I. Levenshtein, "Binary codes capable of correcting deletions, insertions and reversals," *Soviet Physics - Doklady*, vol. 10, number 8, pp. 707–710, February 1966.

[1] This is conjectured due to the result in [1] that coding in inter-arrival times is unnecessary when the alphabet size of the transmitted symbol is large (packet sizes in current networks range from a few tens of bytes to a few thousand). Though this was proved in the context of infinite buffer channels, we believe that this is true in our case as well.

[2] Note that in our model, feedback is only used for channel coding; we assume that the packet arrival process does not depend on feedback. If we remove this assumption, we are in the realm of congestion control, and schemes can be developed that achieve higher throughput. We have not addressed that problem here.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Output distribution of the Burrows-Wheeler transform[1]

Karthik Visweswariah
T. J. Watson Research Center
IBM, NY, USA
kv1@watson.ibm.com

Sanjeev Kulkarni
Dept. of Elec. Eng.
Princeton University, USA
kulkarni@ee.princeton.edu

Sergio Verdú
Dept. of Elec. Eng.
Princeton University, USA
verdu@ee.princeton.edu

Abstract — **The Burrows-Wheeler transform is a block-sorting algorithm which has been shown empirically to be useful in compressing text data. In this paper we study the output distribution of the transform for i.i.d. sources, tree sources and stationary ergodic sources. We can also give analytic bounds on the performance of some universal compression schemes which use the Burrows-Wheeler transform.**

I. Introduction

Burrows and Wheeler [2] proposed a lossless transformation which they showed (with empirical evidence) to be useful for the lossless compression of data. Recently there has been increasing interest in understanding and improving the performance of data compression algorithms using the Burrows-Wheeler transform (BWT). From empirical evidence [2] it appears that compression methods using this transform achieve better performance than Lempel-Ziv techniques, while not being computationally as intensive as compression methods using statistical modeling techniques. While there has been a large amount of empirical evidence to show the efficacy of the transform (e.g., [2], [3]), the analysis of the compression efficiency of methods based on the transform has received less attention. Sadakane [5], Arimura and Yamamoto [6], Balkenhol and Kurtz [4] and Effros [1] have provided the first steps in this direction.

In this paper we investigate the joint distribution at the output of the Burrows-Wheeler transform. For various classes of input sources, we show that the output distribution of the transform is approximately memoryless and piecewise stationary, in the sense that the normalized divergence between the output distribution and a memoryless and piecewise stationary distribution is small. Thus coding schemes that are good for memoryless, piecewise stationary sources can be used to give good coding performance. We also derive bounds on the coding rate for some data compression algorithms that use the BWT. The schemes that we analyze were also analyzed in [1] where bounds were obtained on average code length. The bounds we give are on individual sequences.

II. Main Result

We now introduce some notation so that we can precisely state our main result. We consider a Markov process $\mathbf{X}$ which is a Markov source taking values in A and the set of states $\mathcal{S}$ is a complete and prefix-free subset of A^*. Let $|\mathcal{S}| = k$ and label the states $s_1, s_2, \ldots, s_k$ in lexicographic order. We assume that the Markov source is irreducible and aperiodic. Let the steady state probability of a state $s \in \mathcal{S}$ be denoted by $\pi(s)$ and $P(a|s)$ denote the probability that $a \in A$ occurs when we are in state $s \in \mathcal{S}$. Let $C(i) = \sum_{j=1}^{i} \pi(s_j)$. We will show that the divergence between the output distribution and a memoryless, piecewise stationary distribution with $k-1$ transitions is small. Let $T_1, T_2, \ldots, T_{k+1}$ be integers defined by $T_i = \lfloor C(i-1)n \rfloor + 1$. Note that $C(0) = 0$ and so $T_1 = 1$. Let us now define a memoryless distribution Q^n with $k-1$ changes in distribution, by

$$Q^n(y^n) = \prod_{j=1}^{k} \prod_{i=T_j}^{T_{j+1}-1} P(y_i|s_j).$$

We show that the output distribution is close to the distribution Q^n.

Theorem 1 *Consider a tree source for which $P(a|s) > 0$ for all $a \in A$, $s \in \mathcal{S}$ with entropy rate H. Let X^n be the output of the tree source in steady state, $Y^n = \phi_{\mathrm{BWT}}(\mathcal{R}(X^n))$ and P_{Y^n} denote the distribution of Y^n. Then*

$$\frac{1}{n} D(P_{Y^n} || Q^n) \leq \frac{c}{\sqrt{n}}$$

for some constant c, where $\mathcal{R}$ is a map from a string to its reverse and ϕ_{BWT} is a map from a string to the string part of its Burrows-Wheeler Transform.

The assumption that $P(a|s) > 0$ for all a, s can be removed and a result similar to the one above can be given. A result similar in spirit to the one above can also be shown for stationary ergodic sources.

Finally, we mention that we have also analyzed various methods to compress the the output of the BWT and obtained bounds on their performance. These results are like those in [1] except that we obtain results for individual sequences.

[1] This work was partially supported by the National Science Foundation under Grants NYI Award IRI-9457645 and NCR 9523805

References

[1] M. Effros, "Universal lossless source coding with the Burrows Wheeler transform," in *Proc. Data Compression Conference*, Snowbird, UT, 1999, pp. 178–187.

[2] M. Burrows and D. J. Wheeler, "A block-sorting lossless data compression algorithm," Tech. Rep. 124, Digital Systems Research Center, 1994.

[3] M. Nelson, "Data compression with the Burrows-Wheeler transform," *Dr.Dobb's Journal*, pp. 46–50, September 1996.

[4] B. Balkenhol and S. Kurtz, "Universal lossless data compression based on the Burrows Wheeler Transformation: Theory and Practice," Tech. Rep. 98-069, Universitat Bielefeld, 1998, http://www.mathematik.uni-bielefeld.de/sfb343/preprints/.

[5] K. Sadakane, "On optimality of variants of block-sorting compression," in *Proceedings Symposium on Information Theory and its applications*, Matsuyama, Japan, December 1997, pp. 357–360.

[6] M. Arimura and H. Yamamoto, "Asymptotic optimality of the block sorting data compression algorithm," *IEICE Transactions on fundamentals of electronics communications and computer sciences*, pp. 2117–2122, October 1998.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Statistical Imaging and Complexity Regularization

Pierre Moulin and Juan Liu[1]
Univ. of Illinois, Beckman Institute and ECE Dept
405 N. Mathews Ave., Urbana, IL 61801
{moulin,j-liuf}@ifp.uiuc.edu

Abstract — **We apply complexity regularization to statistical ill-posed inverse problems in imaging. We formulate a natural distortion measure in image space and develop nonasymptotic bounds on estimation performance in terms of an index of resolvability that characterizes the compressibility of the true image. These bounds extend previous results that were obtained under simpler observational models.**

I. Statement of the Problem

In imaging problems such as tomography, astronomical imaging, ultrasound imaging, radar imaging, forensic science, and image restoration, a statistical model relating the observations to the underlying image is often available [1]. Consider a penalized-likelihood approach to statistical imaging: $\hat{f}(y) = arg\min_f[-\ln p(y|f) + \mu\Phi(f)]$, where $p(y|f)$ is the conditional density relating the observations $y \in \mathcal{Y}$ to the unknown image $f \in \mathcal{F}$, and $\Phi(f)$ is the regularization functional, which penalizes "unlikely" estimates and stabilizes the ML estimator. The regularization parameter μ controls the trade-off between the log-likelihood term and the regularization penalty. The choice of $\Phi(f)$ depends on available *a priori* knowledge. L^1, Besov, total-variation and robust smoothness penalties are state of the art in image processing.

In this paper, we investigate the choice of complexity measures for the regularization penalty $\Phi(f)$. Such penalties favor estimates with low complexity in a data compression sense. Compared to the more standard L^2, L^1 and Besov penalties, complexity regularization penalizes unlikely estimates in a more flexible way, as complexity measures may be based on rather sophisticated, possibly implicit, flexible probability models. The complexity–regularization criterion is stated as $\hat{f}(y) = arg\min_{f\in\Gamma}[-\ln p(y|f) + \mu L(f)]$, where Γ is a discrete set of candidate images, informally referred to as a *codebook*. Complexity is measured by a codelength $L(f)$ associated with each $f \in \Gamma$. Codewords should satisfy Kraft's inequality $\sum_{f\in\Gamma} e^{-L(f)} \leq 1$. The MDL principle [2] is a familiar instance of complexity regularization, where $\mu = 1$.

The use of MDL and complexity regularization has found theoretical justification in a variety of inference problems [3, 4, 5]. Extending such analysis to problems of interest in imaging entails several technical difficulties. First, the data are not identically distributed. Second, the bounds derived by extension of the techniques in [3, 4, 5] are often too large to be useful in practical imaging problems.

Consider the relative–entropy loss $d(f^*, f) = \frac{1}{N}D(p(y|f^*)||p(y|f))$ for $f^*, f \in \mathcal{F}$, where $D(p||q) = \int_{\mathcal{Y}} p(y)\ln\frac{p(y)}{q(y)}\,dy$. The estimation risk is defined as $r(f^*, \hat{f}) = E[d(f^*, \hat{f})]$, where the expectation is with respect to $p(y|f^*)$. Relative-entropy loss is the natural choice to characterize the performance of penalized likelihood estimators. This loss becomes a squared-error loss for additive white Gaussian noise (AWGN) models, and an I-divergence loss for Poisson noise models. If $d(f^*, f)$ for some $f \neq f^*$, then f^* is not identifiable. For ill-posed problems, the class of images $\mathcal{C}_\epsilon(f^*) = \{f : d(f^*, f) \leq \epsilon\}$ is large for any $\epsilon > 0$.

II. Upper Bounds on Estimation Performance

We now give upper bounds on $d(f^*, \hat{f})$. See [6] for more details. Define the index of resolvability $R_\mu(f^*) = \min_{f\in\Gamma}\left[d(f^*, f) + \mu\frac{L(f)}{N}\right]$, $f^* \in \mathcal{F}$. This quantity describes how well f^* can be approximated in the relative-entropy sense by a moderately-complex element of the codebook Γ.

The upper bounds are essentially proportional to the index of resolvability, with a very small ($O(1/N)$) additive constant. For the AWGN model $y_i = f_i^* + w_i$, $1 \leq i \leq N$, $w_i \sim$ i.i.d. $\mathcal{N}(0, \sigma^2)$, we have Theorem 1 below, which applies to any $\mu \geq 1$ (recall $\mu = 1$ is the MDL choice). The techniques used in [4], which do not require knowledge of the noise distribution but assume that Bernstein's inequality applies to that distribution, provide looser bounds.

Theorem 1 *For any $\mu > 1$ and $\eta > 0$, the loss of the complexity-regularized estimator $\hat{f}$ under the AWGN model satisfies $Pr\left[d(f^*, \hat{f}) \leq \frac{\mu+1}{\mu-1}R_\mu(f^*) + \frac{2\mu^2\ln\frac{1}{\eta}}{(\mu-1)N}\right] \geq 1 - \eta$. The risk is upper-bounded by $E[d(f^*, \hat{f})] \leq \frac{\mu+1}{\mu-1}R_\mu(f^*) + \frac{2\mu^2}{(\mu-1)N}$.*

For some non-Gaussian models, under certain large-sample assumptions, log-likelihood ratios are asymptotically normally distributed, and tight inequalities can be obtained again. Under some additional technical assumptions, the first bound of Theorem 1 still applies, provided that the inequality is replaced with an asymptotic inequality.

[1]Work supported by the National Science Foundation under award MIP-9732995 (CAREER), by ARO under contract numbers ARO DAAH-04-95-1-0494 and ARMY WUHT-011398-S1, and by DARPA under Contract F49620-98-1-0498, administered by AFOSR.

References

[1] J. A. O'Sullivan, R. E. Blahut, and D. L. Snyder, "Information-theoretic image formation," *IEEE Trans. on Info. Theory*, vol. 44, pp. 2094-2123, Oct. 1998.

[2] J. Rissanen, *Stochastic Complexity in Statistical Inquiry*. Singapore: World Scientific, 1989.

[3] A. R. Barron and T. M. Cover, "Minimum complexity density estimation," *IEEE Trans. on Information Theory*, vol. 37, pp. 1034-1054, July 1991.

[4] A. R. Barron. "Complexity regularization with application to artificial neural networks," in *Nonparametric Function Estimation and Related Topics* (G. Roussas, ed.), (Kluwer, Dordrecht), pp. 561–576, NATO ASI Series, 1991.

[5] D. S. Modha and A. Masry, "Minimum complexity regression estimation with weakly dependent observations," *IEEE Trans. on Information Theory*, vol. 42, Nov. 1996.

[6] P. Moulin and J. Liu, "Statistical Imaging and Complexity Regularization," to appear in *IEEE Trans. Info Thy*, Special issue on information-theoretic imaging, Aug. 2000.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

ISI Channel Estimation Using Complementary Sequences

Predrag Spasojević [1]
Dept. of Electrical and Computer Engineering
WINLAB, Rutgers University
94 Brett Road, Piscataway, NJ 08854-8058, USA
e-mail: spasojev@winlab.rutgers.edu

Costas N. Georghiades
Dept. of Electrical Engineering,
Texas A&M University,
College Station, TX 77843-3128, USA
e-mail: georghia@ee.tamu.edu

Abstract — **Pairs of binary pilot symbol sequences are jointly designed to minimize an introduced merit factor whose minimization leads to the reduction in Crámer-Rao lower bound (CRLB) for the "two-sided" intersymbol interference channel estimation.**

I. Introduction

It is a common approach to periodically insert known symbols in order to reliably estimate the channel parameters prior to detection. In the case of time-variant multi-path fading channels where the path delay spread is on the order of several symbols or larger, pilot symbol blocks that span the channel memory need to be inserted. In deriving optimal, or some decision-feedback detection and channel estimation algorithms, the signal is frequently assumed to be quasi-static in an interval encompassing a number of transmitted symbols.

Here it is assumed that both pilot symbol blocks (preamble and postamble) that frame a block of data (see Fig. 1) are employed for estimation of the (quasi-static) channel coefficients pertaining to a particular data block. This approach we term "two-sided" channel estimation. It is shown the constructed optimal sequences for two-sided channel estimation require that the two pilot symbol blocks framing a data block almost always differ and, therefore, the optimal signaling requires alternating periodically inserted training blocks.

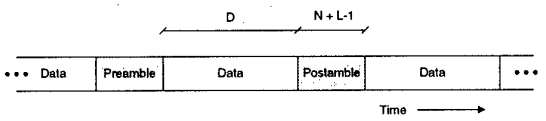


Figure 1: Two-sided pilot symbol block insertion.

II. Signal Model

A symbol-spaced received signal is assumed and a normalized block of received samples over which the channel is (quasi-)static can be expressed as follows:

$$\mathbf{r} = \mathbf{A}\mathbf{h} + \mathbf{n}.$$

$\mathbf{n}$ is a sample vector of a white circular Gaussian noise process with a two-sided PSD N_0/E_s, where E_s is the symbol energy; $\mathbf{h}$ is a Lx1 vector of channel coefficients. $\mathbf{A}$ is a Toeplitz matrix corresponding to the transmitted sequence of symbols from $\{+1,-1\}$ of the form $\mathbf{A} = \left[\mathbf{P}_1^T\mathbf{D}^T\mathbf{P}_2^T\right]^T$. $\mathbf{P}_1$ and $\mathbf{P}_2$ are N by L pilot symbol Toeplitz submatrices consisting of only preamble and postamble symbol sequences of length $(N+L-1)$ and no data symbols $\mathbf{D}$ is a $D+L-1$ by L submatrix that holds all the data symbols. $N \geq L$ is assumed so that each pilot-symbol block spans the channel.

III. Mini-Max Criterion and Optimal Sequences

The CRLB of the two-sided ML channel estimation based on the "two-sided" pilot-symbol matrix $\mathbf{P} = \left[\mathbf{P}_1^T\mathbf{P}_2^T\right]^T$ is

$$\frac{N_0}{E_s}\mathrm{tr}\{\mathbf{R}^{-1}\},$$

where $\mathbf{R} = \mathbf{P}^H\mathbf{P} = \mathbf{P}_1^H\mathbf{P}_1 + \mathbf{P}_2^H\mathbf{P}_2$. Instead of directly minimizing $\mathrm{tr}\{\mathbf{R}^{-1}\}$ we suggest minimizing the largest absolute sum

$$\rho_{\max} = \max_i \sum_{j\neq i} |\rho_{ij}|,$$

where ρ_{ij} is the ij-th element of $\mathbf{R}$. Minimization of $\rho_{\max}$ is equivalent to the minimization of the maximum Gerschgorin disc radius of $\mathbf{R}$. Thus, it attempts a reduction in the eigenvalue spread and forces the matrix $\mathbf{R}$ to have a form which is as close as possible to the diagonal form.

When $\rho_{\max} = 0$ the Grammian matrix $\mathbf{R} = 2N \cdot \mathbf{I}$, where $\mathbf{I}$ is the identity matrix. The ML channel estimation achieves the absolute minimum variance lower bound $\frac{N_0}{E_s}\frac{L}{2N}$. Binary odd- and even-periodic complementary sequence ([1], [3]) pairs achieve $\rho_{\max} = 0$ and, thus, are optimal for "two-sided" ISI channel estimation for even $N \geq L$.

When N is odd, $\rho_{\max} = 0$ (and the CRLB $\frac{N_0}{E_s}\frac{L}{2N}$) cannot be achieved. For a subset of odd N "almost-complementary" periodic binary sequence pairs achieve the minimum possible $\rho_{\max} = 2\lfloor\frac{L-1}{2}\rfloor$. Additionally, "good" sequence pairs achieve $\rho_{\max} = 4\lfloor L/2\rfloor < 2N$ which assures that $\mathbf{R}$ is non-singular and, consequently, that the CRLB is bounded. Given a generator sequence $\mathbf{u} = [u_0,\ldots,u_{N-1}]$, both almost-complementary and good sequences pairs ($\mathbf{p}_1 = [p_{1,0},\ldots,p_{1,N+L-2}]$, $\mathbf{p}_2 = [p_{2,0},\ldots,p_{2,N+L-2}]$) are formed as follows:

$$p_{1,k} = u_{k \bmod N} \quad \textit{and} \quad p_{2,k} = (-1)^k p_{1,k},$$

for $0 \leq k \leq N+L-2$. For almost complementary sequences the periodic autocorrelation of the periodic extension $\mathbf{u}^p$ of $\mathbf{u}$ is $|\sum_{k=0}^{N-1} u_k^p u_{k+l}^p| = 1$ for $0 < l \leq N-1$. That is, they can be formed from m-, Barker, Legendre, and twin-prime sequences (see e.g. [2]). "Good" sequences are based on sequences given in [4] whose periodic autocorrelation has values in $\{1,-3\}$.

References

[1] M. J. E. Golay, "Complementary series," *IEEE Trans. on Information Theory*, vol. 7, pp. 82–87, April 1961.

[2] S. W. Golomb, *Shift Register Sequences.* Laguna Hills, California: Aegean Press, 1982.

[3] H. D. Luke, "Binary odd-periodic complementary sequences," *IEEE Trans. on Information Theory*, vol. 43, pp. 365 – 367, January 1997.

[4] A. M. Boehmer, "Binary pulse compression codes," *IEEE Trans. on Information Theory*, vol. 13, pp. 156–167, April 1967.

[1]This work was supported in part by the NSF grant NCR-9314221.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Some Aspects of Multivariate Rayleigh and Exponential Distributions

Ranjan K. Mallik
Department of Electrical Engineering
Indian Institute of Technology, Delhi
Hauz Khas, New Delhi 110016, India
e-mail: rkmallik@ee.iitd.ernet.in

Abstract — **We obtain a general form of the multivariate Rayleigh and exponential probability density functions (p.d.f.s) when these are generated by correlated Gaussian random variables. A general expression for the exponential characteristic function (c.f.) is also derived.**

I. Introduction

Multivariate Rayleigh and exponential distributions [1] arise in the performance analysis of digital modulation schemes over correlated Rayleigh fading channels using diversity combining techniques. The Rayleigh distribution is a special case of the Nakagami distribution, while the exponential is a special case of the gamma. A bivariate Rayleigh case [2] has been applied to fading channels using dual diversity [3]. A multivariate gamma case has been dealt with in situations in which the c.f. has a specific form [4][5]. Here we obtain a general form of the multivariate Rayleigh and exponential p.d.f.s when these are generated by correlated Gaussian random variables. We also derive a general expression for the exponential c.f.

II. Probability Density Functions

Consider zero-mean real Gaussian $L \times 1$ random vectors $\underline{X}_c \triangleq \left[\ X_{c_1}, \cdots, X_{c_L}\ \right]^T$, and $\underline{X}_s \triangleq \left[\ X_{s_1}, \cdots, X_{s_L}\ \right]^T$, with covariance matrices $\underline{K}_{cc}$ and $\underline{K}_{ss}$ and cross-covariance matrix $\underline{K}_{cs}$, such that

$$\mathbf{E}\left[X_{c_i}^2\right] = (\underline{K}_{cc})_{ii} = (\underline{K}_{ss})_{ii} = \mathbf{E}\left[X_{s_i}^2\right],$$
$$\mathbf{E}[X_{c_i} X_{s_i}] = (\underline{K}_{cs})_{ii} = 0, \quad i = 1, \ldots, L.$$

In other words, X_{c_i} and X_{s_i} are i.i.d. Gaussian for each i.

Define random variables $\alpha_1, \ldots, \alpha_L$, $\Phi_1, \ldots, \Phi_L$ as $\alpha_i \triangleq \left(X_{c_i}^2 + X_{s_i}^2\right)^{\frac{1}{2}}$, $\Phi_i \triangleq \tan^{-1}\left(\frac{X_{s_i}}{X_{c_i}}\right)$, $i = 1, \ldots, L$. Let $\underline{\alpha} = \left[\ \alpha_1, \cdots, \alpha_L\ \right]^T$ be a *Rayleigh random vector*. Denote

$$\underline{K} = \begin{bmatrix} \underline{K}_{cc} & \underline{K}_{cs} \\ \underline{K}_{cs}^T & \underline{K}_{ss} \end{bmatrix}, \quad \underline{K}^{-1} = \begin{bmatrix} \underline{A} & \underline{B} \\ \underline{B}^T & \underline{D} \end{bmatrix},$$

such that $\underline{A} = [A_{ij}]_{i,j=1}^L$, $\underline{B} = [B_{ij}]_{i,j=1}^L$, $\underline{D} = [D_{ij}]_{i,j=1}^L$. From the joint p.d.f. of $(\underline{X}_c, \underline{X}_s)$, the p.d.f. of $\underline{\alpha}$, which is *multivariate Rayleigh*, is given by

$$f_{\underline{\alpha}}(\underline{u}) = \frac{\prod_{i=1}^{L} u_i}{(\det(\underline{K}))^{\frac{1}{2}}} \frac{1}{(2\pi)^L} \int_{-\pi}^{\pi} \cdots \int_{-\pi}^{\pi} \exp\left(-\frac{1}{2} g(\underline{u}, \underline{\phi})\right) d\phi_1 \cdots d\phi_L,$$

$\underline{u} \geq \underline{0}$, where

$$g(\underline{u}, \underline{\phi}) = \sum_{i=1}^{L} \left(A_{ii}\cos^2\phi_i + D_{ii}\sin^2\phi_i + 2B_{ii}\cos\phi_i\sin\phi_i\right) u_i^2 + \sum_{\substack{i,j=1 \\ i \neq j}}^{L} \left(A_{ij}\cos\phi_i\cos\phi_j + D_{ij}\sin\phi_i\sin\phi_j + 2B_{ij}\cos\phi_i\sin\phi_j\right) u_i u_j,$$

$$\underline{u} = [u_1, \cdots, u_L]^T, \quad \underline{\phi} = [\phi_1, \cdots, \phi_L]^T. \tag{1}$$

The p.d.f. of the *exponential random vector* $\underline{\gamma}$ given by $\underline{\gamma} = \left[\ \gamma_1, \cdots, \gamma_L\ \right]^T = \left[\ \alpha_1^2, \cdots, \alpha_L^2\ \right]^T$ can be obtained from the multivariate Rayleigh p.d.f. (1).

When $\underline{X}_c + \jmath\underline{X}_s$ is a circular complex Gaussian random vector satisfying $\mathbf{E}\left[(\underline{X}_c + \jmath\underline{X}_s)(\underline{X}_c + \jmath\underline{X}_s)^T\right] = \underline{0}$, we have, for $i, j = 1, \ldots, L$,

$$A_{ij} = A_{ji} = D_{ji} = D_{ij}, \quad B_{ij} = -B_{ji} \text{ when } i \neq j, \quad B_{ii} = 0$$

in (1), and therefore

$$g(\underline{u}, \underline{\phi}) = \sum_{i=1}^{L} A_{ii} u_i^2 + 2 \sum_{\substack{i,j=1 \\ i<j}}^{L} \left(A_{ij}^2 + B_{ij}^2\right)^{\frac{1}{2}} u_i u_j \cos\left(\phi_i - \phi_j + \theta_{ij}\right),$$

where $\theta_{ij} = \tan^{-1}[B_{ij}/A_{ij}]$. Further, if $\underline{X}_c$ and $\underline{X}_s$ are i.i.d. zero-mean Gaussian random vectors, then $\underline{B} = \underline{0}$.

III. Characteristic Function

Although it is difficult to obtain a closed-form expression for the multivariate Rayleigh c.f., the multivariate exponential c.f. can be expressed in closed form as

$$\Psi_{\underline{\gamma}}(\jmath\underline{\omega}) = \left\{\det\left(\underline{I}_L - 2\jmath\mathrm{diag}(\underline{\omega})\underline{K}_{cc}\right)\right\}^{-\frac{1}{2}} \times \left\{\det\left(\left[\underline{I}_L - 2\jmath\mathrm{diag}(\underline{\omega})\underline{K}_{ss}\right] + 4\mathrm{diag}(\underline{\omega})\underline{K}_{cs}^T \times \left[\underline{I}_L - 2\jmath\mathrm{diag}(\underline{\omega})\underline{K}_{cc}\right]^{-1}\mathrm{diag}(\underline{\omega})\underline{K}_{cs}\right)\right\}^{-\frac{1}{2}}, \tag{2}$$

where $\underline{I}_L$ is the $L \times L$ identity matrix.

If we have the condition that $\underline{X}_c$ and $\underline{X}_s$ are i.i.d. random vectors, then the c.f. (2) simplifies to

$$\Psi_{\underline{\gamma}}(\jmath\underline{\omega}) = \left\{\det\left(\underline{I}_L - 2\jmath\mathrm{diag}(\underline{\omega})\underline{K}_{cc}\right)\right\}^{-1}. \tag{3}$$

The gamma c.f.s in [4][5] reduce to (3) when the gamma parameter equals unity.

IV. Bivariate Case

By putting $L = 2$ and the circularity condition in (1), we obtain the bivariate Rayleigh p.d.f. of [2]. The structure of this p.d.f. does not simplify further in the case of i.i.d. generating vectors $\underline{X}_c$ and $\underline{X}_s$.

References

[1] S. Kotz and N. L. Johnson, editors-in-chief, *Encyclopedia of Statistical Sciences, vol. 6.* New York: Wiley, 1985, pp. 43–66.

[2] C. C. Tan and N. C. Beaulieu, "Infinite series representations of the bivariate Rayleigh and Nakagami-m distributions," *IEEE Trans. Commun.*, vol. 45, no. 10, pp. 1159–1161, Oct. 1997.

[3] M. K. Simon and M.-S. Alouini, "A unified performance analysis of digital communication with dual selective diversity over correlated Rayleigh and Nakagami-m fading channels," *IEEE Trans. Commun.*, vol. 47, no. 1, pp. 33–43, Jan. 1999.

[4] Q. T. Zhang, "Exact analysis of postdetection combining for DPSK and NFSK systems over arbitrarily correlated Nakagami channels," *IEEE Trans. Commun.*, vol. 46, no. 11, pp. 1459–1467, Nov. 1998.

[5] P. Lombardo, G. Fedele, and M. M. Rao, "MRC performance for binary signals in Nakagami fading with general branch correlation," *IEEE Trans. Commun.*, vol. 47, no. 1, pp. 44–52, Jan. 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

A New Decoding Algorithm for Spherical Codes Generated by Binary Partitions of Symmetric Pointsets

John K. Karlof
Mathematics Department
The University of North Carolina
Wilmington, NC 28403 U.S.A.
e-mail: karlof@uncwil.edu

Guodong Liu
Intelligent Information Systems
Durham, NC 27713
U.S.A.

Abstract — **Recently, Ericson and Zinoviev presented a clever, new construction for spherical codes for the Gaussian channel using ideas of code concatenation and set partitioning. This family of new spherical codes is generated from sets of binary codes using equally spaced symmetric pointsets on the real line. The family contains some of the best known spherical codes in terms of minimum distance. In this paper, we present a new decoding algorithm for this family of spherical codes which is more efficient than maximum likelihood decoding. At low signal to noise ratios, it is 99% equivalent to maximum likelihood but takes just 2% of the computational time.**

I. Ericson and Zinoviev's Code Construction

In [1], a clever construction of spherical codes, some with optimal minimum distance, for Gaussian channel is presented. We include those same results in a modified form for even alphabet size.

The code construction begins with choosing K even and the code alphabet $L_K = \{\pm\frac{1}{2}, \pm\frac{3}{2}, \ldots, \pm\frac{K-1}{2}\}$ Let $\overline{L}_K = \{0, 1, \ldots, \frac{K}{2} - 1\}$ and form a tree with node labels, $\Gamma = \overline{L}_K \cup \{\lambda, *\}$, using the following rules.

1. The root of the tree is λ and λ is adjacent only to $*$. Every internal node has exactly two children except for λ . We will say that node λ is at level -1, $*$ is at level 0, the children of $*$ are at level 1, etc.
2. The children of $*$ are labeled 0 and 1 with 0 being the left child.
3. For succeeding levels, say level k, the left child of a node at level $k-1$ is labeled the same as its parent and the right child is chosen from $\overline{L}_K$ so that the sum of the labels of the two children is $2^k - 1$. If that is impossible, the node at level $k-1$ is a leaf.

We choose a binary code for each internal node of the tree. Codes at level k will be designated C_γ^k where γ is the label of the corresponding node on the tree. An arbitrary code, C_λ^{-1} of length n is chosen for node λ. A code, C_*^0 of length n and constant weight w_* is chosen for node $*$. Suppose internal node γ at level $k-1, (k \geq 1)$ has internal node left child γl and internal node right child γr and code C_γ^{k-1} of length n_γ^{k-1} and constant weight w_γ^{k-1} has been chosen for node γ. Then code $C_{\gamma l}^k$ of length $n_{\gamma l}^k = n_\gamma^{k-1} - w_\gamma^{k-1}$ and constant weight $w_{\gamma l}^k$ is chosen for node γl and code $C_{\gamma r}^k$ of length $n_{\gamma r}^k = w_{\gamma r}^{k-1}$ and constant weight $w_{\gamma l}^k$ is chosen for node γr.

The tree of binary codes and alphabet L_K is used to form a spherical code, X, of length n for the Gaussian channel. For each collection of codewords $\{c_\gamma^i \in C_\gamma^i \mid C_\gamma^i$ is a code in the tree$\}$, we form a codeword $x \in X$ in the following manner. Suppose the tree has $m+1$ levels of internal vertices. We form a $m+1$ by n matrix where the rows are labeled by the levels of the tree and the $i^{\underline{th}}$ row consists of the codewords chosen from the codes at that level in the tree. We arrange the codewords in row i in a special manner depending on the binary codes chosen in the $i^{\underline{th}}$ level of the tree. The binary sequences that are the columns of the matrix correspond to the components of x and there is an algorithm to translate each binary sequence into an element of L_K.

The following result relating the minimum distance of the spherical code X to the minimum distances of the binary codes $\{C_\gamma^k | k \geq -1\}$ appears in [1].

Theorem 1 *Let X be the spherical code generated by Ericson and Zinoviev's construction using the binary codes $\{C_\gamma^k | k \geq -1\}$. Let d_γ^k be the minimum Hamming distance of the code C_γ^k and let d^2 be the (unnormalized) minimum squared distance of X. Then $d^2 \geq min\{d_\gamma^k \cdot 4^{k+1} | k \geq -1\}$.*

II. Decoding Algorithm

The first step is to perform binary partitions of the alphabet L_K which we now simply denote L. Our partitions are made in a tree structure and have the same properties of partitions of the set $Z + \frac{1}{2}$ in [1]. We call the elements of the partition subalphabets.

Let $x = (x_1, x_2, \ldots, x_n) \in X$, where $x_1, x_2, \ldots, x_n \in L$, be the word obtained by Ericson and Zinoviev's construction from the code words $c^1, c^2, \ldots, c^s$ of $C^1, C^2, \ldots, C^s$, respectively. Suppose d_i = minimum Hamming distance of C^i and ρ_i = squared minimum distance of the subalphabets at level i. Let $y = (y_1, y_2, \ldots, y_n), y_j \in R$ be the received word corrupted by noise. The new decoding algorithm consists of s steps, where each step finds $c^i, i = 1, \ldots, s$. At each step, the decoding algorithm is divided into an inner code decoding algorithm and an outer code decoding algorithm. The outer code decoding algorithm incorporates Forney's idea of error and erasure decoding and Zinoviev's idea of distance decoding.

Theorem 2 *Let x be the transmitted codeword constructed by the binary codewords $c^1, c^2, \ldots, c^i, \ldots, c^s$ and y the received word corrupted by noise. Assume that the first code vectors $c^1, c^2, \ldots, c^{i-1}$ have been found correctly, if $\rho(x, y) < d_i\rho_i/4$ then the decoding algorithm will correctly decode to codeword c^i.*

References

[1] T. Ericson and V. Zinoviev, "Spherical Codes Generated by Binary Partitions of Symmetric Pointsets," IEEE Trans. Inform. Theory, vol. 41, no.1, Jan 1995.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Slepian-Type Codes on a Flat Torus

Sueli I. R. Costa
Institute of Mathematics
UNICAMP, 13081-970
Campinas - SP, Brazil
sueli@ime.unicamp.br

Edson Agustini[1]
PhD. Program of Institute of
Mathematics, UNICAMP,
13081-970, Campinas, Brazil
agustini@ime.unicamp.br

Marcelo Muniz[2]
PhD. Program of Institute of
Mathematics, UNICAMP,
13081-970 Campinas, Brazil
muniz@ime.unicamp.br

Reginaldo Palazzo Jr.[3]
Department of Telematics
UNICAMP, 13081-970
Campinas - SP, Brazil
palazzo@dt.fee.unicamp.br

Abstract — **Quotients of $\mathbb{R}^2$ by translation groups are metric spaces known as flat tori. We start from codes which are vertices of closed graphs on a flat torus and, through an identification of these with a 2-dimensional surface in a 3-dimensional sphere in $\mathbb{R}^4$, we show such graph signal sets generate $[M, 4]$ Slepian-type cyclic codes for $M = a^2 + b^2$; $a, b \in \mathbb{Z}$, $\gcd(a, b) = 1$. The cyclic labeling of these codes corresponds to walking step-by-step on a (a, b)-type knot on a flat torus and its performance is better when compared with either the standard M-PSK or any cartesian product of M_1-PSK and M_2-PSK, $M_1 M_2 = M$.**

Group codes introduced by D. Slepian and developed in subsequent articles are defined as finite sets on a n-dimensional sphere generated by the action of a group of orthogonal matrices. Geometrically uniform codes introduced by Forney [3] generalize this concept by considering also infinite sets of points in Euclidean space having a transitive symmetry group. We consider here like in [2] those codes extended to the wider context of metric spaces: a signal set $S \subset X$ is a geometrically uniform code if and only if for s, t in S there is an isometry f (depending on s, t) in X such that $f(s) = t$ and $f(S) = S$. We still have all the highly desirable properties that come from homogenity: same distance profile, congruent Voronoi regions and same error transmition probability for each codeword. The metric space considered here is the flat torus, obtained by identifying the opposite sides of a parallelogram based on plane vectors $\vec{u}$ and $\vec{v}$. If G is the group generated by translations by $\vec{u}$ and $\vec{v}$, the correspondent flat torus can be defined as the quotient $T_{(a,b)} = \mathbb{R}^2/G$, what means that the equivalence relation in the plane is given by

$$P' \approx P \Leftrightarrow P - P' = m\vec{u} + n\vec{v} : m, n \in \mathbb{Z}.$$

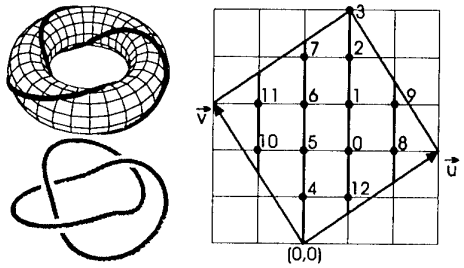
A flat torus can be visualized as a standard torus in 3-space, but it can distinguished from the later by being perfectly homogeneous and locally like a piece of plane (flat). It can only be realized isometrically as a 2-dimensional surface in $\mathbb{R}^4$ which is contained in a 3-dimensional sphere.

Starting from the squared lattice $\mathbb{Z}^2$ on the plane, we induce a closed graph $\Gamma_{(a,b)}$ of $M = a^2 + b^2$ vertices on the flat torus generated by the rotated square based on vectors $\vec{u} = (a, b)$ and $\vec{v} = (-b, a)$, $a, b \in \mathbb{Z}$. An isometry which embeds this flat torus in 3-dimensional sphere in $\mathbb{R}^4$ can be induced by:

$$\varphi(x, y) = \frac{\sqrt{a^2+b^2}}{2\pi}\left(\cos\frac{2\pi(ax+yb)}{a^2+b^2}, \sin\frac{2\pi(ax+yb)}{a^2+b^2}, \cos\frac{2\pi(ay-xb)}{a^2+b^2}, \sin\frac{2\pi(ay-xb)}{a^2+b^2}\right).$$

0-2-3 This work was supported by FAPESP grants 97/12269-0 (1); 97/12270-8 (2); 95/4720-8 (3); CNPq grant 301416/85-0 (3).

Vertical translation by one in the plane corresponds to an orthogonal 4×4 matrix g which is product of rotations of angles $\frac{2\pi b}{a^2+b^2}$ and $\frac{2\pi a}{a^2+b^2}$. If a and b are coprimes, this matrix generates a cyclic group of order $a^2 + b^2$, what means all plane vertices can be reached starting from any point and going north. This labeling can be identified with a walking step-by-step along a (a, b)-type knot on T. The included figure illustrates the homogeneous 13 vertex closed graph on the flat torus (right side) labeled by $\mathbb{Z}_{13}$ through vertical translation walking on a $(2, 3)$-type (trefoil) knot (left side).



Formally, considering the above notation for $T_{(a,b)}$, $\Gamma_{(a,b)}$ and g, we can state:

Proposition 1 *The vertices of the unit squared graph $\Gamma_{(a,b)}$ on the flat torus $T_{(a,b)}$ correspond through the isometry induced by φ to a Slepian-type code S of order $M = a^2 + b^2$ on the 3-sphere of radius $\frac{\sqrt{a^2+b^2}}{\sqrt{2}\pi}$ in $\mathbb{R}^4$. Besides:*

(i) If $\gcd(a, b) = 1$, S is generated by a single point $\varphi((0,0)) = \frac{\sqrt{a^2+b^2}}{\sqrt{2}\pi}(1, 0, 1, 0)$ through the action of the cyclic group $\langle g \rangle = \mathbb{Z}_{a^2+b^2}$ (g is the direct product of rotations whose angles are $\frac{2\pi b}{a^2+b^2}$ and $\frac{2\pi a}{a^2+b^2}$).

(ii) If $\gcd(a, b) = m > 1$, S is generated by a minimal set $\varphi((k, 0))$, $0 \leq k \leq m - 1$ through the cyclic group $\langle g_1 \rangle = \mathbb{Z}_{(a^2+b^2)/m}$, that is, this subgroup of orthogonal 4×4 matrices that acts transitively on S is isomorphic to $\mathbb{Z}^2_{(a^2+b^2)/m}$.

(iii) The minimal Euclidean distance, d, in $\mathbb{R}^4$ between two Slepian-signals, considering the 3-sphere re-scaled to radius one is given by:

$$d^2 = 2\left(\sin^2\left(\frac{\pi b}{a^2+b^2}\right) + \sin^2\left(\frac{\pi a}{a^2+b^2}\right)\right).$$

In [1] a graph metric approach for geometrically uniform codes of any order M on flat tori is summarized.

References

[1] Agustini, E. et alli. "Codes in Regular Graphs on a Flat Torus". *Proceedings of ISIT-2000.*

[2] Costa, S. I. R. et alli. "The Symmetry Group of $\mathbb{Z}_q^n$ in the Lee Space and the $\mathbb{Z}_q$-Linearity". *Lecture Notes in Computer Science*. Springer Verlag. New York. n.1255, pp.66-77, 1997.

[3] Forney, D. "Geometrically Uniform Codes". *IEEE Transactions on Information Theory*, vol. 37, n.5, 1991, pp. 1241-1260.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Decoding Algorithm for the High-Dimensional Discrete Torus Knot Code

Masayasu Hata and Eisaku Yamaguchi
Aichi Prefectural University
Ibaragabasama, Kumabari,
Nagakute-cho Aichi 480-1198, Japan
e-mail: hata@ist.aichi-pu.ac.jp

Ichi Takumi
Nagoya Institute of Technology
Gokiso-cho, Shouwa-ku,
Nagoya Aichi 466-5588, Japan
e-mail: takumi@ics.nitech.ac.jp

Yuuichi Hamasuna and Kenji Miyoshino
DDS Inc.
Otohbashi, Nakagawa-ku,
Nagoya Aichi 466-5588, Japan
e-mail: hamasuna@dds.co.jp

Abstract — **A majority logic decoding is suitable for ASIC design of the proposed code. Four-dimensional size-five code of 625-bit length was implemented on a VLSI and attained an operation speed up to 50Mbps and 32-bit burst correction.**

I. Introduction

Recent code requirements are to attain high-speed operation and robust correction ability for a long burst error. The proposed code has been constituted on a geometric structure of high-dimensional cube or torus. The code properties are dependent not on the Hamming distance but on the geometric size and symmetry of the code. The characteristics and uncorrectable symmetrical solid are discussed. This paper describes a majority logic decoding which is suitable for high-speed operation on an ASIC.

II. Code Principle

A code block is wound up to a small symmetrical cube with size m on a high n-D code space. Each digit of the cube satisfies n parity check relations of each axial check line containing m digits. The transmission rate becomes n power of one minus m-inverse. Both edges of each parity line are identified as a closed circle by way of the parity function. So, the cube topologically becomes an n-dimensional discrete torus. If the size of the cube is smaller than the geometrical mesh modeled by the inverse of the mean error rate of the channel, the cube could be transferred through the channel without serious errors. The transmission order of the code digits varies in many ways with the winding of the torus knot. For a high-D long-block code, errors introduced by a channel become random on each parity line, since the errors are dispersed by the winding, regardless of random or burst errors. The correction ability for both errors is roughly given as follows; correctable burst length versus block size or the mean error rate for random are equally given by a function of the inverse of the code size m.

III. Decoding Characteristics

The code works efficiently on a majority logic decoding scheme of the number of erroneous parity lines of the said digit. When a digit exceeds the threshold is correctly corrected, the other erroneous digits on the connected parity line come up and are corrected at the next decoding, since the erroneous weights becomes high by one. With this code alone, it is possible to iterate hard decision decoding any number of times because the parity line does not lose the function due to the preceding correction. Through iteration, error successively decreases to the probabilistic limit given by the symmetrical error solid. The error remains uncorrected for the high-D error solid, for example, the symmetric n-D solid is undetected on account of the parity function, so the $n-1$D solid can be detected but not corrected because the error position is not determined. The half-error symmetrical n-D solid is also uncorrected, since error and true digits are interchanged during each decoding. In order to correct the error solid perfectly, the dimensions of the solid should be two degrees less than the code space dimensions.

IV. VLSI Implementation

The code consists of a simple parity check calculation and the relationship between the parity and the data digits was clearly obtained. A large part of the encoding and decoding processes was built in by adopting wired connection between the memory cells of the VLSI. The majority logic decoding of each cycle in the iteration was performed with just one clock time, excepting one block time delay to receive a full code block. The VLSI architecture resulted in increased code speed. The encoder and decoder circuits of the four-dimensional and five-size 4Dm5 code whose code length is 625 bits and the rate is 0.41 were installed on a 50-kilogate, 0.6 micron rule ASIC.

V. Performance

The code attained high-speed operation up to 50Mbps and robust correction ability for burst error with 7 iterations. The code corrected burst error up to 32 bits in length with zero error. The performance is much better than that of conventional codes, that is, 16 bits for Reed-Solomon code of $(15, 7)$ on $q = 4$, and 4 bits for Viterbi decoding Convolution code with constrain length $K = 7$. The Turbo code with the Log-MAP decoding of 624 bits in length corrects almost 4 bits burst, but fails in the decoding two times out of ten thousand trials. It took the simulation time more than hundred times of that of the proposed code. When the code is evaluated for random errors, the performance for a low-grade decoding bit error rate of ten to the minus 3 to 5 is approximately the same as the Convolution code of rate $R = 7/8$, $K = 7$ with Viterbi decoding. But for higher grade performance of ten to the minus 8 or less, the proposed code shows more coding gain than Viterbi decoding of Convolution code of $R = 1/2$, $K = 7$.

References

[1] Hata M., Yamaguchi E., Ando A. and Takumi I., "High-dimensional discrete torus knot code", Block code p.18, ISIT 1998, Cambridge, MA, USA.

[2] Kuroda S., Yamaguchi E., Takumi I. and Hata M., "A Geometrical decoding algorithm and correcting limit of high-dimensional hyper-cubic ring code — correcting ability in BER of $10^{-2} \sim 10^{-1}$", *IEICE Trans.*, J80-A, 12, Dec. 1997.

[1]This work was supported by the 98 NEDO project of the Ministry of International Trade and Industry of Japan.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Extremal Polynomials for Codes in Polynomial Metric Spaces

Svetla Nikova
Dept. Electr. Eng. ESAT/COSIC
Katholieke Universiteit Leuven
Kardinal Mercierlaan 94
B-3001 Heverlee, Belgium
e-mail:
svetla.nikova@esat.kuleuven.ac.be

Ventsislav Nikov
Dept. of Mathematics and Informatics
Veliko Turnovo University
5000 Veliko Turnovo
Bulgaria
e-mail: vnikov@mail.com

Abstract — **Let $\mathcal{M}$ be a polynomial metric space (PMS) [2] with metric $d(x,y)$ and standard substitution $t = \sigma(d(x,y))$. Any finite nonempty subset C of $\mathcal{M}$ is called a code. A code for which $\sigma(d(x,y)) \leq \sigma(d)$ $(x,y \in C)$ and d is the minimum distance of C is an $(\mathcal{M}, |C|, \sigma)$-code. We will give some properties of the so called test functions for codes and we will improve the Levenshtein bound with polynomials of degree $h(\sigma)+2$ and $h(\sigma)+3$.**

I. Introduction

PMS are *finite* metric spaces represented by P- and Q- polynomial association schemes as well as *infinite* metric spaces, which are the real sphere, the real, complex or quaternions projective space and the Cayley projective plane. On the other hand PMS are distinguished as **antipodal** and **non-antipodal**. Any PMS is connected with a system of constants r_i, a system of orthogonal polynomials $\{Q_i(t)\}$ and **adjacent** system of polynomials $\{Q_k^{a,b}(t)\}$ with roots $-1 < t_{k,i}^{a,b} < 1$, $i = 1, \ldots, k$, ordered in increasing order, $t_k^{a,b} = t_{k,k}^{a,b}$. Most of the properties of $\{Q_k^{a,b}(t)\}$ can be found in [2]. By definition $T_k^{a,b}(x,y) = \sum_{i=0}^{k} r_i^{a,b} Q_i^{a,b}(x) Q_i^{a,b}(y)$. Many bounds for the cardinality of codes and designs were obtained by using the Linear Programming Theorem [2, p.544]. If we denote by $A_{\mathcal{M},\sigma}$ the set of real polynomials which satisfy the conditions of the LP Theorem, then $|C| \leq \Omega(f)$, for $f \in A_{\mathcal{M},\sigma}$. We will investigate the Levenshtein bound $L(\mathcal{M},\sigma)$ for codes, which can be presented in the following form [2]:

$$|C| \leq L(\mathcal{M},\sigma) = \Omega(f^{\sigma}(t)) = \left(1 - \frac{Q_{k-1+\varepsilon}^{1,0}(\sigma)}{Q_k^{0,\varepsilon}(\sigma)}\right) \sum_{i=0}^{k-1+\varepsilon} r_i, \quad (1)$$

where $\varepsilon = 0$ if $t_{k-1}^{1,1} \leq \sigma < t_k^{1,0}$ and $\varepsilon = 1$ if $t_k^{1,0} \leq \sigma < t_k^{1,1}$, and $f^{\sigma}(t) = (t-\sigma)(t+1)^{\varepsilon}(T_{k-1}^{1,\varepsilon}(t,\sigma))^2$ of degree $h(\sigma)$.

II. Test functions and new bound

Boyvalenkov, Danev and Bumova [1] obtain necessary and sufficient conditions for the optimality of $f^{\sigma}(t)$ over $A_{\mathcal{M},\sigma}$, introducing the *test functions* $G_{\sigma}(\mathcal{M}, Q_j)$. They prove that the bound (1) can be improved by a polynomial in $A_{\mathcal{M},\sigma}$ of degree j if and only if $G_{\sigma}(\mathcal{M}, Q_j) < 0$. In [3] we define analogous test functions $G_{\tau}(\mathcal{M}, Q_j)$ for designs.

In this section we use the connections between codes and designs and the corresponding test functions. Applying analogous approach as in [3] we investigate the properties of the test functions for codes and derive an analytical form of the polynomials, which improve the Levenshtein bound. For fixed j, $G_{\sigma}(\mathcal{M}, Q_j)$ is a continuous function of σ and $G_{\sigma}(\mathcal{M}, Q_j) \equiv 0$, when $h(\sigma) \geq j$. We examine the sign of $G_{\sigma}(\mathcal{M}, Q_j)$. Let us consider the interval $I_{h(\sigma)} = [t_{k+\varepsilon-1}^{1,1-\varepsilon}, t_k^{1,\varepsilon})$ and denote $h(t_{k+\varepsilon-1}^{1,1-\varepsilon}) = \tau$. We have $G_{\sigma}(\mathcal{M}, Q_{h(\sigma)+1}) > 0$.

Lemma 1 *If $G_{\tau}(\mathcal{M}, Q_{\tau+2}) \geq 0$ then $G_{\sigma}(\mathcal{M}, Q_{h(\sigma)+2}) > 0$ for $\sigma \in I_{h(\sigma)}$. If $G_{\tau}(\mathcal{M}, Q_{\tau+k}) < 0$ for $k \geq 2$ then there exist $z_0 < t_{k+\varepsilon-1}^{1,1-\varepsilon}$ and $z_1 > t_{k+\varepsilon-1}^{1,1-\varepsilon}$ such that $G_{\sigma}(\mathcal{M}, Q_{h(\sigma)+k}) < 0$ for $\sigma \in [t_{k+\varepsilon-1}^{1,1-\varepsilon}, z_1)$ and $G_{\sigma}(\mathcal{M}, Q_{h(\sigma)+k+1}) < 0$ for $\sigma \in (z_0, t_k^{1,\varepsilon})$.*

In other words there exists an interval $\tilde{I}_{\tau} = (z_0, z_1)$ for σ, containing $t_{k+\varepsilon-1}^{1,1-\varepsilon}$ in which $G_{\sigma}(\mathcal{M}, Q_{\tau+k})$ is negative, i.e. the Levenshtein bound can be improved in this interval using polynomial of degree $\tau + k$, $k \geq 2$.

Corollary 2 *For antipodal PMS the test function $G_{\sigma}(\mathcal{M}, Q_{h(\sigma)+2})$ is positive.*

As a consequence of the above using our results from [3] we conclude that the smallest possible degree of the improving polynomials is $\tau + 2 = h(\sigma) + 2$ or $h(\sigma) + 3$ for non-antipodal spaces and $\tau + 3 = h(\sigma) + 3$ or $h(\sigma) + 4$ for antipodal PMS. Here we present the analytical form of the polynomial which improve the Levenshtein bound in the non-antipodal case.

Theorem 3 *Let $\mathcal{M}$ be non-antipodal PMS, $\tau = h(t_{k+\varepsilon-1}^{1,1-\varepsilon})$ and let us consider the interval $\tilde{I}_{\tau}$. Then the polynomial*

$$\begin{aligned} f^{\sigma}(t;\tau+2) &= (t-\sigma)(t+1)^{\varepsilon} \; [\alpha(T_{k-1}^{1,\varepsilon}(t,\sigma))^2 \\ &+ (\beta_1 T_{k-2}^{1,\varepsilon}(t,\sigma) + \beta_2 T_{k-1}^{0,\varepsilon}(t,\sigma) + T_k^{0,\varepsilon}(t,\sigma))^2], \end{aligned}$$

of degree $\tau + 2$ belongs to $A_{\mathcal{M},\sigma}$ for constants α, β_1, β_2 satisfying certain conditions.

Now using the LP Theorem with the polynomial $f^{\sigma}(t;\tau+2)$ we derive new analytical bound $V(\mathcal{M},\sigma)$.

Theorem 4 *If the conditions of Theorem 3 are satisfied then*

$$|C| \leq V(\mathcal{M},\sigma) = \Omega(f^{\sigma}(t;\tau+2)) \leq L(\mathcal{M},\sigma).$$

Acknowledgments

The authors would like to thank to Peter Boyvalenkov for the very helpful discussions and comments.

References

[1] P.G.Boyvalenkov, D.P.Danev, S.P.Bumova, Upper bounds on the minimum distance of spherical codes, *IEEE Transactions on Information Theory* 42, 1996, 1576-1581.

[2] V.I.Levenshtein, Universal bounds for codes and designs, Chapter 6 in Handbook of Coding Theory, ed. V.Pless and W.C.Huffman, 1998, Elsevier Science B.V., 449-648.

[3] S.I.Nikova, V.S.Nikov, Improvement of the Delsarte bound for τ-designs when it is not the best bound possible, submitted in *Designs Codes and Cryptography.*

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Algebraic Soft-Decision Decoding of Reed-Solomon Codes

Ralf Kötter
University of Illinois at Urbana-Champaign
Urbana, IL 61801, U.S.A.
koetter@shannon.csl.uiuc.edu

Alexander Vardy
University of California at San Diego
La Jolla, CA 92093-0407, U.S.A.
vardy@kilimanjaro.ucsd.edu

Abstract — **A polynomial-time soft-decision decoding algorithm for Reed-Solomon codes is developed. The algorithm is algebraic in nature and builds upon the interpolation procedure proposed by Guruswami and Sudan for hard-decision decoding. Algebraic soft-decision decoding is achieved by means of converting the soft-decision reliability information into a set of interpolations points along with their multiplicities. The conversion procedure is shown to be optimal for a certain probabilistic model. The resulting soft-decoding algorithm significantly outperforms both the Guruswami-Sudan decoding and the generalized minimum distance (GMD) decoding, while maintaining a complexity that is polynomial in the length of the code. Asymptotic analysis for a large number of interpolation points is presented, culminating in a complete geometric characterization of the decoding regions of the proposed algorithm. The algorithm easily extends to polynomial-time soft-decision decoding of BCH codes and codes from algebraic curves.**

I. Introduction

Reed-Solomon (RS) codes are one of the most extensively used families of error-control codes. Since the discovery of these codes four decades ago, a steady stream of work has been devoted to their decoding. Nevertheless, *soft-decision* decoding of Reed-Solomon codes is still essentially out of reach of present-day methods. Indeed, all the known *optimal* soft-decoding algorithms for RS codes are non-algebraic and run in time that scales *exponentially* with the length of the code. On the other hand, all the available polynomial-time algorithms, except for GMD decoding [1], are based mainly on heuristics. Thus, in light of the ubiquity of Reed-Solomon codes, efficient soft-decision decoding of RS codes remains one of the most important problems in coding theory and practice.

II. Algebraic Soft-Decision Decoding

In the full version of this paper [3], we present an efficient soft-decision decoding algorithm for Reed-Solomon codes. The algorithm is algebraic in nature and, for any desired level of performance (within a certain fundamental bound), its complexity is bounded by a polynomial in the codeword length. Our algorithm significantly outperforms both the Guruswami-Sudan [2] decoding and the GMD-based [1] decoding methods. Figure 1 shows the performance of these algorithms for a simple coding scheme: a $(256, 144, 113)$ RS code over GF(256) concatenated with the $(9, 8, 2)$ binary code.

Our algorithm is based on the algebraic interpolation techniques developed by Sudan [2,4]. To achieve soft-decision decoding, we translate the soft-decision reliability information into a set of algebraic constraints. More specifically, given the channel output vector $(y_1, y_2, \ldots, y_n)$ and the a posteriori transition probabilities $\Pr(c_i|y_i)$, we iteratively compute a set of interpolation points along with their multiplicities. We show that, at each step of the computation, this choice of interpolation points is optimal, in a certain precise sense. The complexity of this computation is $O(n^2 \log n)$.

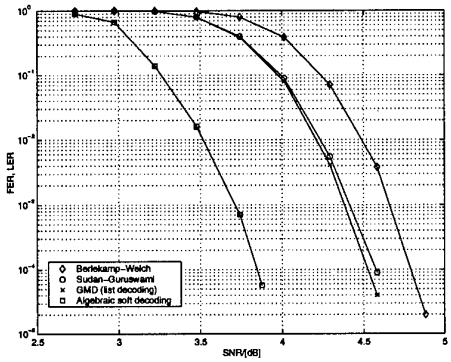


Figure 1. *Performance comparison on an AWGN channel*

The algorithm of Guruswami-Sudan [2,4] is based on algebraic interpolation and factorization techniques that can be implemented efficiently in polynomial time. Our soft-decision decoding procedure inherits these properties of Guruswami-Sudan decoding. One of its most intriguing characteristics of our soft-decoding algorithm is a complexity/performance trade-off that can be chosen freely. Thus the coding gain provided by the Reed-Solomon code can be traded for complexity, in real-time, in any application. Another interesting feature of our algorithm is that it readily extends to the decoding of BCH codes and most algebraic-geometric codes.

We also present asymptotic performance analysis, as the number of interpolation points approaches infinity. The analysis leads to a simple geometric characterization of the (asymptotic) decoding regions of the algorithm. We find that under soft-decision list-decoding, arbitrarily small probability of error is achievable in polynomial time, providing the rate of the code does not exceed a certain constant $\mathscr{C}$ that depends on the channel. Finally, we consider modifications to our algorithm designed to maximize the set of correctable error patterns on the following channels: q-ary symmetric channel, q-ary symmetric channel with erasures, and a simplified q-PSK channel. Surprisingly, our results for the q-ary symmetric channel are stronger than those reported in [2], even though this channel provides no soft-decision information.

References

[1] G.D. Forney, Jr., "Generalized minimum distance decoding," *IEEE Trans. Inform. Theory*, vol. 12, pp. 125–131, April 1966.

[2] V. Guruswami and M. Sudan, "Improved decoding of Reed-Solomon and algebraic-geometric codes," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1755–1764, September 1999.

[3] R. Kötter and A. Vardy, "Algebraic soft-decision decoding of Reed-Solomon codes," preprint.

[4] M. Sudan, "Decoding of Reed-Solomon codes beyond the error correction bound," *J. Complexity*, vol. 12, pp. 180–193, 1997.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Soft Decision Decoding of Reed Solomon Codes

Vishakan Ponnampalam and Branka Vucetic
School of Electrical and Information Engineering
University of Sydney
NSW 20006
Australia
e-mail: {vishakan, branka}@ee.usyd.edu.au

Abstract — **The paper presents a Maximum Likelihood Decoding and a sub-optimum decoding algorithm for Reed-Solomon codes. The proposed algorithms are based on the algebraic structure of RS codes represented in $GF(2)$. Theoretical bounds on the performance are derived and shown to be accurate. The proposed sub-optimum algorithm is seen to have better error performance compared to other sub-optimum decoding algorithms while the new MLD algorithm has significantly lower decoding complexity when compared to other MLD algorithms.**

I. Introduction

Reed-Solomon (RS) codes are a powerful class of maximum separable block codes, suitable for error control on real channels. Algebraic Hard Decision Decoding (HDD) algorithms are widely used for RS codes. It has been shown that Soft Decision Decoding offers 2-3 dB coding gain in excess of HDD. Unfortunately most SDD algorithms proposed in the past have either been of high computational complexity or fail to demonstrate significant performance improvement over HDD. Hence the search for efficient SDD algorithms for RS codes still continues.

Vardy and Beery proposed a MLD algorithm [1] based on the structure of the generator matrix of RS codes represented in $GF(2)$. RS codes can be be represented as a union of cosets. Such partitions into cosets allow a decoding algorithm to be developed. The algorithm is several orders of magnitude lower in complexity compared to trellis decoding for high rate codes up to length 15 and low rate (≤ 0.5) codes of any length.

We present two SDD algorithms based on the same structural properties the Vardy-Beery algorithm uses. Hence the algorithms may be considered as modifications of the Vardy-Beery algorithm. It is shown that a RS codeword is formed by interleaving words chosen (with a certain order) from either a binary BCH code or one of its cosets. This property is used to derive a computationally efficient ML SDD algorithm. The reduction in complexity achieved with reference to the Vardy-Beery algorithm is considerable. The proposed algorithm can be changed into a sub-optimum algorithm, thus trading-off complexity with performance.

II. Decoding

Let $\mathbf{g_{RS}}(X)$ be the generator polynomial of an (N,K) RS code, $\mathbb{C}_{RS}$, over $GF(2^m)$. If α is a primitive element of $GF(2^m)$, $\mathbf{g_{RS}}(X)$ is given by

$$\mathbf{g_{RS}}(X) = \prod_{i=1}^{2t} \left(X + \alpha^i\right) \qquad (1)$$

where $2t = N - K$. Now define an (N,k) binary BCH code, $\mathbb{C}_{BCH}$ with generator polynomial $\mathbf{g_{BCH}}(X)$ with roots $\{\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{2t}\}$ and their cyclotomic conjugates over $GF(2^m)$. The message length k, is less than or equal to K. Define a transformation $\phi : \mathbf{GF(2^m)} \rightarrow \mathbf{GF(2)^m}$ with basis $\{\gamma_0, \gamma_1, \ldots, \gamma_{m-1}\}$. Using this transformation, a code polynomial, $\mathbf{c_{RS}}(X)$ of $\mathbb{C}_{RS}$ is given by:

$$\begin{aligned} \mathbf{c_{RS}}(X) &= \sum_{j=0}^{m-1} \gamma_j \left[\mathbf{c_{BCH}^{(j)}}(X) + \mathbf{l^{(j)}}(X)\right] \\ &= \sum_{j=0}^{m-1} \gamma_j \mathbf{c_{BCH}^{(j)}}(X) + \sum_{j=0}^{m-1} \gamma_j \mathbf{l^{(j)}}(X) \qquad (2) \end{aligned}$$

where $\mathbf{c_{BCH}^{(j)}}(X) \in \mathbb{C}_{BCH}$ and $\mathbf{l^{(j)}}(X)$ is a coset leader polynomial.

We use the above algebraic property to device an efficient decoding algorithm.

III. Simulation Results

The proposed algorithms were applied to a range of Reed-Solomon codes up to length 127 and the minimum Hamming distance up to 7. The simulation results are obtained for antipodal signalling over an AWGN channel. Table 1 gives the required bit energy to noise ratio $\frac{E_b}{N_o}$ to achieve 10^{-5} BER for the proposed algorithms, GMD and the Berlekemp-Massey HDD algorithm. It is observed that the proposed MLD algorithm requires 1.9-3dB lower SNR to achieve the target BER of 10^{-5}, compared to the HDD algorithm. It is also shown in Table 1 that the proposed sub-optimum algorithm achieves near-MLD performance for all codes tested. The loss in performance at BER of 10^{-5} is consistently below 1.0 dB.

RS Code	d_{min}	$\frac{E_b}{N_o}$ at $BER = 10^{-5}$			
		MLD	SOPT	GMD	HDD
(31,29)	3	6.4 dB	6.6 dB	7.9 dB	8.4 dB
(63,61)	3	6.6 dB	6.8 dB	8.1 dB	8.6 dB
(127,125)	3	6.8 dB	7.0 dB	8.4 dB	8.8 dB
(15,11)	5	5.3 dB	5.6 dB	7.2 dB	7.8 dB
(31,27)	5	5.2 dB	5.3 dB	7.2 dB	7.6 dB
(63,59)	5	5.5 dB	6.3 dB	7.6 dB	7.8 dB
(15,9)	7	4.5 dB	5.1 dB	6.9 dB	7.6 dB
(31,25)	7	4.2 dB	5.2 dB	6.7 dB	7.2 dB

Table 1: Required $\frac{E_b}{N_o}$ to achieve BER of 10^{-5} for various codes and decoding algorithms.

References

[1] A. Vardy and Y. Be'ery, "Bit level soft-decision decoding of Reed-Solomon codes" *IEEE Trans. on Inf Thr.* , vol. 39, no. 3, pp. 440-444, 1991.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Recursive decoding of Reed-Muller codes

Ilya Dumer[1]
College of Engineering
University of California at Riverside
Riverside, CA 92521, USA

Kirill Shabunov[1]
College of Engineering
University of California at Riverside
Riverside, CA 92521, USA

Abstract — **We use the Plotkin $(u, u+v)$-construction for general Reed-Muller codes (m,r) and relegate decoding to the two constituent RM codes. First, we use the better protected code (m-1,r-1) to find a subblock v. Then we proceed with the block u from the code (m-1,r). We repeat this recursion on both halves and recalculate the reliabilities of the received symbols. In the end, we perform ML decoding on the biorthogonal codes.**

I. Recursive techniques

Below, general Reed-Muller codes $\mathrm{RM}(r,m)$ are denoted $\left\{ {m \atop r} \right\}$. *Plotkin* construction represents these codes in the form $(u, u+v)$, where $u \in \left\{ {m-1 \atop r} \right\}$ and $v \in \left\{ {m-1 \atop r-1} \right\}$. By splitting both halves, we obtain shorter RM codes until we arrive at the biorthogonal codes $\left\{ {j \atop 1} \right\}$ or single-parity check codes $\left\{ {j \atop j-1} \right\}$.

Now consider the received block $(\widehat{u}, \widehat{u+v})$ corrupted by noise. We first try to find the better protected block v. In hard decision decoding, we use its corrupted version $\widehat{u}+(\widehat{u+v})$. In more general setting, we first use the left half $\widehat{u}$, and find the posterior probability $p'_i = \Pr\{u_i = 0 \mid \widehat{u}_i\}$ of each symbol u_i.

Similarly, we use the right half $\widehat{u+v}$ to find the posterior probability p''_i of any symbol $u_i + v_i$. Then any symbol v_i has posterior probability:

$$p(v_i) = p'_i p''_i + (1-p'_i)(1-p''_i).$$

In Step 1 of our algorithm, we use probabilities $p(v_i)$ to execute soft-decision decoding of vector $\widehat{v}$ into the $\left\{ {m-1 \atop r-1} \right\}$-code. The result of decoding is (presumably correct) codeword v.

After v is found, we have two corrupted copies of vector u, namely $\widehat{u}$ in the left half, and $(\widehat{u+v})+v$ in the right half. Our next goal is to jointly decode both copies. Similarly to Step 1, we use posterior probabilities $p(u_i)$ of symbols u_i. Here we combine the two estimates of u_i obtained on both corrupted copies. Finally, we perform soft decision decoding and find (presumably correct) subblock $u \in \left\{ {m-1 \atop r} \right\}$.

In a general scheme, decoding on the length $n/2$ is again relegated to the shorter codes. On all intermediate steps we only recalculate symbol reliabilities. Maximum likelihood decoding is executed at the end nodes $\left\{ {j \atop 1} \right\}$ and $\left\{ {j \atop j-1} \right\}$. Decoding requires about $O(n \log n)$ operations.

It can be shown that the output bit error rates significantly vary on different end nodes. In particular, the highest (worst) BER is obtained on the node $\left\{ {m-r+1 \atop 1} \right\}$ that is decoded first. An important conclusion is to set the corresponding information bits as zeros. In this way, we improve on the overall performance by taking the subcodes that eliminate a few least protected information bits in the original code $\left\{ {m \atop r} \right\}$.

[1]This work was supported by the NSF grant NCR-9703844.

In asymptotic setting [4], our decoding increasingly outperforms both the majority algorithm and the former recursive techniques [1]-[3] as the block length grows. In particular, for long RM codes of fixed rate, we increase bounded-distance threshold $\ln d$ times and correct most error patterns of weight up to $(d \ln d)/2$. Simulation results presented below show that this improvement starts at very short lengths.

II. Simulation results

Table 1 summarizes simulation results for the RM code $\left\{ {9 \atop 4} \right\}$ of length 512 and dimension 256. We also consider a subcode of dimension 223 and present both bit- (BER) and block (BLER) error rates. The results are compared with the former recursuve technique presented in [3]. Similar results are obtained in Table 2 for RM code $\left\{ {9 \atop 3} \right\}$ of dimension 130 and its subcode of dimension 87.

Table 1. Output error rates for code $\left\{ {9 \atop 4} \right\}$.

SNR (dB)	2	3	4
Recursive [3]	0.9	0.5	0.2
Recursive (new)	0.2	0.03	$2{\cdot}10^{-3}$
BER for subcode	0.05	$3{\cdot}10^{-3}$	$3{\cdot}10^{-5}$
BLER for subcode	0.2	0.02	$2{\cdot}10^{-4}$

Table 2. Output error rates for code $\left\{ {9 \atop 3} \right\}$.

SNR (dB)	2	3	4
Recursive	0.2	0.08	$8{\cdot}10^{-3}$
BER for subcode	0.02	10^{-3}	$3{\cdot}10^{-5}$
BLER for subcode	0.08	$3{\cdot}10^{-3}$	10^{-4}

Further improvements of recursive techniques are presented below for RM code $\left\{ {8 \atop 2} \right\}$ of length 256 and dimension 37. For these (or similar) parameters, our decoding outperforms all suboptimal algorithms known to date.

Table 3. Output bit error rates for RM code $\left\{ {8 \atop 2} \right\}$.

SNR (dB)	1	1.5	2	2.5	3
BER	10^{-2}	$4{\cdot}10^{-3}$	10^{-3}	$2{\cdot}10^{-4}$	$2{\cdot}10^{-5}$
BLER	$4{\cdot}10^{-2}$	10^{-2}	$3{\cdot}10^{-3}$	$5{\cdot}10^{-4}$	$8{\cdot}10^{-5}$

References

[1] S.N. Litsyn, "On decoding complexity of low-rate Reed-Muller codes," Proc. Ninth All-Union Conf. on Coding Theory and Info. Transmission, Odessa, USSR, pp. 202-204, 1988.

[2] G.A. Kabatyanskii, "On decoding of Reed-Muller codes in semicontinuous channels," Proc. Second Int. Workshop "Algebr. and Combin. Coding Theory", Leningrad, USSR, 1990, pp. 87-91.

[3] G. Schnabl and M. Bossert, "Soft-Decision Decoding of Reed-Muller Codes as Generalized Multiple Concatenated Codes," IEEE Trans. Info. Theory, vol. 41, pp. 304-308, 1995.

[4] I. Dumer, "Recursive decoding of Reed-Muller codes," Proc. 37 Annual Allerton Conf. on Commun., Control, and Comp., Monticello, IL, Sept. 23-25, 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Error Performance Analysis for Reliability-Based Decoding Algorithms

Marc Fossorier and Shu Lin[1]
Dept. of Electrical Engineering,
University of Hawaii,
Honolulu, Hawaii 96822, USA
marc<slin>@spectra.eng.hawaii.edu

Abstract — **In this paper, the statistical approach proposed by Agrawal and Vardy to evaluate the error performance of the Generalized Minimum Distance (GMD) decoding is extended to other reliability based decoding algorithms for binary linear block codes, namely Chase-type, combined GMD and Chase-type, and ordered statistic decodings. In all cases, tighter and simplier bounds than previously proposed ones have been obtained with this approach.**

I. Summary

A difficult task related to suboptimum decoding algorithms is their error performance analysis at practical SNR values. It has long been believed that a good criterion to design a suboptimum soft decision decoding algorithm was to prove that the algorithm achieves bounded distance decoding (or is asymptotically optimum). However, recent studies indicate that this simple criterion usually does not reflect the behavior of the algorithm considered at practical SNR values. In particular, an approach based on the union bound is highly misleading and more sophisticated bounding methods are needed.

In [1], a new upper bound on the error performance of GMD decoding [2] has been presented. Interestingly, under some mild assumptions, this upper bound is tight at all SNR values. The error performance analysis of [1] is based on the probability density functions of the j-th ordered reliability value among i hard-decision errors in a received sequence of length N for $1 \leq j \leq i$, and on the probability density functions of the l-th ordered reliability value among the remaining $N-i$ correct hard-decisions in the received sequence of length N, for $1 \leq l \leq N-i$.

In this paper, we first extend the approach of [1] to evaluate the error performance of Chase-type decoding. For the algorithm-2 introduced in [3] and BPSK transmission over an AWGN channel, the obtained bound falls on top of the simulated results at all SNR values, as depicted in Fig. 1 for Chase-2 decoding applied to the $p = 7$ and $p = 10$ least reliable positions of the received sequence for the (127,64) BCH code. The bounding method is then applied to the combination of GMD and Chase-type decodings as introduced in [4]. Tight bounds are obtained for the entire family of algorithms corresponding to this generalization. Finally, the bounding method is applied to the ordered statistic decoding (OSD) algorithm of [5]. The computational complexities of the corresponding bounds are smaller than that of the bounds derived in [5] for high orders of reprocessing. The new bounds are compared with the simulation results of OSD of the (128,64) extended BCH (eBCH) code in Fig. 2. The detailed derivations of these bounds are given in [6].

[1]This work was supported by the National Science Foundation under Grant CCR-97-32959.

References

[1] D. Agrawal and A. Vardy, "Generalized Minimum Distance Decoding in Euclidean-Space: Performance Analysis," *IEEE Trans. Inform. Theory*, IT-46, pp. 60-83, Jan. 2000.

[2] G. D. Forney Jr., "Generalized Minimum Distance Decoding," *IEEE Trans. Inform. Theory*, IT-12, pp. 125-131, Apr. 1966.

[3] D. Chase, "A Class of Algorithms for Decoding Block Codes with Channel Measurement Information," *IEEE Trans. Inform. Theory*, IT-18, pp. 170-182, Jan. 1972.

[4] M. Fossorier and S. Lin, " Chase-Type and GMD Coset Decodings," *IEEE Trans. Commun.*, COM-48, Mar. 2000.

[5] M. Fossorier and S. Lin, "Soft-Decision Decoding of Linear Block Codes based on Ordered Statistics," *IEEE Trans. Inform. Theory*, IT-41, pp. 1379-1396, Sept. 1995.

[6] M. Fossorier and S. Lin, "Error Performance Analysis for Reliability-Based Decoding Algorithms," submitted to *IEEE Trans. Inform. Theory*, June 1999.

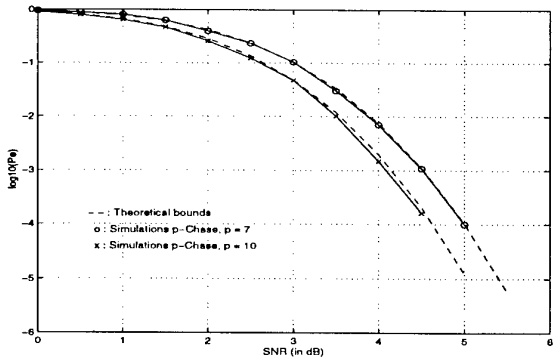


Figure 1: Word error rate for p-Chase decoding of the (127,64) BCH code with $p = 7$ and $p = 10$.

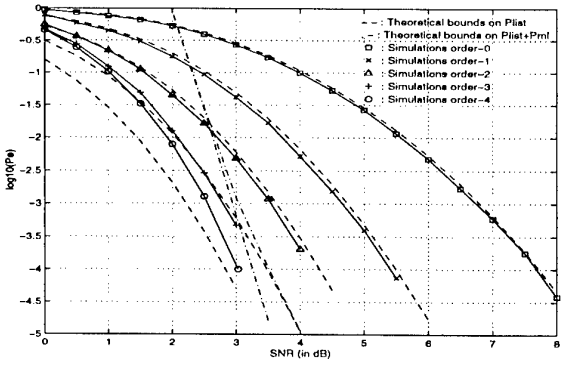


Figure 2: Word error rate for each stage of order-4 OSD of the (128,64) eBCH code.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Analysis of the Trellis Complexity of Interleavers and Turbo Codes

Roberto Garello *, Guido Montorsi **, Sergio Benedetto **, Giovanni Cancellieri *

* Dipartimento di Elettronica ed Automatica
Università di Ancona, Italy
e-mail: roberto.garello@ieee.org

** Dipartimento di Elettronica
Politecnico di Torino, Italy
e-mail: benedetto@polito.it

Abstract — **The trellis complexity of causal and non-causal interleavers are studied via the introduction of the input-output interleaver code. The "average" complexity of a uniform interleaver is computed. The trellis complexity of a turbo code is then tied to the complexity of the constituent interleaver. A procedure of complexity reduction by coordinate permutation is also presented, together with some examples of its application.**

I. Introduction

For a block code $C(n,k)$, the most used trellis complexity parameters are: the **maximum state complexity** $S(C) = \max_{0\le i\le n} s(i)$, where $s(i) = \log_2 |\Sigma(i)|$, and $\Sigma(i)$ is the **state space** at time $0 \le i \le n$; the **maximum branch complexity** $B(C) = \max_{1\le i<n} b(i)$, where $b(i) = \log_2 |\Gamma(i,i+1)|$, and $\Gamma(i,i+1)$ is the **trellis section** at time $0 \le i < n$; the **average branch symbol complexity** $E(C) = (\sum_{i=0}^{n-1} |\Gamma(i,i+1)|)/k$. It is well known that coordinate permutations ρ can strongly change the complexity parameters. In other words, given C, one can base a "real" measure of the complexity of C upon the parameters $\overline{S} = \min_\rho\{S(\rho(C))\}, \overline{B} = \min_\rho\{B(\rho(C))\}$, and $\overline{E} = \min_\rho\{E(\rho(C))\}$.

II. Interleavers

An **interleaver** $\mathcal{I}$ is a device characterized by a fixed permutation $\rho_\mathcal{I} : \mathbf{Z} \leftrightarrow \mathbf{Z}$. $\mathcal{I}$ maps bi-infinite input binary sequences $\mathbf{x}$ into permuted output sequences $\mathbf{y}$ with $y(i) = x(\rho_\mathcal{I}(i))$. Given an interleaver $\mathcal{I}$, we introduce the **(input-output) interleaver code** $C_\mathcal{I}$ defined as the set of all input/output interleaver sequence pairs $(\mathbf{x},\mathbf{y})$. For causal interleavers, it is well known and intuitive that the state space size is constant. When more general interleavers (non-causal, too) we have [1]:

Theorem 1

For every interleaver code $C_\mathcal{I}$: $s_\mathcal{I}(i) = |\mathcal{A}_i| + |\mathcal{P}_i|$, where: $\mathcal{A}_i = \{j \in \mathbf{Z} : j < i, \rho(j) \ge i\}$, $\mathcal{P}_i = \{j \in \mathbf{Z} : j \ge i, \rho(j) < i\}$. $\triangledown$

III. The trellis complexity of turbo codes

Let us consider **turbo codes** of rate-1/3 obtained from two equal binary systematic convolutional encoders of rate-1/2 and constraint length ν and a block interleaver $(\mathcal{I},\pi)$ of length N.

Theorem 2

For a turbo code C the state profile is equal to: $s_C(i) = s_\mathcal{I}(i) + c(i)$, with $c(i) \le 2\nu$. $\triangledown$

A **uniform interleaver** of length N is a probabilistic interleaver that acts as the "average" of all possible interleavers of length N.

Theorem 3

For an uniform block interleaver of length N:

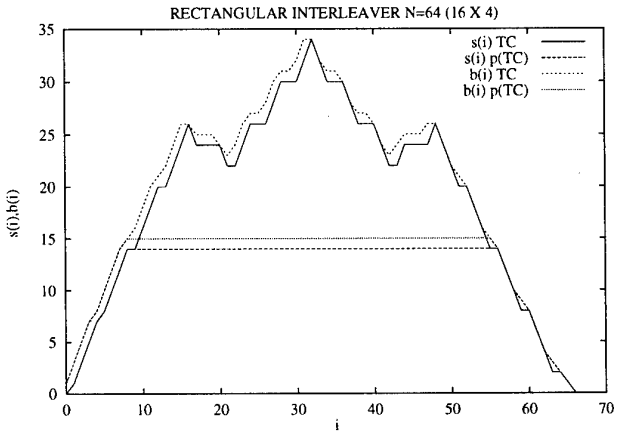


Fig. 1: State and branch profile for the turbo code of Example 1.

$s_{IU}(i) = \frac{2(N-i)i}{N}$ with $0 \le i \le N$. Its maximum state complexity is equal to $S^{(2)}_{IU} = N/2$.

Theorem 4

For a turbo code C formed by two constituent encoders of constraint length ν and a uniform block interleaver $\mathcal{I}$ of length N: $s_{CU}(i) = \frac{2\cdot(N-i)\cdot i}{N} + c(i)$, with $c(i) \le 2\nu$. Its maximum state complexity is $S^{(3)}_{CU} = N/2 + c$, with $c \le 2\nu$. $\triangledown$

IV. Reducing the complexity of turbo codes

Given an interleaver $(\mathcal{I},\rho_\mathcal{I})$ the permutations $p_1 = (I,\rho^{-1})$ and $p_2 = (\rho, I)$ minimizes the complexity parameters of $p(C_\mathcal{I})$ to $\overline{S} = 0$, $\overline{B} = 1$, and $\overline{E} = 4$. Using this result, to reduce the complexity of a turbo code employing a block interleaver π, we have considered these two permutations: $p_{min1} = (I, I, \pi^{-1})$ and $p_{min2} = (\pi, \pi, I)$.

As an example, impressive results in terms of complexity reduction through the application of p_{min1} and p_{min2} can be obtained for the class of turbo codes employing row-by-column block interleavers. It can be proved that, when N is a power of two, $N/2 \le S^{(3)} \le N/2 + 2\nu$. By applying p_{min1} (p_{min2}, respectively) when $N_R \ge N_C$ ($N_R \le N_C$), we obtain a consistent reduction to $S^{(3)} = \nu(2N_C - 1)$ ($S^{(3)} = \nu(2N_R - 1)$).

Example 1

Consider a turbo code composed by two equal 4-state convolutional encoders and a block rectangular interleaver with $N = 64, N_R = 16$ and $N_C = 4$. In Fig. 1 we report the state and branch profiles of the turbo code evaluated directly and through the permutation p_{min1}, showing a significant complexity reduction.

References

[1] Garello, Montorsi, Benedetto, Cancellieri. "Interleaver properties and applications to the trellis complexity analysis of turbo codes", *submitted to IEEE Transactions on Communications.*

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Improving Turbo Decoding via Cross-Entropy Minimization

M. Eoin Buckley, Bhaskar Krishnamachari, Stephen B. Wicker
School of Electrical Engineering, Cornell University,
Ithaca, NY 14850, U.S.A
{eoin,bhaskar,wicker}@ee.cornell.edu

Joachim Hagenauer
Institute for Communications Engineering
TU München, Germany
hag@LNT.e-technik.tu-muenchen.de

Abstract — **We show that the decoding performance of a simple turbo code can be improved by cross-entropy minimization via manipulation of the initial *a priori* probabilities.**

I. Improving Turbo Decoding

While Turbo decoding of parallel concatenated codes (PCC) has been shown to offer near Shannon-limit performance, it is known that the decoding is sub-optimal. For example it has been shown analytically by McEliece *et al.* [1] that, for certain received values of a (14, 3) PCC, the turbo decoding process does not converge . However, this does not cover all cases of non-convergence. Furthermore, there are also cases where the turbo decoding process converges to a non-maximum *a posteriori* probability (non-optimum) decision.

We investigated the turbo decoding performance when the initial *a priori* probabilities (APRP) are biased to the optimally decoded message for this (14,3) turbo code. This method, which assumes knowledge of the optimum decision, is referred to in this paper as the "Genie" Turbo Decoding method (GT). Figure 1a shows the BER surface when initial APRPs for the first two of the three information bits are biased with respect to the optimum decision with values ranging from $\delta_1 = \delta_2 = 0$ (correctly biased) to $\delta_1 = \delta_2 = 1$ (incorrectly biased). The BER, which is measured for an E_b/N_o of 5dB, shows a slight improvement when both bits are biased correctly as opposed to the unbiased case ($\delta_i = 0.5, \forall i$).

Hagenauer *et al.* [2] have proposed using cross-entropy between the outputs of the component decoders to detect convergence. The similarity between the cross-entropy surface (figure 1b) and the BER surface (figure 1a) suggests that the cross-entropy values may be used to infer initial APRP settings in order to improve decoding performance.

We modified the turbo-decoding process by biasing the APRPs to the eight possible messages, each for a fixed number of iterations. The output of the bias that yields the lowest cross-entropy at the final iteration is then chosen. We refer to this technique as Entropy Minimization Turbo Decoding (EMT). Table 1 compares the percentage increase in BER with respect to optimum decision decoding for the traditional turbo decoding, EMT, and GT approaches at various E_b/N_o values. The performance for GT and the traditional turbo decoding are shown for the average obtained between 50 and 100 iterations, while the EMT performance is for just 2 iterations (at each of the 8 possible messages).

II. Results

It is seen that GT always out-performs the traditional turbo decoder showing that there is a potential for improvement at all E_b/N_o by biasing the initial APRPs; further, this potential for improvement is significantly greater at higher E_b/N_o. Above 2 dB, EMT also performs better than traditional turbo decoding and nears the performance of GT at 5 dB.

Based on these results, we believe it is possible to improve the performance of more practical turbo-decoders by pre-setting the initial APRPs.

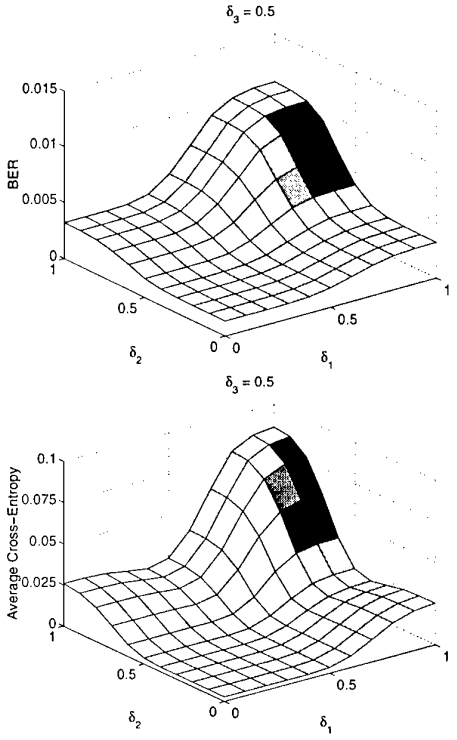


Figure 1: BER and Cross-Entropy Surfaces

	2 dB	3 dB	4 dB	5 dB
Turbo	6.07	8.17	10.81	14.74
EMT	6.93	7.29	8.67	8.71
GT	5.10	6.15	7.40	8.46

Table 1: Percentage Increase in BER w.r.t. Optimum

References

[1] R.J. McEliece, E.R. Rodemich and J.-F. Cheng, "The Turbo Decision Algorithm", *Thirty-Third Annual Allerton Conference on Communication, Control, and Computing*, pp. 366-79, 1995.

[2] J. Hagenauer, E. Offer, L. Papke, "Iterative decoding of binary block and convolutional codes," *IEEE Transactions on Information Theory*, vol. 42, no. 2, March 1996.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Simplified Turbo Decoding for Binary Markov Channels

Javier Garcia-Frias
Department of ECE
University of Delaware
307 Evans Hall
Newark, DE 19716, USA
e-mail: jgarcia@ee.udel.edu

John D. Villasenor
Electrical Engineering Department
UCLA
405 Hilgard Avenue
Los Angeles, CA 90024-1594, USA
e-mail: villa@icsl.ucla.edu

Abstract — **We present a simplified method for combining turbo decoding and binary Markov channels. The resulting performance is slightly worse than that of the best known methods using supertrellis approaches, but it clearly outperforms traditional systems based on channel interleaving. Moreover, the complexity is much lower than in the supertrellis case and the structure of the encoder does not depend on the parameters of the hidden Markov model describing the channel.**

I. Introduction

Many practical digital communications channels exhibit statistical dependencies among errors. The error pattern of the discrete channel (modulator-real channel-demodulator) can be modeled using binary Markov channels [1, 2]. It is intuitive that the presence of memory in these channels leads to increased capacity relative to memoryless channels with the same stationary bit error probability. In practice, many communications systems make use of a channel interleaver to distribute the errors so that codes designed for a memoryless channel can be used. While the application of interleaving does not change the capacity of the channel, the achievable performance of a decoder which assumes that the channel is memoryless is far away from the real capacity of the channel.

Turbo coding for binary Markov channels has been previously described in [3]. However, the methods proposed in [3] involve a considerable increase in complexity, since supertrellises jointly describing the constituent encoders and the hidden Markov models have to be built. We propose a simplified decoding method, which performs slightly worse than the method in [3] but the main advantage (besides the reduced complexity) is that there is no need to change the turbo encoder structure depending on the channel parameters.

II. Simplified turbo decoding for binary Markov channels

The basic idea of the proposed method is to treat the trellis describing the binary Markov channel as another constituent decoder which exchanges extrinsic information with the other constituent decoders in each one of the turbo decoding iterations. The channel block uses as extrinsic information the estimation of the probability of the error pattern that is provided by the constituent decoder blocks. On the other hand, it produces a new estimation of such a probability which will be used as extrinsic information by the constituent convolutional decoders. This results in three different classes of extrinsic information that are interchanged among the decoding blocks. The proposed method resembles the ones proposed in [4, 5] for continuous hidden Markov channels and hidden Markov sources, although, contrarily to [4], in this case it is necessary to iterate over the hidden Markov trellis.

III. Simulation Results

In order to assess the performance of the proposed method, we consider two binary Markov channels with two states. For the first channel, the transition probability from the good to the bad state is .0486, and .0914 is the value of the transition probability from the bad to the good state. For the second channel these values are .006943 and .013057, respectively. In both cases, the bit error probability in the bad state is fixed to .5. The performance of the system is studied as a function of the value of the bit error probability in the good state (notice that, since all the other parameters are fixed, there is a one to one correspondence between the bit error probability in the good state and the stationary bit error probability, ρ.)

We use a rate 1/3 turbo code that includes a systematic bit and two identical recursive 8-state convolutional encoders with generator matrix $G(D) = \frac{1+D+D^2+D^3}{1+D^2+D^3}$ and an interleaver with length 16384. In order to obtain good performance it is necessary to use a channel interleaver which "separates" the Markov channel and the turbo decoder. Each simulation consisted of at least 40 million bits. For rate 1/3 codes, the bit error probability corresponding to the capacity of a binary symmetric channel is $\rho = .174$. Therefore, by using channel interleaving and ignoring the memory of the channel (the usual approach to cope with bursty channels,) it is impossible to send reliable information through any of these channels when the stationary bit error probability is higher than .174. However, using the proposed method, convergence for the first channel is achieved at $\rho = .18 - .185$, which is higher than the memoryless limit and close to the theoretical limit for this channel (which corresponds to a value $\rho = .2083$.) For the second channel convergence is achieved at $\rho = .19 - .195$. The theoretical limit in this case is $\rho = .2307$.

References

[1] L. N. Kanal and A. R. K Sastry, "Models for Channels with Memory and Their Application to Error Control," *Proc. IEEE*, vol. 66, no. 7, pp. 724-744, 1978.

[2] W. Turin, "Performance Analysis of Digital Transmission Systems," New York: Computer Science, 1990.

[3] J. Garcia-Frias and John D. Villasenor, "Exploiting Binary Markov Channels with Unknown Parameters in Turbo Coding," *Proc. IEEE Globecom'98*, pp. 3244-3249, November 1998, Sydney, Australia.

[4] J. Garcia-Frias and John D. Villasenor, "Turbo Codes for Continuous Hidden Markov Channels with Unknown Parameters," *Proc. IEEE Globecom'99*, December 1999, Rio de Janeiro, Brazil.

[5] J. Garcia-Frias and John D. Villasenor, "Simplified Methods for Combining Hidden Markov Models and Turbo Codes," *Proc. IEEE VTC'99 (fall)*, September 1999, Amsterdam, Holland.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Approximate Performance Analysis of Turbo Codes with Fixed Interleavers

Jianqiu Zhang and Nam Phamdo
Department of Electrical and Computer Engineering
State University of New York at Stony Brook
Stony Brook, NY, 11794-2350
e-mail:{jizzhang, phamdo}@ece.sunysb.edu

I. Introduction

The weight spectrum of a turbo code [1] is useful in deriving its performance bounds. Due to the randomness and large size of the interleaver, it is extremely difficult to obtain the exact weight spectrum. In the past, the average weight spectrum, averaged over all interleavers [2], is used in deriving the bounds.

By introducing several limiting factors, we are able to derive an approximate weight spectrum for turbo codes with fixed interleavers. The complexity of the algorithm grows only linearly with the size of the interleaver.

II. Evaluating the Weight Spectrum

A "global" turbo *codeword* consists of three binary vectors: $(\underline{u}, \underline{r}_1, \underline{r}_2)$, where $\underline{u}$ represents information bits, $\underline{r}_1$ and $\underline{r}_2$ represent redundant bits. A *subcodeword* refers to either $(\underline{u}, \underline{r}_1)$ or $(\underline{u}, \underline{r}_2)$. One limiting factor introduced is the maximum weight, D_{max}, of codewords. We ignore weights greater than D_{max} because they have little impact on the bit error rate (BER). We only consider low input-weight codewords since these codewords dominate the lower end of the weight spectrum when the interleaver guarantees a minimum spreading. A low input-weight codeword may consist one or several Elementary Low-weight Subcodewords (ELWSC). By definition, the error path of an ELWSC deviates from the zero state only once in a constituent code. An ELWSC, say with input weight 2, is referred to as w2ELWSC. The weight of an ELWSC is less than D_{max}. This implies the length of its error path must be less than a limit M. We define M as the span of ELWSCs. Special treatments are given to input weights in the "tail" (or last L bits) of the input sequence to account for the large number of ELWSCs with these input weights.

To evaluate the weight spectrum, we need to find possible arrangements (or error patterns) of input weights that result in low-weight codewords. For example, the most probable input-weight 4 error pattern involving bit a is shown in Fig. 1. CC1 stands for constituent code 1 and CC2 for constituent code 2. Input bit pairs $\{a, b_i\}$ and $\{c_i, d_i\}$ form two w2ELWSCs in CC1. In CC2, these input bits swap their positions and form two other w2ELWSCs. Note that subscripts are used for b_i, c_i, and d_i to indicate that there are more than one set of input bits that can form such an error pattern with bit a. The search for these bits are conducted within the span of ELWSCs. For example, b_i is searched in the range $(I_a - M, I_a + M)$ where I_a is the index of bit a in CC1.

This searching process is applied to error patterns of input-weight up to 6.

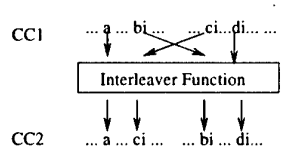


Fig. 1: Input Weight 4 Error Pattern.

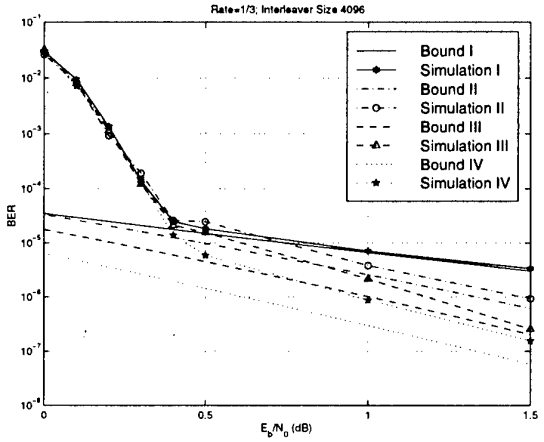


Fig. 2: Union Bound Analysis and Simulation Results of Turbo Code with Different Interleavers.

III. Analysis of Different Interleavers

In Fig. 2, the legends stand for: I: Uniform Interleaver. II: Modified Block Interleaver with the prime number set from [1]. III: Modified Block Interleaver with the prime number set selected from our analysis. IV: Modified S-pseudorandom Interleaver as described in [3] selected from our analysis. Over 100 bit errors were accumulated for each simulation point. The union bounds plotted are calculated using the weight spectrum derived from our analysis which is performed on the rate-1/3, (37,21) turbo code with interleaver size 4096. Due to the randomness of the generating process of interleavers, our analysis is very useful in picking out the "best" one. Also the analysis provides an approximation of the error floor.

References

[1] C. Berrou, and A. Glavieux, "Near Optimum Error Correcting Coding and Decoding: Turbo-Codes," *IEEE Trans. Communications*, vol. 42, pp. 1261-1271, Oct. 1996.

[2] S. Benedetto, and G. Montorsi, "Unveiling Turbo Codes: Some Results on Parallel Concatenated Coding Schemes," *IEEE Trans. Information Theory*, vol. 42, No. 2, March 1996.

[3] J. Yuan, B. Vucetic, and W. Feng, "Combined Turbo Codes and Interleaver Design," *IEEE Trans. Communications*, vol. 47, No. 4, April 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

A Universal Prediction Lemma and Applications to Universal Data Compression and Prediction (Abstract)

Jacob Ziv[1],[2]
EE Dept, Technion, Haifa 32000
ISRAEL
jz@ee.technion.ac.il

We consider finite-alphabet sequences which are emitted by a stationary source with unknown statistics.

$$\begin{aligned}\mathbf{X} &= \mathbf{X_1}, \mathbf{X_2}, \ldots, \mathbf{X_i}, \ldots; \\ \mathbf{X_1^m} &= \mathbf{X_1}, \mathbf{X_2}, \ldots, \mathbf{X_m}\,;\, \mathbf{X_i} \in \mathbf{A}\,;\, |\mathbf{A}| = A\,.\end{aligned}$$

Assume that we are given a training vector Y_{-N}^{-1} which is governed by the same probability law that governs $\mathbf{X}$, but is drawn independently of $\mathbf{X}$. In the case where $Y_{-N}^{-1} = X_{-N+1}^{0}$, (Sliding-window case), the independence assumption is essentially replaced by the assumption the source is a finite-order Markov source. Given Y_{-N}^{-1}, we need to estimate $P(X_1|X_{-t}^{0})$ (in order to predict X_1 given X_{-t}^{0}, or compress X_1 given X_{-t}^{0}, etc. in cases where the actual measure $P(X_1|X_{-t}^{0})$ is not available to us).

In order to estimate $P(X_1|X_{-t}^{0})$ one constructs, for any training-sequence Y_{-N}^{-1}, some empirical conditional probability measure $Q_{Y_{-N}^{-1}}^{t}(X_1|X_{-t}^{0})$ of X_1 given X_{-t}^{0}, hoping that this empirical conditional probability measure will be "close" in some sense to the true $P(X_1|X_{-t}^{0})$.

One common way for generating such an empirical measure is to evaluate the relative frequency of appearance of each $t+2$ vector X_{-t}^{1} in Y_{-N}^{-1}, and use it to generate an empirical probability measure for $t+2$ vectors, which will be denoted by $q_{Y_{-N}^{-1}}(X_{-t}^{1})$ and from this measure to generate a **conditional** probability measure $Q_{Y_{-N}^{-1}}^{t}(X_1|X_{-t}^{0})$=$q_{Y_{-N}^{-1}}(X_1|X_{-t}^{0})$ for any t such that X_{-t}^{0} appears in Y_{-N}^{-1} at least once.

For example, let $Y_{-N}^{-1} = 0101100$; $t=0$, $X_{-t}^{1} = 01$,$X_{-t}^{0} = X_0^0 = X_0 = 0$. Then, $q_{Y_{-N}^{-1}}(01) = 2/6$; $q_{Y_{-N}^{-1}}(00) = 1/6$; $q_{Y_{-N}^{-1}}(1|0) = \frac{2/6}{2/6+1/6} = 2/3$.

For X_{-t}^{0} that do not appear in Y_{-N}^{-1}, we may set $q_{Y_{-N}^{-1}}(X_1|X_{-t}^{0}) = q_{Y_{-N}^{-1}}(X_1|X_{-K_0}^{0})$, where $X_{-K_0}^{0}$ is the longest suffix of X_{-t}^{0} that does appear in Y_{-N}^{-1}. (K_0 is defined more precisely below).

But is this choice of an empirical conditional probability measure optimal for relatively short training sequences? Our aim is to try to minimize the K-L relative entropy (divergence) between the true $P(X_1|X_{-t}^{0})$ and $Q_{Y_{-N}^{-1}}^{t}(X_1|X_{-t}^{0})$, namely $E\log\frac{P(X_1|X_{-t}^{0})}{Q_{Y_{-N}^{-1}}^{t}(X_1|X_{-t}^{0})}$, where $E(\cdot)$ denotes expectation with respect to $P(Y_{-N}^{-1}, X_{-t}^{1})$.

In this presentation we are treating this optimization problem by deriving performance bounds for a restricted class of empirical conditional distributions(predictors).

Assumption 1 *Let us define a random variable $K_0 = K_0(X_{-t+1}^{0}; Y_{-N}^{-1})$ to be the largest integer $i \le t$ such that $X_{-i}^{0} = Y_{-i-j}^{-j}$ for some $1 \le j \le N-i$. ($K_0 = 0$ if X_0 does not appear in Y_{-N}^{-1}).*

We assume that the discussion is limited to the class of empirical conditional probabilty distributions such that, for $K_0 \le t$,

$$Q_{Y_{-N}^{-1}}^{t}(X_1|X_{-t}^{0}) = Q_{Y_{-N}^{-1}}^{t}(X_1|X_{-K_0}^{0})$$

(since for $K_0 \le t$ the conditioning is on an event X_{-t}^{0} that was never observed in Y_{-N}^{-1}: only it's suffix $X_{-K_0}^{0}$ was observed in Y_{-N}^{-1}).

Lemma 1 *Under Assumption 1 and for any $t = 0, 1, 2, 3\cdots$*

$$\begin{aligned}& -E_{Y_{-N}^{-1}} \log Q_{Y_{-N}^{-1}}^{t}(X_1|X_{-t}^{0}) \\ = \;& -E_{Y_{-N}^{-1}} \log Q_{Y_{-N}^{-1}}^{t}(X_1|X_{-K_0}^{0}) \\ \ge \;& -E_{Y_{-N}^{-1}} \log P(X_1|X_{-K_0-1}^{0}) = H_{Y_{-N}^{-1}}(X_1|X_{-K_0-1}^{0})\,.\end{aligned}$$

where $E_{Y_{-N}^{-1}}(\cdot)$ denotes conditional expectation given the value of Y_{-N}^{-1}.

If Y_{-N}^{-1} is drawn independently of X_{-t}^{0}, we have:

$$\begin{aligned}& -E\log Q_{Y_N^{-1}}^{t}(X_1|X_{-t}^{0}) \\ & \quad \ge -E\log P(X_1|X_{-K_0-1}^{0}) = H(X_1|X_{-K_0-1}^{0})\end{aligned}$$

We call the reader's attention to the fact that in the "entropy" expression $H(X_1|X_{-K_0-1}^{0})$ K_0 is a r.v. Furthermore, this "entropy" may be evaluated only if the probabilistic characterization of the source is available. However, it's usefulness stems from the fact that it is demonstrated that there indeed exist *universal* algorithms for generating conditional empirical measures $q_{Y_N^{-1}}^{t}(X_1|X_{-t}^{0})$ which are members in the admissible class that is defined by Assumption 1, for which $-E\log q_{Y_N^{-1}}^{t}(X_1|X_{-t}^{0})$ is close to $H(X_1|X_{-K_0-1}^{0})$.

It should be pointed out that,

$H(X_1) \ge H(X_1|X_{-K_0-1}^{0}) \ge H(X_1|X_{-t-1}^{0})$

thus demonstrating the non-asymptotic effect of having a "short" training sequence.

While these imposed restrictions are apparently intuitively satisfying, they also lead to new useful non-asymptotic bounds on the performance of universal data compression algorithms such as CTW, LZ and HZ [1](where similar bounds where drived in the minimax sense only).

References

[1] Y. Hershkovits and J. Ziv, "On Sliding-Window Universal Data Compression with Limited Memory", *IEEE Trans. on Information Theory*, Vol. 44, pp. 66–78, January 1998.

[1]This work was done in part while visiting Lucent Bell Laboratories

[2]This work was supported by the Fund for the Promotion of Research at the Technion

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On Sequential Strategies for Loss Functions with Memory

Neri Merhav[1]
Electrical Engineering Department
Technion, Haifa 32000, Israel
merhav@ee.technion.ac.il

Erik Ordentlich[2]
iCompression
Santa Clara, CA 95051, USA
eordentlich@icompression.com

Gadiel Seroussi and
Marcelo J. Weinberger
Hewlett-Packard Laboratories
Palo Alto, CA 94304, USA
{seroussi,marcelo}@hpl.hp.com

Abstract — **The sequential decision problem is studied for loss functions with memory and finite action spaces. Based on the theory of Markov decision processes (MDP's), off-line reference strategies are characterized. An infinite horizon on-line strategy, with corresponding normalized "regret" which is upper-bounded by an $O(n^{-1/3})$ term for an arbitrary individual sequence of observations of length n, is derived.**

I. Introduction

Consider a sequence of observations $x^n = x_1 x_2 \cdots x_n$ for which corresponding actions $b^n = b_1 b_2 \cdots b_n$ result in non-negative instantaneous losses $\ell(s_t, b_{t-1}, b_t, x_t)$, $1 \le t \le n$, where s_t is a state driven by $s_{t+1} = f(s_t, x_t)$ in a finite set S, and s_1 is fixed. The action space B is assumed finite, and $b_0 \in B$ is an initial action. While including the classical "sequential decision problem" [1, 2], for which the loss at time t is independent of b_{t-1}, this formulation also captures cases where there is a cost for switching between actions, or a long term effect ("memory") for actions taken at a given time. Extensions to longer past action memories are straightforward.

In an on-line strategy, b_t is a (possibly random) function of x^{t-1} and b^{t-1}. For *memoryless* loss functions, the excess loss accumulated by an on-line strategy over the best off-line finite-state (FS) strategy (i.e., one in which $b_t = g(s_t)$, where g is optimized with *full knowledge* of x^n) is termed the *regret*. An on-line randomized strategy is demonstrated in [1] for $|S| = 1$ (see [2] for $S > 1$), for which the *normalized* expected regret vanishes at an $O(1/\sqrt{n})$ rate, uniformly over $\{x^n\}$. Here, we present an analogous result for loss functions with memory.

II. The reference off-line strategy

For memoryless loss functions, reference FS *deterministic* strategies are justified as follows: If the data are drawn from an FS source $\{p(x|s), s \in S\}$ (on a discrete or continuous data space), the expected (normalized) loss over infinite sequences is minimized (over all strategies $b_t = \mu_t(x^{t-1}, b^{t-1})$) by the FS strategy $g(s) = \arg\min_{b \in B} E_p \ell(s, b, x)$. Similarly, here, the expected loss is given by

$$\bar{L}_{p,\mu} = \limsup_{n \to \infty} \frac{1}{n} \sum_{t=1}^{n} \sum_{s \in S,\, b', b \in B} P_t(s, b', b) L(s, b', b)$$

where $P_t(s, b', b)$ is the joint probability (w.r.t. $\{p(x|s)\}$ and $\{\mu_t\}$) that $(s_t, b_{t-1}, b_t) = (s, b', b)$, and $L(s, b', b) = E_p \ell(s, b', b, x)$. The minimization of $\bar{L}_{p,\mu}$ over $\{\mu_t\}$ is an *average cost per stage* problem for a particular MDP. Assuming that $\{p(x|s)\}$ yields an irreducible Markov chain, there is [3, Vol. 2, Ch. 4] a *deterministic* minimizing strategy $b_t = \mu(s_t, b_{t-1})$, independent of s_1 and b_0. The strategy μ is obtained as a solution to a linear program. As $\{p(x|s)\}$ varies, it generates a finite set $\mathcal{F}$ of deterministic off-line reference strategies. In particular, if the state transitions are deterministic (e.g., if $|S| = 1$), then the off-line strategies are described in terms of simple cycles with minimum average weight in a graph whose nodes are in $S \times B$, and an edge from (s, b') to $(f(s), b)$ has a weight $L(s, b', b)$, where s transitions to $f(s)$.

III. On-line strategy

The design of an on-line strategy is actually an instance of learning with expert advice [4], where $\mathcal{F}$ is a set of β experts. However, the instantaneous loss of a strategy that follows an expert $F \in \mathcal{F}$ at time t depends on b_{t-1}, which may not agree with F. This memory calls for an additional block-length parameter that determines how long the advice of an expert is followed. The discrepancy between on-line and expert losses at the start of each block is amortized over the block. Our on-line strategy, inspired by [4], is first presented for the horizon-dependent case. For a fixed block length M, at $t = Mk + 1$, $k = 0, 1, \cdots$, we randomly select F according to

$$P_k(F | \{\mathcal{L}_{F,k}\}, F \in \mathcal{F}) = \frac{\exp\{-\eta \mathcal{L}_{F,k}\}}{\sum_{F' \in \mathcal{F}} \exp\{-\eta \mathcal{L}_{F',k}\}}$$

where $\eta > 0$ is a given constant and $\mathcal{L}_{F,k}$ is the cumulative loss of F through time $t = Mk$. The actions of F are followed through $t = N_{k+1}$.

Theorem 1 *Let* $M = 2\left(\frac{n}{\ln \beta}\right)^{1/3}$ *and* $\eta = \frac{2}{\ell_{\max}}\left(\frac{\ln \beta}{n}\right)^{2/3}$, *where* $\ell_{\max}$ *denotes the maximum loss* $\ell(s, b', b, x)$ *over* $s \in S$, $b', b \in B$, *and* $x \in A$. *Then, the normalized regret of the on-line strategy is* $\le 1.5 \ell_{\max} [(\ln \beta)/n]^{1/3}$.

For infinite horizon, time is divided into exponentially growing super-segments of sizes $\{N_i\}$, in each of which the above algorithm is used with N_i replacing n in the specification of M and η. We show that for all n, the normalized regret is bounded as in Theorem 1, but with a larger constant.

Acknowledgments

Many thanks to Tom Cover for useful discussions.

References

[1] J. F. Hannan, "Approximation to Bayes risk in repeated plays," in *Contributions to the Theory of Games, Volume III, Annals of Mathematics Studies*, pp. 97–139, Princeton, NJ, 1957.

[2] N. Merhav and M. Feder, "Universal prediction," *IEEE Trans. Inform. Theory*, vol. IT-44, pp. 2124–2147, Oct. 1998.

[3] D. P. Bertsekas, *Dynamic programming and optimal control.* Belmont, Massachusetts: Athena Scientific, 1995.

[4] V. G. Vovk, "Aggregating strategies," in *Proc. of the 3rd Annual Workshop on Computational Learning Theory*, (San Mateo, California), pp. 372–383, 1990.

[1] Work partially done while visiting at HP Labs.
[2] Work done while this author was with HP Labs.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On Asymptotically Optimal Methods of Prediction and Adaptive Coding for Markov Sources with Unknown Memory

Boris Ryabko[1]
Siberian State University of
Telecom. and Inform. Sci.
Kirov St. 86, Novosibirsk 630102
Russia
e-mail: ryabko@neic.nsk.su

Flemming Topsøe
Department of Mathematics,
University of Copenhagen
Universitetsparken 5, Copenhagen
DK-2100 Denmark
e-mail: topsoe@math.ku.dk

Abstract — **The asymptotically optimal methods of prediction for Markov sources with unknown memory are suggested. The methods are based on modified twice universal scheme.**

I. Introduction

The problem of prediction and the closely related problem of adaptive coding of time series is well known in Information Theory, Probability Theory and Statistics [1].

We consider a source with unknown statistics which generates sequences $x_1x_2\ldots$ of letters from a finite alphabet $A = \{a_1, \ldots, a_n\}$. We imagine that we have at our disposal a computer for solving the prediction problem. As input we consider any finite string $x_1x_2\ldots x_t$ of letters from A and as output we receive at each time instant t non-negative numbers $p^*(a_1|x_1\ldots x_t), \ldots, p^*(a_n|x_1\ldots x_t)$ which are estimates of the unknown conditional probabilities $p(a_1|x_1\ldots x_t), \ldots, p(a_n|x_1\ldots x_t)$, i.e., of the probabilities $p(x_{t+1} = a_i|x_1\ldots x_t)$; $i = 1, \ldots, n$. The set $p^*(a_i|x_1\ldots x_t)$; $i \le n$ is called the *prediction*.

The *precision* of a prediction method is measured by the divergence between p and p^* and the *complexity* of a method is characterized by two numbers: the *average time* of calculation at each time instant in bit operations and the *memory size* in bits of the program defining the method. Let us denote the set of Markov sources of memory (or connectivity) k as $M_k(A)$ and let $M_0(A)$ be the set of all Bernoulli sources.

In this report we consider the prediction problem for Markov sources with unknown statistics and memory.

II. The Main Results

We will use two asymptotically optimal prediction methods for $M_i(A), i = 0, 1, \ldots$, which were suggested in [2]. The method α_i is asymptotically optimal in average and β_i with probability one.

According to twice universal scheme, at each time instant t a computer compares the average precision of all methods $\beta_0, \beta_1, \ldots, \beta_N$ on the interval $t = 1, 2, \ldots, T-1$ and finds j_0 for which β_{j_0} gives the best precision on the interval $t = 1, 2, \ldots, T-1$. Then the computer uses β_{j_0} in order to predict for the next moment T. (It looks like the likelihood principle).

It is clear that the computer should calculate $(N+1)$ prediction sets (for $\beta_0, \beta_1, \ldots, \beta_N$) instead of one set as it does in case of known memory of the source. So the time of calculation increases $(N+1)$ times. Similarly, the memory space of the computer should be divided into $(N+1)$ parts in order to store statistics for $\beta_0, \beta_1, \ldots, \beta_N$.

The new methods are based on a simplified twice universal scheme (STUS). According to STUS, a computer which is used for the implementation of the suggested method compares two methods β_{i_1} and β_{i_2} at each time instant t. First, at $t = 1, 2, \ldots, T$ the computer compares β_0 and β_1 which are optimal for $M_0(A)$ and $M_1(A)$ (T is a parameter of the method). Then the computer removes the worst method and includes β_2 instead of it. After that both methods are compared during the period of $[T+1, \ldots, 2T]$, the worst of them is removed and so on. At each time instant t the computer uses the best method β_{i_j} for prediction. (At the first interval $[1, \ldots, T]$ β_0 is used). At the moment $(N+1)T+1$ the computer again includes β_0 instead of removed β_{i_j}. And so on. It is quite obvious that the computer will find the best β_i and will use it almost all time for prediction if T is quite large. On the other hand, this universal scheme is fast and space-efficient because at every moment only two methods are compared instead of N in the "conventional" twice universal scheme. We designate this method as β^1_{stu} and describe two other modifications.

The β^1_{stu} is effective with probability 1. We obtain the method β^2_{stu} which is simpler if the computer stops to look for the best method β^1_{stu} after the moment $(N+1)T$ and uses for prediction at the moments $(N+1)T+1, (N+1)T2, \ldots$ the β_{i_j} which was the best during $[NT+1, \ldots, (N+1)T]$. The new method β^2_{stu} is effective in average only. (For simplification of the method it is possible to use optimal in average α_{i_j} instead of β_{i_j}). The last modification β^3_{stu} may be used when N is infinite or when it is known only that a source is ergodic. The method β^3_{stu} looks like β^2_{stu} but the computer includes randomly chosen method β_i from the $\beta_0, \beta_1, \ldots$ (Recall, that β_i is included instead of the worst method β_{i_j} at the moments $T+1, 2T+1, 3T+1, \ldots$).

The main property of the suggested STUS may be formulated as follows: if β^1_{stu} is used with $T(r) = \left\lceil \left(\log \frac{1}{r}\right)^2 \right\rceil$, where r is the precision, then for every $M_i(A)$ its precision is asymptotically equal to the precision of the method which is optimal for $M_i(A)$, when r goes to 0.

References

[1] P. Algoet, "Universal schemes for learning the best nonlinear predictor given the infinite past and side information," *IEEE Trans. Inform. Theory*, vol. 45, no. 4, pp. 1165–1185, 1999.

[2] B. Ryabko and F. Topsoe, "On asymptotically optimal methods of prediction and adaptive coding," in *Proc. IEEE Int. Symp. Inform. Theory*, Cambridge, MA, August 1998, p. 316.

[1]This work was supported by RFBR Grant 99-01-00586.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

A Technique for Prediction and Probability Assignment (PPA) in Lossless Data Compression

Nicklas Ekstrand
Dept. of Information Technology
Lund University, Sweden
E-mail: nicklas@it.lth.se

Ben Smeets
Ericsson Mobile Communications
Ericsson Research, Sweden
E-mail: ben.smeets@ecs.ericsson.se

Abstract — **The prediction and probability assignment (PPA) concept is important in lossless image compression. We report on a new approximate technique for PPA based on local optimization.**

I. Introduction

The aim in universal lossless data compression is to achieve a performance, in terms of average redundancy, that asymptotically fulfills Rissanen's lower bound [1] for universal coding. A slightly different aim is to minimize the maximal individual redundancy for any sequence. This approach is well studied by for example Shtarkov [2]. An important difference between these two different measurements are that by studying individual sequences we get a tool for short or limited sequences, i.e., we may get a desired behavior from the first symbol to the last. This difference plays an important roll in e.g. lossless image compression where the data is, by nature, limited to the bounds of the image.

We know that the lower bound for universal data compression depends not only on the length of the sequence but also on number of unknown parameters, K, roughly like: $\rho(n) \approx \frac{K}{2} \log n$. Thus it is the aim when constructing a data compression scheme for practical applications to find a parameterization of the source with a minimal number of unknown parameters without loosing any information. It is well known, in the lossless image compression community, that (linear) prediction is an excellent tool for such reduction of the number of unknown parameters. Much work has focused on different strategies for universal prediction schemes. These prediction schemes have often some kind of connection with universal data compression, e.g. [3]. Although the excellent results in the area the application in lossless image compression require some further investigation due to the fact that we want to minimize the resulting codeword length which may be a different goal compared to minimizing the error from the prediction scheme.

In the way the data is treated in most image compression schemes with independent prediction and probability assignment (or estimation) we cannot guarantee that it is possible to make a probability assignment that has an optimal behavior according to Rissanen's bound. For this reason the *prediction and probability assignment* (PPA) concept was introduced in [4]. The aim with PPA is to optimize the prediction and the probability assignment together in order to control the behavior of the redundancy in a desired way. This is also of major importance since we usually use some kind of context tree model for our data and the sequences in each node of a context tree tends to be very small, e.g. less than 100 samples, except for a few nodes at small depth. For sequences of limited length it could be disastrous to use a universal source coding scheme which only performs asymptotically correct and have an non-optimal initial behavior.

[0]This work was supported by TFR project 271-98-244.

II. The approximate PPA algorithm

From a theoretical point of view we should be able to construct a PPA scheme with a desired behavior by using a weighting technique. We could calculate the weighted block probability according to: $P_w(\cdot) = \int_{\mathbf{a}} \int_{\theta} \alpha(\mathbf{a}, \theta) P_B(\cdot, \mathbf{a}, \theta) d\mathbf{a} d\theta$, where $P_B(\cdot, \mathbf{a}, \theta)$ denotes the block probability for the input data given the prediction parameters $\mathbf{a}$ and the probability distribution parameters θ. The $\alpha()$-function sets the behavior for the parameter description costs, i.e., the redundancy for not knowing the parameters.

For practical use it might not be feasible to calculate or to find a closed form expression for the block probability $P_B()$. For this reason we use the local optimization method as a tool since it will be possible to approximate the block probability. The precision in the approximation will, however, influence the performance of the redundancy.

In our suggested scheme we find the next symbol probability distribution according to $P_{lo}(y) = P_B^*(\mathbf{x}y) / \sum_i P_B^*(\mathbf{x}i)$ where the max-probability function is determined by $P_B^*(\mathbf{x}) = \max_{\mathbf{a}} \max_{\theta} \alpha(\mathbf{a}, \theta) P_B(\mathbf{x}, \mathbf{a}, \theta)$. For the Gaussian probability distribution we have used an approximate distribution function and then simplified the max-probability function further by finding the parameter $\mathbf{a}$ by a least square criteria followed by finding the parameter θ, i.e., individual maximization. Our tests show a superior redundancy performance compared to traditional methods.

References

[1] J. Rissanen, "Universal Coding, Information, Prediction and Estimation", *IEEE Trans. on Information Theory*, July 1984.

[2] Y. Shtarkov, "Universal Sequential Coding of Single Messages", *Problems of Information Transmission*, July-Sept 1987.

[3] Merhav and Feder, "Universal Prediction", *IEEE Trans. on Information Theory*, Oct. 1998.

[4] N. Ekstrand, "Some Results on Lossless Compression of Grayscale Images", Tekn. lic. thesis 1998, Lund University.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On the Reliable Throughput Supported by Multiple-Antenna Rayleigh-Faded Links for QAM Coded Transmissions

E. Baccarelli, G. Di Blasio, A. Fasano, A. Zucchi

INFO-COM Dpt., University of Rome "La Sapienza", Via Eudossiana 18, 00184 Rome, Italy
e-mail: enzobac@wsghepardo.ing.uniroma1.it

Abstract – **In this short contribution we present some novel results about the reliable information-rates supported by point-to-point multiple-antenna Rayleigh-faded wireless links for QAM coded data-transmissions. After deriving the (symmetric) capacity of these links, we present *fast-computable* analytical upper and lower bounds that are asymptotically exact *both* for high and low SNR's and give rise to reliable evaluation of the link-capacity. The proposed bounds apply when (perfect) Channel-State-Information (CSI) is available at the receiver and allow us to understand clearly the ultimate performance of the considered multiple-antenna QAM systems. Furthermore, asymptotically exact simple upper bounds are also presented for a tight evaluation of the corresponding outage probability when quasi-static fading occurs and coded packet-transmission with interleaving is used.**

EXTENDED SUMMARY

The growing demand for high-throughput wireless services experienced in the last years motivates the design of digital transmission systems able to convey increasing data-rates without substantial bandwidth-expansion. At the present, typical cellular wireless standards support data-services at about 9-10 kb/s but, recently, there has been interest in providing more sophisticated services at ISDN-compatible data-rates exceeding 100 kb/s using the cellular spectrum. Since the wireless channel is inherently band-limited by multipath phenomena, bandwidth-efficient coding with diversity constitutes an effective means in coping with the deleterious effects of fading. Although wireless systems with multiple antennas at the receiver are today quite common, several important contributions [1,2,6] have recently pointed out that space-diversity at the transmitter can give rise to an extraordinary improvement in the reliable rates conveyable by wireless bandwidth-limited links when CSI is available at the receiver and this last also employs space-diversity (see [8] for a comprehensive reference list on this topic). The ultimate reliable throughput supported by point-to-point Rayleigh-faded links with multiple transmit/receive antennas has been evaluated in [1,2] for continuous Gaussian-shaped coding alphabets and it has been found to scale linearly with the number of the transmit/receive antennas, becoming unbounded for large SNR's. Motivated by these promising information-theoretic results, several coding strategies suitable for actual implementations have been more recently presented [3,4,5,6].

Since the coded systems presented in the contributions provide data-transmissions and then rely on *finite-size* QAM-type constellations, a natural question that is still unanswered concerns the reliable rates effectively supported by multiple-antenna/point-to-point wireless systems which employ *finite-size* data-constellations and are *peak-power* limited (at this regard, we remark that in [1,2] only the case of continuous coding alphabet with an *average* power-constraint is addressed). In this contribution we attempt to give an answer to this question. In particular, we consider a point-to-point multiple-antenna link affected by flat Rayleigh-distributed fadings and under the assumption of perfect CSI at the receiver we compute the (symmetric) Shannon capacity of the coded channel for QAM transmissions. Since the formula for the capacity resists to a closed-form evaluation and its computation requires multiple nested numerical integrations, we present some fast-computable upper and lower bounds which provide reliable (and asymptotically exact) evaluation of the capacity. In addition, the proposed bounds *also unveil* the ultimate performance limits of peak-power-limited QAM multiple-antenna faded links and point out the impact on the capacity of some important system parameters such as, for example, the number of transmit/receive antennas, the constellation size and the employed (average) SNR.

Finally, since actual cellular wireless systems may be impaired by slow-variant (i.e., quasi-static) fading that, by fact, makes meaningless the link-capacity [7,8], in the last part of this contribution we investigate on the outage probability of point-to-point QAM multiple-antenna systems. Being the latter *not analytically computable* in a closed form, we present some simple Chernoff-type upper-bounds which are *asymptotically exact* and can be utilized in practice for a reliable evaluation of the actual outages. In addition, these bounds directly stress the impact of the number of employed antennas and the interleaving depth on the performance of the considered QAM systems when "block-fading" phenomena affect the transmission link between transmit/receive antennas.

REFERENCES

[1] G.J. Foschini, M.J. Gans, "On Limit of Wireless Communications in Fading Environment when Using Multiple Antennas", *Wireless Personal Communications*, Vol.6, no.3, pp.311-335, June 1998.

[2] E. Teletar, "Capacity of Multiantenna Gaussian Channel", AT&T Bell Labs, Techn. Memo., 1995.

[3] V. Tarokh, N. Seshadri, A.R. Calderbank, "Space-time Codes for High Data Rate Wireless Communications: Performance Criterion and Code Construction", *IEEE Trans. on Inform. Theory*, vol.44, no.2, pp.744-765, March 1998.

[4] V. Tarokh, H. Jafarkhani, A.R. Calderbank, "Space-Time Block Coding for Wireless Communications: Performance Results", *IEEE Journ. on Sel. Ar. in Comm.*, vol.17, no.3 pp.451-460, March 1999.

[5] A.F. Naguib, V. Tarokh, N. Seshadri, A.R. Calderbank, "A Space-Time Coding Modem for High-data rate Wireless Communications", *IEEE Jour. on Sel. Ar. in Comm.*, vol.16, no.8, pp. 1459-1477, October 1998.

[6] G.G. Raleigh, J.M. Cioffi, "Spatio-temporal Coding for Wireless Communication", *IEEE Trans. on Comm.*, vol.46, no.3, pp.357-366, March 1998.

[7] G. Kaplan, S. Shamai, "Error Probabilities for the Block-Fading Gaussian Channel", A.E.U., vol.49, no.4, pp. 192-205, April 1995.

[8] E. Biglieri, J. Proakis, S. Shamai, "Fading Channels: Information-Theoretic and Communications Aspects", *IEEE Trans. on Inform. Theory*, vol.44, no.6, pp. 2619-2692, October 1998.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Code Design for Combined Channel Estimation and Error Correction Coding

Mikael Skoglund and Stefan Parkvall[1]
Signals, Sensors, and Systems
Royal Institute of Technology
SE-100 44 Stockholm, Sweden
{skoglund,parkvall}@s3.kth.se

Abstract — **The problem of data transmission over an unknown channel is considered and an approach to code design for *joint* channel estimation, equalization and error correction is proposed. In contrast to most traditional approaches, where the receiver is designed given knowledge of the code used at the transmitter, this paper proposes an approach where the code is designed based on knowledge of the receiver structure and the statistical properties of the channel.**

I. System Model

Consider one-shot transmission of a binary block, $\mathbf{b} \in \{\pm 1\}^N$, over a linear filter channel using binary modulation. Assume that for each transmitted block, $\mathbf{b}$, a complex vector-valued output, $\mathbf{y} = \mathbf{B} \cdot \mathbf{h} + \mathbf{n} \in \mathbb{C}^L$, is measured at the receiver, where $\mathbf{n} \in \mathbb{C}^L$ is zero-mean complex Gaussian noise, and $\mathbf{B}$ is a matrix containing the transmitted bits; $(\mathbf{B})_{ij} = (\mathbf{b})_{i-j+1}$ for $j \le i$ and $i-j+1 \le N$, and $(\mathbf{B})_{ij} = 0$ otherwise. The channel coefficients $\mathbf{h} \in \mathbb{C}^P$ (with $P = L - N + 1$, assuming $P \le N$) are drawn from a complex-valued Gaussian distribution and are assumed constant over the transmission of one block, $\mathbf{b}$, but are allowed to vary between blocks. Furthermore, it is assumed that the realization of $\mathbf{h}$ is *unknown* both at the transmitter and at the receiver. A detailed description of the system and the assumptions made can be found in [1].

Since the P channel coefficients in $\mathbf{h}$ are unknown, the receiver implements joint maximum likelihood (ML) estimation of $\mathbf{h}$ and detection of the transmitted bits, $\mathbf{b}$, that is $(\hat{\mathbf{h}}, \hat{\mathbf{b}}) = \arg\min_{\mathbf{b}\in\mathcal{C}, \mathbf{h}\in\mathbb{C}^P} \|\mathbf{y} - \mathbf{B}\mathbf{h}\|^2$. Hence,

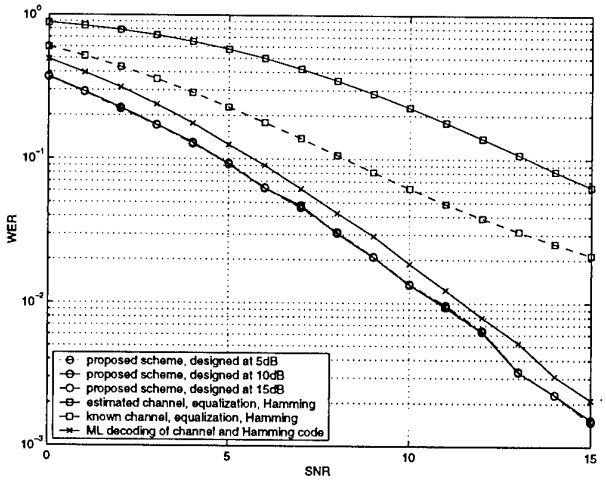
$$\hat{\mathbf{b}} = \hat{\mathbf{b}}(\mathbf{y}) = \arg\min_{\mathbf{b}\in\mathcal{C}} \|\mathbf{y} - \mathbf{B}\mathbf{B}^+\mathbf{y}\|^2,$$

where $\mathcal{C} \subset \{\pm 1\}^N$ is the set of allowed *codewords* and $\mathbf{B}^+$ is the pseudo-inverse of $\mathbf{B}$. The mapping $\hat{\mathbf{b}} : \mathbb{C}^L \to \{\pm 1\}^N$ is the *decoder* of the system. The operation of this mapping includes (implicit) channel identification. The decoder output, $\hat{\mathbf{b}}$, is, however, a function of $\mathbf{y}$ *only*, and a particular received vector is always mapped into the same $\hat{\mathbf{b}}(\mathbf{y})$.

II. Code Design and Performance

The problem of code design is that of choosing the set of codewords, $\mathcal{C}$, for a given value of $|\mathcal{C}| < 2^N$, such that the word error rate (WER), $\Pr(\hat{\mathbf{b}}(\mathbf{y}) \neq \mathbf{b})$, is minimized *without explicit knowledge of the channel.* Note that this implies that the code must allow for both estimation of the channel impulse response, as well as providing good error correcting capabilities. That is, $\mathcal{C}$ is to be chosen such that it provides an optimal *combination* of *redundancy* for *channel estimation* ("training data") and *error protection.* Finding the optimal set of code words, $\mathcal{C}$, is a integer optimization problem, which, in general, is very hard to solve. Therefore, an approach based on simulated annealing [2] is used herein, where the energy of the system is given as a function of the WER. Unfortunately, the WER is, in general, hard to derive and therefore a technique based on the union bound is used instead. The union bound gives an upper bound on the WER, given knowledge of the pairwise error probabilities. These can be calculated using a moment generating function approach and closed form expressions are available for both Rice and Rayleigh channels [1].

The proposed scheme has been used to design a rate $\log_2|\mathcal{C}|/N = 1/2$ code for a channel with $P = 2$ equally strong Rayleigh fading paths. Three reference cases are also considered: The first scheme uses 7 pilot bits for least squares channel estimation, Viterbi equalization and hard decoding of a (15,11) Hamming code, resulting in an overall code rate of $11/(15+7) = 1/2$. The second scheme is identical to scheme one except that the equalizer is provided with genie aided channel estimates. Finally, the third reference scheme uses optimal ML decoding of the overall code defined by concatenating the 7 pilot bits and the Hamming (15,11) code [1].



As can be seen in the figure, the proposed coding approach significantly outperforms the other cases, clearly illustrating the performance benefit of designing the code for joint channel estimation and error protection. Furthermore, in [1] it is illustrated that the new scheme is quite insensitive to mismatch in the design parameters compared with their true values.

[1]This work was partially funded by the Swedish Research Council for Engineering Sciences, under grant 271-99-194.

References

[1] M. Skoglund and S. Parkvall, "Code design for combined channel estimation and error protection" *Submitted to IEEE Transactions on Information Theory*, Feb. 2000.

[2] S. Kirkpatrick, J. C. D. Gelatt, and M. P. Vecchi, "Optimization by simulated annealing" *Science*, vol. 220, no. 4598, pp. 671–680, 1983.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Optimal 4- and 8-State Across-the-subchannels TCM Encoders for DMT Systems

V. Shashidhar
Department of Electrical Communication Engineering
Indian Institute of Science
Bangalore 560 012
India
shashidhar@protocol.ece.iisc.ernet.in

B. Sundar Rajan[1]
Department of Electrical Communication Engineering
Indian Institute of Science
Bangalore 560 012
India
bsrajan@ece.iisc.ernet.in

V .Umapathi Reddy[2]
Department of Electrical Communication Engineering
Indian Institute of Science
Bangalore 560 012
India
vur@ece.iisc.ernet.in

Abstract — **We give the optimal 4- and 8-state trellises for across-the-subchannels TCM for DMT systems.**

I. Introduction

TCM can be performed for DMT systems in two ways : coding parallely and coding across the subchannels. The decoding delay in the latter case is M times less than that in the former case, where M is the number of subchannels [1]. We refer the latter as across-the-subchannels TCM for DMT systems.

At the receiever input, the SNR's in different subchannels are different due to the channel impulse response. Thus, the minimum weighted Euclidean distance becomes the decision criteria for ML decoding, and hence we use weighted Viterbi decoding. Due to this weighting, the best trellis known for single carrier systems need not be the best in our case.

II. Classification of Trellises

We classify all the S-state trellises into γ classes (where $\gamma = \log_2 S$) as $\left\{S^{(2^x;p)} : 1 \leq x \leq \gamma\right\}$, where $S^{(2^x;p)}$ denotes an S-state trellis with a node at a level connected to 2^x nodes in the next level and having 2^p parallel transitions. We label the top most node as s_0 and the last node as $s_{2^\gamma-1}$.

Definition 1 : A cyclic trellis is a trellis in which the branches diverging from a node s_n at any level connect to 2^{b-p} nodes of the next level, beginning from $s_{(n\cdot 2^{b-p}) \bmod 2^\gamma}$ and ending at $s_{((n+1)\cdot 2^{b-p}-1) \bmod 2^\gamma}$, where b is the number of input bits per symbol.

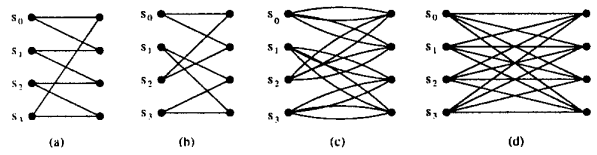


Figure 1: Some possible 4-state trellises : (a) $4^{(2;0)}$ non-cyclic (b) $4^{(2;0)}$ cyclic (c) $4^{(2;1)}$ cyclic (d) $4^{(4;0)}$ cyclic

Definition 2 : The Convergence length of a trellis is defined as the minimum of all lengths of pairs of paths that diverge from a node, excepting the parallel transitions, and converge at another node.

The upper bound on the convergence length of a trellis is given by [2]

$$L_{max} = \lfloor \frac{\gamma}{b_1} \rfloor + 1$$

where b_1 refers to that part of the input bits which affects the state of encoder and $\lfloor x \rfloor$ denotes the largest integer less than or equal to x.

Theorem 1 : The convergence length of a cyclic trellis is equal to L_{max}, i.e., cyclic trellises achieve the upper bound on the convergence length.

III. Optimal 4- and 8-State Trellises

Let $b_{min} = \min_{i\in[0,M-1]}\{b_i\}$, where b_i is the number of input bits in i^{th} subchannel and $s_t w_t = \min_{i\in[0,M-1]}\{s_i w_i\}$, where s_i and w_i are the squared miniumum Euclidean distance of the i^{th} subchannel symbol constellation and weighting factor for that subchannel, respectively.

Theorem 2 : The best trellis for 4-state across-the-subchannels TCM is
(a) the $4^{(2;0)}$ cyclic trellis, for $b_{min} = 1$,
(b) the $4^{(4;b_{min}-2)}$ cyclic trellis if

$$\min_{i\in[0,M-1]} \{2s_i w_i + s_{i\oplus 1} w_{i\oplus 1}\} > 4 s_t w_t$$

else the $4^{(2;b_{min}-1)}$ cyclic trellis, for $b_{min} \geq 2$.

Theorem 3 : The best trellis for 8-state across-the-subchannels TCM is
(a) the $8^{(2;0)}$ cyclic trellis, for $b_{min} = 1$,
(b) the $8^{(4;0)}$ cyclic trellis, for $b_{min} = 2$,
(c) the $8^{(8;b_{min}-3)}$ cyclic trellis if

$$\min_{i,k\in[0,M-1]} \{2s_i w_i + s_k w_k\} > 8 s_t w_t$$

else the $8^{(4;b_{min}-2)}$ cyclic trellis, for $b_{min} \geq 3$.

Acknowledgments

B.S.Rajan gratefully acknowledges IBM India Research Lab, for the travel support to present this paper.

References

[1] J. A. C. Bingham, "Multicarrier Modulation for Data Transmission: An Idea Whose Time Has Come," *IEEE Communication Magazine*, pp.5-14, May 1990.

[2] S. Hamidreza Jamali and Tho Le-Ngoc, "Coded-modulation Techniques for Fading Channels," *Kluwer Academic Publishers*, 1994.

[1]This work was partly supported by CSIR, India, through Research Grants (No:25(0086)/97/EMRI-II) and (22(0298)/99/EMR-II) to B.S.Rajan

[2]This work was supported in part by DARPA Grant F49620-95-1-0525-P00005 during his stay at Stanford university.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Coding for Noncoherent Communication

Dilip Warrier[1]
Aware Inc.,
40 Middlesex Turnpike,
Bedford, MA 01730, USA.
e-mail: dwarrier@aware.com

Upamanyu Madhow
Dept. of ECE,
Univ. of California,
Santa Barbara, CA 93106, USA.
e-mail: madhow@ece.ucsb.edu

Ralf Koetter
Dept. of ECE and Coordinated
Science Laboratory,
Univ. of Illinois,
Urbana, IL 61801, USA.
e-mail: koetter@uiuc.edu

Abstract — **In this paper, we consider noncoherent communication over a frequency nonselective channel. Results from coherent coding theory are used to devise both low and high rate codes for noncoherent systems. Further, one-dimensional noncoherent codes with good Hamming distance properties can be transformed into space-time noncoherent codes which achieve full transmit diversity using a block transformation.**

I. Introduction

Noncoherent transmission is considered over a frequency nonselective channel. The channel gain is assumed to be unknown but piecewise constant over a length of time called the *coherence interval* (and denoted by N), which lasts several symbol durations. In prior work [1], a noncoherent "distance" was identified as a performance measure for noncoherent codes, analogous to the Euclidean distance in the coherent case. Also, a near-optimal algorithm of linear complexity was found for noncoherent demodulation. This work considers the design of one-dimensional and space-time codes for noncoherent channels, with a focus on adapting simple coherent codes for the noncoherent setting.

II. One-dimensional noncoherent codes

Our results so far indicate that the vast body of knowledge regarding coherent codes can be leveraged, with appropriate modifications, to obtain noncoherent codes. First, the low rate case is considered. A noncoherent code $\mathcal{S}_{\rm nc}$ can be obtained from a linear binary code $\mathcal{S}$ containing the all ones codeword as the set of equivalence classes of $\mathcal{S}$, where an equivalence class consists of a vector in $\mathcal{S}$ and its complement. In this case, the minimum noncoherent distance of $\mathcal{S}_{\rm nc}$, as formulated in [1], can be shown to be proportional to the minimum Hamming distance of $\mathcal{S}$. Hence, the choice of a good coherent linear binary code for $\mathcal{S}$ yields a good low-rate noncoherent code $\mathcal{S}_{\rm nc}$. In particular, the $(7,4,3)$ Hamming code yields an optimal set of 8 vectors of length $N = 7$ on a unit sphere, for the noncoherent setting.

For the high rate case, multilevel coding can be employed to yield good noncoherent codes. Varying degrees of protection are provided to each bit position in the bit labeling of symbols, using stronger or weaker codes. The linear complexity algorithm for the uncoded case can be extended to the multilevel coding case, resulting in a low-complexity demodulation algorithm. Simulation results show that a (7,4,3) Hamming code applied to the least significant bit of an 8-PSK alphabet with Ungerboeck-set partitioning gives a performance 1.5 dB better than 8-QAM.

[1]This work was supported by the National Science Foundation under a CAREER award NSF NCR96-24008CAR.

III. Space-time codes

A *space-time code* consists of matrices of size $N \times N_t$ where N_t is the number of transmitter antennae (known as space-time codewords) where the $i^{\rm th}$ column denotes the symbols transmitted over antenna i from time 1 to N. A common design goal for space-time codes is to achieve full diversity, which implies that the symbol error probability decays asymptotically as $1/\mathrm{SNR}^{N_t}$, where SNR denotes the signal-to-noise ratio and it is assumed that $N \geq N_t$.

In the noncoherent case, full diversity gain can be shown to be achieved by a code, if for every pair of codewords Φ, Θ, the matrix $(\ \Phi \quad \Theta - \Phi\ )$ has full column rank. In comparison, full coherent diversity gain is achieved if $\Theta - \Phi$ has full column rank. Thus, the following remark holds.

Remark

A space-time code that achieves full diversity in the noncoherent case also achieves full diversity in the coherent case, although the converse does not hold.

Space-time codes that achieve full noncoherent diversity gain can be derived from one-dimensional noncoherent codes, as a result of the following theorem.

Theorem

Consider a code C such that, for every codeword $\mathbf{c} = (c_0, c_1, \ldots, c_{N-1})^T$ in C, $|c_i| = \frac{1}{\sqrt{N}}$ $\forall i = 0, 1, \ldots, N-1$, and a noncoherent space-time code $\mathcal{S}_{\rm nc}$ whose codewords are derived from C as

$$\Phi(\mathbf{c}) = \begin{pmatrix} c_0 & c_0 & \ldots & c_0 \\ c_1 & c_1 z & \ldots & c_1 z^{N_t-1} \\ \vdots & \vdots & & \vdots \\ c_{N-2} & c_{N-2} z^{N-2} & \ldots & c_{N-2}(z^{N_t-1})^{N-2} \\ c_{N-1} & c_{N-1} z^{N-1} & \ldots & c_{N-1}(z^{N_t-1})^{N-1} \end{pmatrix}$$

where $z = \exp\left(j\frac{2\pi}{N}\right)$ is an $N^{\rm th}$ root of unity. Then, $\mathcal{S}_{\rm nc}$ achieves full noncoherent diversity gain if and only if $N_t \leq N/2$ and the Hamming distance d_H of C satisfies $N_t \leq d_H \leq (N - N_t)$.

The preceding link between one-dimensional and space-time codes enables us to exploit constructions for one-dimensional noncoherent codes (e.g., the multilevel codes of Section II) for the design of space-time noncoherent codes. The interested reader is referred to [2] for details.

References

[1] D. Warrier and U. Madhow, "Noncoherent communication in space and time," in *Conference on Information Sciences and Systems*, The Johns Hopkins University, Baltimore, MD, USA, March 1999.

[2] D. Warrier, *A Framework for Spectrally Efficient Noncoherent Communication*, Ph.D. thesis, Univ. of Illinois, Urbana-Champaign, 2000.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Feedback Regulation for Sequencing and Routing in Multiclass Queueing Networks

Sean P. Meyn[1]
Coordinated Science Laboratory
1308 W. Main Street
Urbana, IL 61801
e-mail: s-meyn@uiuc.edu.

Abstract —

This paper establishes new criteria for stability and for instability of multiclass network models under a given sequencing or routing policy. It also extends previous results on the approximation of the solution to the average cost optimality equations through an associated fluid model: It is shown that an optimized network possesses a fluid limit model which is itself optimal with respect to a total cost criterion. A full version of the paper is available at `http://black.csl.uiuc.edu:80/~meyn`.

I. Introduction

A traditional academic approach to scheduling and routing is to construct a Markov decision process model for the network. This involves constructing a controlled transition operator $P_a(x, y)$, which gives the probability of moving from state x to state y when the *control decision* a is applied. The state space X where x and y live are typically taken as the set of all possible buffer levels at the various stations in the network.

Given an MDP model, and a one step cost function $c\colon \mathsf{X} \to \mathbb{R}_+$, a solution to the average cost optimal control problem is found by solving the resulting dynamic programming equations. The difficulty with this approach is very well known: When buffers are infinite, this becomes an infinite dimensional optimization problem. Even when considering finite buffers, the complexity grows exponentially with the dimension of the state space. Hence some form of aggregation is necessary - the Markovian model is simply too detailed to be useful in optimization.

An elegant approach is to consider the model in heavy traffic where a reflected Brownian motion model is appropriate. The paper [2], and many others, develop these ideas for the network scheduling or sequencing problems. One is then faced with optimizing a controlled stochastic differential equation (SDE) model.

This paper builds upon the results of [5, 1]. We develop a general framework for constructing control algorithms for multiclass queueing networks based on a fluid model. Network sequencing and routing problems are considered as special cases. The following aspects of the resulting *feedback regulation policies* are developed in the paper:

(i) The policies are stabilizing, and are in fact geometrically ergodic for a Markovian model.

(ii) Numerical examples are given. In each case it is shown that the feedback regulation policy closely resembles the average-cost optimal policy.

(iii) A method is proposed for reducing variance in simulation for a network controlled using a feedback regulation policy.

The viewpoint arrived at in this paper leads to policies which are similar to those found through a heavy traffic analysis using a Brownian motion approximation. In all of the network models which have been considered to date, one could perform designs on the fluid model, translate these policies as described in the paper, and arrive at the same policy that was obtained using a Brownian motion approximation. Given the greater complexity of the Brownian motion model, we conclude that while diffusion approximations are tremendously useful for analysis, they appear to be less useful for the puposes of control design.

[1] Work supported in part by NSF Grants ECS 9403742, ECS 99 72957.

References

[1] D. Eng, J. Humphrey and S.P. Meyn. Fluid network models: Linear programs for control and performance bounds. In J. Cruz J. Gertler and M. Peshkin, editors, *Proceedings of the 13th IFAC World Congress*, volume B, pages 19–24, San Francisco, California, 1996.

[2] J.M. Harrison. The BIGSTEP approach to flow management in stochastic processing networks, pages 57–89. *Stochastic Networks Theory and Applications*. Clarendon Press, Oxford, UK, 1996. F.P. Kelly, S. Zachary, and I. Ziedins (ed.).

[3] J. M. Harrison. Brownian Models of Open Processing Networks: Canonical Representations of Workload. *Preprint*. 1–29, 1999.

[4] S.G. Henderson and S.P. Meyn. Variance reduction for simulation in multiclass queueing networks. *submitted to the IIE Transactions on Operations Engineering: special issue honoring Alan Pritsker on simulation in industrial engineering*, 1999.

[5] S.P. Meyn. Stability and optimization of multiclass queueing networks and their fluid models. volume 33 of *Lectures in Applied Mathematics*, pages 175–199. American Mathematical Society, 1997.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Measurement-Based Network Monitoring: Missing Data Formulation and Scalability Analysis

Chuanyi Ji
Department of Electrical Computer and System Engineering
Rensselaer Polytechnic Institute
Troy, NY 12180

Anwar Elwalid
Department of Mathematics of Networks and Systems
Bell-labs Lucent Technologies
Murray Hill, NJ 07974-0636

Abstract — **Although of practical importance to managing large IP networks, measurement-based network monitoring using distributed monitors has not been rigorously formulated nor investigated. This work develops a missing data framework for distributed monitoring based on multicast, and investigates, through density estimation, how resources needed for network monitoring scale with the size of the network under various network (loss) conditions. The results on the scalability provide insights into feasibility of using only edge monitors, and provide design guidelines for future network management systems.**

I. Missing Data Formulation

To assist network managers in monitoring large and heterogeneous networks in dynamic environments, network monitors can be allocated at either the interior or the edges of a managed network to monitor Quality of Service (QoS) measures such as packet loss or delay. Even if network monitors are deployed everywhere in the network, some of them may be occasionally inaccessible for various reasons. Hence, a general formulation of network monitoring should consider this missing information aspect.

We have developed a general theoretical framework for network monitoring using distributed monitors based on missing data formulation [3], where (a set (U) of) missing variables correspond to unobservable network nodes where monitors are neither available nor accessible, and (a set (O) of) observable variables correspond to nodes with functional monitors. Our model is in the form of the complete likelihood on both observable and missing variables. We consider network monitoring in the context of multicast probing [2], where network monitors measure the number of probe packets lost at the nodes of a multicast tree. Define the state X_j of node j to be a binary random variable, where $X_j = 1$ if node j receives a probe packet, and $X_j = 0$, otherwise. The resulting complete likelihood function possesses a very simple analytical form

$$\Pr(X_j = x_j, \forall j) = \prod_{j=1}^{L} \{\alpha_j^{x_{f(j)} x_j} [(1-\alpha_j) C_j]^{x_{f(j)} - x_{f(j)} x_j}\}, \quad (1)$$

where the parameter $\alpha_j = \Pr(X_j = 1 \mid X_{f(j)} = 1)$ with node $f(j)$ being the parent of node j, x_j equals to 0 or 1, L is the depth of a multicast tree, and C_j is quantity which does not depend on α_j's. As such a model belongs to an exponential parametric family, it results in a simple Expectation-Maximization algorithm to estimate the unknown parameters, α_j's, corresponding to unobservable nodes.

II. Scalability Analysis

The estimation error between the true (α_j^*'s) and estimated parameters ($\hat{\alpha}_j$'s) given measurements D_{obs} (losses measured by monitors) can be related to the convergence rate as

$$\mathbf{E}[\sum_{j \in U \bigcup O} (\alpha_j^* - \hat{\alpha}_j)^2 \mid D_{obs}] = \sum_{j \in U} \frac{\hat{\sigma}_j^2}{n \hat{\lambda}_j} + \sum_{j \in O} \frac{(1-\hat{\alpha}_j)\hat{\alpha}_j}{n} + e, \quad (2)$$

where e is an error term depending on the missing information, $\hat{\sigma}_j^2$ corresponds to the complete information for the j-th unobservable node[3], $\hat{\lambda}_j$ is the convergence rate of the j-th EM equation and n is the number of probes.

Using the theory of density estimation[1], we define the scalability of measurement-based network monitoring in terms of how the estimation error and the convergence rate vary with respect to the number of probes and the size of a multicast tree under various network conditions. For a uniform multicast tree[1] with small packet loss ($\alpha_j = 1 - o(1), \forall j$) and assuming only edge monitors, the estimation error is $O(\frac{M}{n})$ with M being the total number of unobservable nodes, and the convergence rate $\hat{\lambda}_j = 1 - o(1), \forall j$. This corresponds to the best achievable scalability suggested by density estimation. When packet losses are large across the multicast tree ($\alpha_j = o(1), \forall j$), the estimation error is $O(\frac{1}{\beta^L} \frac{M}{n})$ with $0 < \beta < 1$, and $\hat{\lambda}_j = o(1), \forall j$. This corresponds to the worst scalability with an exponentially large number of probes in the depth of a multicast tree, and an exponentially slow convergence rate. When large losses occur locally, properly allocated distributed monitors can improve the scalability to the best achievable.

References

[1] A. Barron, T.M.Cover, " Minimum Complexity Density-Estimation," *IEEE Trans Information Theory*, 37: (4) 1034-1054 July 1991.

[2] R. Caceres, N.G. Duffield, J. Horowitz, D. Towsley "Multicast-based Inference of Network-Internal Loss Characteristics" *IEEE Transactions on Information Theory*, November 1999.

[3] A. Dempster, N. Laird, and D. Rubin, "Maximum Likelihood from Incomplete Data via the EM Algorithm," *Journal of Royal Statistical Society, B* 39:1-38.

Acknowledgments

CJ gratefully acknowledges the hospitality and support from Debasis Mitra and the Department of Mathematics of Networks and Systems at Bell-labs Lucent Technologies during her sabbatical when this work was performed, and the support from NSF and DARPA.

[1] with the same packet loss probability at all network nodes

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Time-Varying Network Tomography: Router Link Data

Bin Yu[1], Jin Cao, Drew Davis, and Scott Vander Wiel
Bell Laboratories, Lucent Technologies
600 Moutain Ave., Murray Hill, NJ 07974, U.S.A.
e-mail: binyu@research.bell-labs.com

Abstract — **In a computer network, the traffic matrix or the origin-destination (OD) byte counts are important statistics needed for design, routing, configuration debugging, monitoring and pricing. However, they are not easily available. For a fixed routing scheme, a statistical inverse algorithm is proposed and validated to estimate the traffic matrix from the easily collectable link counts which are aggregations of the origin-destination counts.**

I. Introduction

Practical realities dictate that information needed for managing computer networks is sometimes best obtained through estimation. This is true even though exact measurements could be made by deploying specialized hardware and software. We consider estimation of origin-destination byte counts from measurements of byte counts on network links. All commercial routers can report their link counts through the Simple Network Management Protocol (SNMP), whereas measuring complete OD counts on a network is far from routine. The problem of estimating the OD byte counts from aggregated byte counts measured on links is called *network tomography* by Vardi [1]. The similarity to conventional tomography lies in the fact that the observed link counts are linear transforms of unobserved OD counts with a known transform matrix determined by the routing scheme.

II. A Moving IID Gaussian Model with a Mean-Variance Relationship

We [2] study the inference of OD byte counts from link byte counts measured at router interfaces under a fixed routing scheme. A basic model of the OD counts assumes that they are independent normal over OD pairs and iid over successive measurement periods. The normal means and variances are functionally related through a power law. We deal with the time-varying nature of the counts by fitting the basic iid model locally using a moving data window. Identifiability of the model is proved for router link data and maximum likelihood is used for parameter estimation. The OD counts are estimated by their conditional expectations given the link counts and estimated parameters. OD estimates are forced to be positive and to harmonize with the link count measurements and the routing scheme.

Simple local likelihood fitting of an iid model is not sufficient because large fitting windows over-smooth sharp changes in OD traffic, while a small windows cause estimates to be unreliable. A refinement in which the logs of positive parameters are modeled as random walks, penalizes the local likelihood surface enough to induce smoothness in parameter estimates while not unduly compromising their ability to conform to sharp changes in traffic. We use a fully normal approximation to this approach and demonstrated how effectively it recovers OD byte counts for our chosen network.

[1]Bin Yu is on leave from University of California, Berkeley.

III. Validation with real data

The proposed method is applied to two simple networks at Lucent Technologies. OD counts are shown to be recovered with good accuracy relative to the degree of ambiguity that remains after marginal and positivity constraints are met. Furthermore, the estimates are validated in a single-router network for which direct measurements of origin-destination counts are available through special software.

IV. A scalable algorithm for large networks

It can be seen that for a network of n origins (destinations), the computational cost of our proposed method will be at least of order $O(n^5)$ even after taking advantage of sparse matrix computation. Even for a network of a moderate size (e.g. $n = 100$), this is not acceptable.

Since the OD counts come with an estimation accuracy, the optimization problem in our method does not have to be solved exactly. This suggests that we could choose subproblems of smaller size to apply our method so that the estimation accuracy remains the same order of magnitude as the full problem but the computational cost is greatly reduced.

A divide-and-conquer scalable algorithm has been devised based on the principle of local information – most of the information in estimating the parameters of a particular OD random variable comes from links nearby. Uner this principle, the OD pairs are clustered into groups, and for each group of OD pairs, links are selected. For each subproblem of an OD group and associated links, a parameter reduction is carried out to minimize the computational cost so that the computation cost of the algorithm is of $O(n^3)$. This algorithm can be used on its own or to find an initial estimate for the full problem.

We are currently implementing this algorithm on a large Lucent network. The results will be compared against those using the full approach.

Acknowledgments

We thank Tom Limoncelli and Lookman Fazal for system administration support in setting up MRTG and Netflow data collection. We also thank Debasis Mitra for pointing us to this problem and Yehuda Vardi and Mor Armony for engaging discussions.

References

[1] Y. Vardi, "Network Tomography: Estimating Source-Destination Traffic Intensities From Link Data," *Journal of the American Statistical Association*, vol. 91, pt. I, pp. 365-377, 1996.

[2] J. Cao, D. Davis, S. Vander Wiel, and B. Yu, "Time-varying network tomography: router link data," *Journal of the American Statistical Association*, submitted, 1999. http://cm.bell-labs.com/stat/binyu/publications.html

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Interval-valued Probability Modeling of Internet Traffic Variables

Pablo I. Fierens
School of Electrical Engineering
Rhodes Hall 319
Cornell University
Ithaca, NY 14853
pifierens@ee.cornell.edu

Terrence L. Fine[1]
School of Electrical Engineering
Rhodes Hall 388
Cornell University
Ithaca, NY 14853
tlfine@ee.cornell.edu

Abstract — **A methodology to build interval-valued probability models is presented. It is shown that this alternative produces temporally stable models of Internet-generated communications variables.**

I. Introduction

Experience with such Internet-generated communications variables as files sizes and packet delays suggests that they have variable statistical characteristics even when these characteristics are estimated from huge sample sizes. This variation is observed over medium duration (months) time periods and between sources of similar types. Thus the observed variations in the parameters of long-range dependent, heavy tailed models suggests the need for another class of mathematical models that can account for the observed common semi-quantitative behavior in a medium-range temporally stable manner.

To this end we turn to the foundations of probability for the class of interval-valued probabilities and more specifically to the subclass of upper and lower envelopes (an introduction can be found, e.g., in [2] and references therein). By doing so we will give up some of the ability of the standard probability models to describe detailed dynamics of the traffic variables in exchange for a more robust, temporally stable stochastic model.

II. Modeling: minimal extension, lower envelopes

We base our construction in the following concept (see Sadrolhefazi and Fine [2]):

Definition. *A kernel $(\mathcal{K}, \rho)$ is a pair with $\mathcal{K}$ a collection of subsets of a set Ω, that includes $\emptyset$ and Ω, and a set function ρ defined on $\mathcal{K}$ satisfying the following four modified axioms of a lower probability (i) $\rho(\Omega) = 1$; (ii) $(\forall A \in \mathcal{K})\rho(A) \geq 0$; (iii) $(\forall A, B \in \mathcal{K})\ A \cap B = \emptyset \Rightarrow \sup\{\rho(C) : C \in \mathcal{K}, C \subset A \cup B\} \geq \rho(A)+\rho(B)$ (superadditivity); (iv) $(\forall A, B \in \mathcal{K})\ 1+\sup\{\rho(C) : C \in \mathcal{K}, C \subset AB\} \geq \rho(A) + \rho(B)$ (conjugacy).*

Theorem. *Given a set Ω, a kernel $(\mathcal{K}, \rho)$, and any algebra $\mathcal{A} \supset \mathcal{K}$, there is a unique minimal extension of ρ to a lower probability $\underline{P}$ on $\mathcal{A}$, such that: (i) $\underline{P}$ agrees with ρ on $\mathcal{K}$; (ii) if $\underline{Q}$ is any other lower probability on $\mathcal{A}$ agreeing with ρ on $\mathcal{K}$, then $(\forall A \in \mathcal{A})Q(A) \geq \underline{P}(A)$.*

By partitioning the range of file sizes we find that several of the intervals of size contain many files, and therefore we are confident that a relative frequency estimate of their probability will have high accuracy. These events then lie in $\mathcal{K}$. In our case, we have frequentist-based probabilities of file size estimated from a variety of servers. We generate the kernel ρ for the events by taking the minima of the individual estimated probabilities. This process is guaranteed to generate a function ρ satisfying the definition of a kernel. We can then proceed to use minimal extension to complete the kernel to a lower envelope $\underline{P}$.

Table 1: File Sizes: 1993 data vs. 1999 data

Survey	Sample Mean	Sample Median	Sample Std. Dev.	Tail index
1993	21,368	1,536	1,024,534	≈ 1.2
1999	49,648	2,416	792,840	≈ 0.7

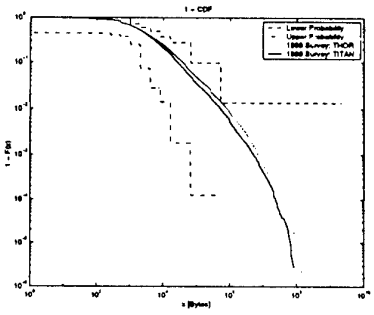


Figure 1: IVP model based on the 1993 Survey accounts well for the 1999 data

III. Application to Modeling Unix File Size Data Sets

Our data on Unix file sizes comes from two surveys:

1. An extensive survey was conducted in 1993 by Irlam ([1]): over 1,000 file systems of different organizations were surveyed, representing roughly 250 gigabytes distributed in approximately 12 million files.
2. A smaller survey was conducted in August 1999 on two Unix file servers, THOR and TITAN, of the Cornell Electrical Engineering department network, with roughly 1 million files, totaling 46.5 gigabytes.

Table 1 reveals some significant differences between the distributions of file sizes in both cases. However, as can be seen in Figure 1, an IVP model built as explained in the previous section and based on the 1993 Survey accounts well for the 1999 data.

References

[1] Irlam, G. [1994] Unix file size survey—1993, found at http://www.base.com/gordoni/ufs93.html.

[2] Sadrolhefazi, Amir, T.L. Fine [1994], Finite-dimensional distributions and tail behavior in stationary interval-valued probability models, *Annals of Statistics*, **22**, 1840–1870.

[1]This work was conducted with partial support from NSF Grant NCR-9725251.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Universal Linear Least-Squares Prediction

Andrew C. Singer
Department of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign
e-mail: acsinger@uiuc.edu

Meir Feder
Department of Electrical Engineering-Systems
Tel Aviv University
e-mail: meir@eng.tau.ac.il

Abstract — **An approach to the problem of linear prediction is discussed that is based on recent developments in the universal coding and computational learning theory literature. This development provides a novel perspective on the adaptive filtering problem, and represents a significant departure from traditional adaptive filtering methodologies. In this context, we demonstrate a sequential algorithm for linear prediction whose accumulated squared prediction error, for every possible sequence, is asymptotically as small as the best fixed linear predictor for that sequence.**

I. Linear Prediction

In this work, we consider the problems of adaptive filtering and linear prediction in a competitive algorithm framework. Given a data sequence $x^n = \{x[t]\}_{t=1}^n$, the optimal set of p coefficients, w_k, $k = 1, \ldots, p$, that minimizes the *total* prediction error

$$E_w[N] = \sum_{n=1}^{N} (x[n] - \sum_{k=1}^{p} w_k x[n-k])^2,$$

is uniquely determined and certainly depends on the input sequence. Recently, a linear prediction algorithm was presented that asymptotically achieves the minimum average *sequentially accumulated* prediction error over all linear predictors of order p, i.e. $\min_w E_w[N]$, for every individual sequence [1]. In this work, we somewhat modify the algorithm, and as a result improve both the algorithm performance, in terms of the bound on the redundancy, and provide a more intuitive proof of this bound.

II. p-th-Order Linear Prediction

We consider the problem of linear prediction with a filter of fixed-order p, parameterized by the vector $\vec{w} = [w_1, \ldots, w_p]^T$, with predicted value $\hat{x}_{\vec{w}}[n] = \vec{w}^T \vec{x}[n]$, where $\vec{x}[n] = [x[n-1], \ldots, x[n-p]]^T$. Let $x[n]$, $n = 1, \ldots, N$, be a bounded, but otherwise arbitrary, sequence such that $|x[n]| < A$, where A need not be known in advance. Let $l_n(x, \hat{x}_{\vec{w}})$ be the running total squared prediction error, i.e. $l_n(x, \hat{x}_{\vec{w}}) = \sum_{t=1}^n (x[t] - \hat{x}_{\vec{w}}[t])^2$. Define a universal predictor $\tilde{x}_u[n]$, as $\tilde{x}_u[n] = \vec{w}_u[n-1]^T \vec{x}[n]$, where, $\vec{w}_u[n] = \left[R_{xx}^{n+1} + \delta I\right]^{-1} r_{xx}^n$, $R_{xx}^n = \sum_{k=1}^n \vec{x}[k]\vec{x}[k]^T$, $r_{xx}^n = \sum_{k=1}^n x[k]\vec{x}[k]$, and $\delta > 0$ is a positive constant.

Theorem 1 *The total squared prediction error of the p-th-order universal predictor, $l_n(x, \tilde{x}_u) = \sum_{t=1}^n (x[t] - \tilde{x}_u[t])^2$, satisfies*

$$l_n(x, \tilde{x}_u) \leq \min_{\vec{w}} \left\{ l_n(x, \hat{x}_{\vec{w}}) + \delta \|\vec{w}\|^2 \right\} + A^2 \ln \left| I + R_{xx}^n \delta^{-1} \right|,$$

$$\frac{1}{n} l_n(x, \tilde{x}_u) \leq \min_{\vec{w}} \frac{1}{n} \left\{ l_n(x, \hat{x}_{\vec{w}}) + \delta \|\vec{w}\|^2 \right\} + \frac{A^2 p}{n} \ln \left(1 + \frac{A^2 n}{\delta} \right).$$

Theorem 1 states that the average squared prediction error of the p-th-order universal predictor is within $O(A^2 p \ln(n)/n)$ of the best batch p-th-order linear prediction algorithm, for every individual sequence x^n. The idea behind the universal predictor and the proof of the Theorem is as follows. We define a "probability" assignment of each of the continuum of predictors $\vec{w} \in R^p$ to the data sequence x^n such that the probability will be an exponentially decreasing function of the total squared-error for that predictor. Over the continuum of predictors with coefficients $\vec{w}$, we assign a Gaussian prior over these probabilities, and define the universal probability to be the Bayesian mixture of these probabilities. With the Gaussian prior, we can obtain the universal probability in closed form. Since the probabilities assigned by every predictor can also be found in closed form, we can compare the universal probability to that of the best batch predictor for each sequence.

We note that the conditional universal probability is Gaussian distributed about same Bayesian (time-varying) mixture of predictor outputs as that applied to the individual predictor probabilities, however it is not in the form of an exponentially decreasing function of the prediction error of a particular predictor. In [1], the conditional mean of this distribution was used as a predictor and was shown to be universal using a convexity argument to bound its excess prediction error. However, the convexity argument required construction of a new Gaussian, centered about the same mean, which was both larger than the universal probability over the range of the data and also in the form of an exponentially decreasing function of the accumulated prediction error. This led to a redundancy proportional to $O(4A^2 p \ln(n)/n)$, four times larger than that achieved here. In this work, we search for a new Gaussian in the proper form, with a different mean and variance, that is larger than the universal probability over the range of the data. By symmetry arguments, we obtain the new mean and variance that minimize the resulting redundancy of the universal predictor. The resulting predictor $\tilde{x}_u[n]$ can be viewed as the least-squares batch solution over the past, where we assume that $x[n] = 0$ and update $r_{xx}^n[0]$ and $R_{xx}^n[0]$ accordingly before predicting $x[n]$.

References

[1] A. Singer and M. Feder, "Twice universal linear prediction of individual sequences," in *1998 IEEE Int. Symp. on Info. Theory*, 1998.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

NON-LINEAR MMSE ESTIMATION AND SBS-MAP RECEIVERS

Stefano Galli

Telcordia Technologies Inc., 445 South Street, Morristown, NJ 07960, USA

***Abstract* – For the first time it is here shown that Symbol-by-Symbol Maximum A Posteriori (SbS-MAP) receivers are able to generate Non-Linear Minimum Mean Square Error (NL-MMSE) estimates of the transmitted symbols.**

I. INTRODUCTION

SbS-MAP receivers have the appealing feature of being able of generating a kind of *soft information* that can be considered intermediate between hard-decisions and A Posteriori Probabilities (APPs): the NL-MMSE estimates of the transmitted symbols. This result is not a surprise since MMSE estimation is defined through an "*a posteriori*" expectation functional. Nevertheless, the fact that one can generate NL-MMSE estimates through an SbS-MAP receiver has never been clearly pointed out in the current literature.

The availability of NL-MMSE estimates of the transmitted symbols is very useful in many applications, especially in those applications where it is necessary to mitigate the effects of wrong hard decisions. This has been recently pointed out in [1], although no method for computing the NL-MMSE was given.

II. A GENERAL MODEL OF THE OBSERVATIONS

The general model of a signal transmitted over a noisy and dispersive time-invariant channel is here considered. The random data sequence $\{s(k)\}$, constituted by M-ary generally complex i.i.d. equiprobable symbols, is transmitted over a linear channel whose time-invariant equivalent L-long discrete-time impulse response is denoted by $\{g(k)\}$. Thus, the ISI-impaired noisy sequence observed at the output of a baud-rate sampled whitened matched receiving filter can be modeled by the usual relationship:

$$y(i) = \sum_{k=0}^{L-1} g(k)s(i-k) + v(i) \equiv G^T x(i) + v(i), \qquad (1)$$

where G is the L-long impulse response vector of the ISI channel, $x(i) \equiv [s(i) \ldots s(i-L+1)]^T$ is the corresponding channel-state vector and $\{v(i)\}$ is a complex zero mean Gaussian noise sequence. The L-variate random sequence $\{x(i)\}$ is a first-order Markov chain known as "state sequence" of the ISI channel and may assume $N \equiv M^L$ distinct values $\{\xi_i\}$.

III. NL-MMSE ESTIMATION AND APPS

The MMSE estimate of the symbol $s(i)$ on the basis of the observations from step 1 to step i is given by the following relationship:

$$\hat{s}_{MMSE}(i) \equiv E\left\{s(i) \mid y_1^i\right\} \equiv \sum_{k=1}^{M} s_k \Pr\left(s(i) = s_k \mid y_1^i\right), \qquad (2)$$

It is possible to prove that (2) can be re-written in the following form:

$$\underline{\hat{s}}_{NL-MMSE}(i;L) = \Xi \pi(i/i) \qquad (3)$$

where $\underline{\hat{s}}_{NL-MMSE}(i;L)$ is the vector containing the NL-MMSE estimates of the last L transmitted symbols, $\pi(i|i)$ is the vector of the APPs of the state sequence of the ISI channel and Ξ is a LxN matrix whose columns are constituted by the vectors $\{\xi_i\}$ of (2). The relationship in (3) shows that the NL-MMSE estimates of the last L transmitted symbols can be expressed as a function of the APPs of the state of the ISI channel.

IV. CONCLUSIONS

In the present contribution, we presented a new method for generating NL-MMSE estimation with an SbS-MAP receiver. This method makes the use of SbS-MAP receivers very appealing because they can generate three kinds of information: a hard-statistics based information (the hard-decisions), a soft-statistics based information (the APPs) and an intermediate case represented by the NL-MMSE estimates of the transmitted symbols.

In general, the use of "estimates" in place of "decisions" is useful whenever the reliability of the hard-decisions is low. In fact, a wrong hard-decision is certainly more harmful (to channel estimation and tracking or to systems with feedback) than an imperfect estimate on the transmitted symbol [2, 3]. Other useful applications that may be foreseen for the proposed technique are in the field of multi-user detection.

REFERENCES

[1] F. Tarköy, "MMSE-Optimal Feedback and its Applications", *Proceedings of the IEEE Intern. Symp. on Infor. Theory*, ISIT'95, Whistler, Canada, 17-22 Sep. 1995.

[2] E. Baccarelli, R. Cusani, S. Galli, "A Novel Adaptive Equalizer with Enhanced Channel-Tracking Capability for TDMA-Based Mobile Radio Communications", *IEEE JSAC - Special Issue on Wireless Comm. (Part II)*, vol.16, no. 8, Dec. 1998.

[3] E. Baccarelli, A. Fasano, S. Galli, A. Zucchi, "A Novel Reduced-Complexity MAP Equalizer Using Soft-Statistics for Decision-Feedback ISI Cancellation", *IEEE Globecom Conference*, Rio de Janeiro, Brazil, 5-12 Dec. 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On the accuracy of estimating tail probabilities in queues

Assaf J. Zeevi

ABSTRACT NOT AVAILABLE AT THE TIME OF PRINT

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Estimation of the Covariance Matrix for Adaptive CFAR Detection in Compound-Gaussian Clutter

E. Conte *and* A. De Maio
Università di Napoli "Federico II"
Via Claudio, 21, 80125 Napoli,
Italy

Giuseppe Ricci
Università degli Studi di Lecce
Via Per Monteroni, 73100 Lecce,
Italy

Abstract — **We deal with the estimation of the structure of the covariance matrix of the noise and its application to adaptive radar detection of coherent pulse trains in compound-Gaussian clutter. Resorting to secondary data, free of signal components, we propose an estimator which, plugged into the NMF in place of the actual covariance matrix, leads to an adaptive detector CFAR with respect to the statistics of the noise.**

I. Introduction

The design of detection schemes optimized under non-Gaussian, clutter-dominated, disturbance is motivated by the experimental evidence that the Gaussian assumption is no longer met for clutter returns as viewed by high resolution radars. These returns are, instead, more accurately described in terms of compound-Gaussian processes [1, and references therein].

It is of primary concern to come up with canonical receivers, namely detectors whose structure as well as the distribution of the decision variable (under the noise-only hypothesis) is independent of the clutter statistics. In [1] it is shown that the Generalized Likelihood Ratio Test admits a sufficient statistic, referred to in the following as NMF, independent of the clutter amplitude probability density function if the number of integrated pulses, N say, becomes increasingly large. In order to come up with a completely-adaptive detector the key point is to substitute into the NMF the covariance matrix $\mathbf{M}$ of the noise with a suitable estimate of the structure of $\mathbf{M}$, $\mathbf{\Sigma}$ say. We propose a new estimate of $\mathbf{\Sigma}$, based upon secondary data, and demonstrate that the corresponding adaptive scheme is CFAR with respect to the clutter statistics. The performance assessment shows that its loss (with respect to the NMF) is always acceptable, and often negligible, in scenarios of practical interest for radar applications.

II. Problem Formulation and System Design

The problem of detecting a radar signal in additive, clutter-dominated, disturbance can be posed in terms of the following binary hypotheses test:

$$\begin{cases} H_0: & \mathbf{r}=\mathbf{c}, & \mathbf{r}_k=\mathbf{c}_k,\ k=1,\dots,K; \\ H_1: & \mathbf{r}=\alpha\mathbf{p}+\mathbf{c}, & \mathbf{r}_k=\mathbf{c}_k,\ k=1,\dots,K; \end{cases}$$

where $\mathbf{r}$, $\mathbf{p}$, $\mathbf{c}$, and the $\mathbf{c}_k$s, $k=1,\dots,K$, denote the $N-$dimensional complex vectors of the samples from the baseband equivalents of the received signal, the signature of the wanted target echo, the noise (all of them from the range cell under test), and of the secondary data, respectively, while α is an unknown, possibly complex, parameter accounting for the target radar cross section. Moreover, $\mathbf{c}$ and the $\mathbf{c}_k$s can be thought of as zero-mean Spherically Invariant Random Vectors or, otherwise stated, they can be written in the form [1]

$$\mathbf{c}=s\mathbf{g},\quad \mathbf{c}_k=s_k\mathbf{g}_k,\ k=1,\dots,K,$$

where $\mathbf{g}$ and the $\mathbf{g}_k$s are complex, zero-mean, Gaussian vectors, s and the s_ks are real, non-negative, random variates, and s and $\mathbf{g}$, similarly s_k and $\mathbf{g}_k$, $k=1,\dots,K$, are each other independent. We also assume that $\{\mathbf{g},\mathbf{g}_1,\cdots,\mathbf{g}_K\}$ is a set of independent, identically-distributed, circularly-symmetric vectors while $\{s,s_1,\cdots,s_K\}$ is a set of samples drawn from a non-negative, possibly correlated, wide-sense stationary random process with finite mean square value that, without loss of generality, we suppose in the sequel to be unitary.

We cluster the K secondary data into groups of cells sharing the same value of the texture: each group consists of K_S cells, i.e.,

$$s_k=S_{\lceil\frac{k}{K_S}\rceil},\qquad k=1,\dots,K,$$

where $K=K_S\times K_G$, with K_G denoting, in turn, the number of groups, and $\lceil x\rceil$ is the minimum integer greater than or equal to x. Finally, we assume that the power spectral density of the baseband equivalent of the clutter is symmetric about $f=0$: it implies that $\mathbf{M}=E[\mathbf{r}_k\mathbf{r}_k^H]=2\mathbf{M}^{(11)}=2E[\mathbf{r}_k^{(1)}\mathbf{r}_k^{(1)\,T}]$ with H denoting transpose conjugate, T transpose, and $\mathbf{r}_k^{(1)}$ the real part of the vector $\mathbf{r}_k$, $k=1,\dots,K$.

Notation. Let $\mathcal{N}=\{1,\dots,N\}$, $\mathcal{P}\subset\mathcal{N}$ with cardinality P and the complement of $\mathcal{P}$ with respect to $\mathcal{N}$ be denoted as $\overline{\mathcal{P}}$. For any N-dimensional vector $\mathbf{x}$, $\mathbf{x}_{\mathcal{P}}$ is obtained from $\mathbf{x}$ by striking out the ith component $\forall i\in\overline{\mathcal{P}}$. For any $N\times N$ matrix $\mathbf{A}$, $\mathbf{A}_{\mathcal{P}\mathcal{P}}$ is obtained from $\mathbf{A}$ by striking out the ith row and the ith column $\forall i\in\overline{\mathcal{P}}$.

We propose the following estimate of the structure $\mathbf{\Sigma}^{(11)}$ of $\mathbf{M}^{(11)}$:

$$\widehat{\mathbf{\Sigma}}^{(11)}=\frac{1}{K_G}\sum_{k_G=1}^{K_G}\frac{\sum_{k=(k_G-1)K_S+1}^{k_G\,K_S}\mathbf{r}_k^{(1)}\mathbf{r}_k^{(1)\,T}}{\left|\left(\sum_{k=(k_G-1)K_S+1}^{k_G\,K_S}\mathbf{r}_k^{(2)}\mathbf{r}_k^{(2)\,T}\right)_{\mathcal{P}\mathcal{P}}\right|^{\frac{1}{P}}},\quad(1)$$

where $|\cdot|$ denotes the determinant of a square matrix and $\mathbf{r}_k^{(2)}$ is the imaginary part of the vector $\mathbf{r}_k$, $k=1,\dots,K$.

It can be shown that $\widehat{\mathbf{\Sigma}}^{(11)}$ is well-defined when $P\le K_S$. Assume also $K\ge N$. Then, it can be shown that the NMF with $\widehat{\mathbf{\Sigma}}^{(11)}$, given by (1), in place of $\mathbf{M}$ is CFAR with respect to $\mathbf{M}$. Obviously, such detector is also CFAR with respect to the statistics of the texture. Finally, not only it tends to the NMF as K diverges, but its loss is acceptable also for finite K, thus showing its effectiveness in real environments.

References

[1] E. Conte, M. Lops and G. Ricci, "Asymptotically Optimum Radar Detection in Compound-Gaussian Clutter," *IEEE Trans. on Aerospace and Electronic Systems*, Vol. 31, No. 2, pp. 611-616, April 1995.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Bounded-Distance Soft Decision Decoding of Binary Product Codes

Ofer Amrani and Yair Be'ery
Department of Elec. Eng.–Systems
Tel Aviv University, Tel Aviv
Ramat Aviv 69978, Israel

Abstract — **A two-step sub-optimal algorithm for decoding binary product codes is discussed. This algorithm realizes at least half the minimum Euclidean distance of the code. The fundamental geometric properties associated with the algorithm are investigated, and bounds on the number of nearest neighbors are derived. This investigation also results with an improved algorithm which achieves the minimum effective error coefficient, the number of minimum-weight codewords in the product code.**

I. Introduction

A product code $\mathcal{C}_p = \mathcal{C}_r \times \mathcal{C}_c$ contains all the matrices whose columns are codewords in the code $\mathcal{C}_c$ and the rows are codewords in $\mathcal{C}_r$. The parameters of the product code are given by $[n_p, k_p, d_p] = [n_r n_c,\ k_r k_c,\ d_r d_c]$, where n denotes the length, k, the dimension, and d, the minimum Hamming distance of the corresponding code.

Product (iterated) codes were introduced by Elias in 1954 [3], and studied by many researchers until the late 70's. Several hard decision decoding techniques were proposed at that time for decoding a product code up to its guaranteed error-correction capability. Reddy and Robinson [6] gave a general decoder for any product code, with good correction capabilities for simultaneous burst and random errors. Yu and Costello [8] proposed a generalized minimum distance decoder for Q-ary output channels. In 1993 product codes gained renewed attention with the soft decision decoder of Lodge *et al.* [5], and the birth of turbo (iterative) decoding. While Lodge *et al.* [5] used the *a posteriori* probability as the reliability-measure for each bit, others, e.g. [7], employed suboptimal reliability measures that are less computationally involved.

II. Decoding

The proposed decoding technique [2] is not an iterative one, nor does it require explicit reliability-measure calculations for each bit. Rather, it is a suboptimal soft decision decoding scheme, more in the line of the aforementioned work [6], [8], operating as follows. Each of the component codes is soft-decision decoded separately, rows (columns) and then columns (rows), while passing a simple, hard-limited, reliability measure from the rows (columns) to the columns (rows). The result of the columns (rows) decoders is taken as the output. Generally speaking, while turbo decoding reduces the probability of bit error, the proposed technique is aimed at reducing the probability of codeword error.

III. Analysis and conclusions

We prove [2] that if the decoders of the component codes realize half the minimum Euclidean distance of these codes, then the complete decoding scheme realizes half the minimum Euclidean distance of the product code. Such a scheme is known as bounded distance (BD) decoding. An analysis of the decision region associated with this decoding scheme is given, revealing the following phenomena: **i)** regardless of the specific choice of a BD decoder used for decoding the component codes, the complete decoding scheme is always better than strictly BD decoding; **ii)** The algorithm contains *pseudo nearest neighbors* [1]. Based on the above analysis, an upper bound on the number of conventional nearest neighbors, i.e. the effective error coefficient, is derived. Furthermore, it is shown that the minimum effective error coefficient is achievable, as in the case of optimal decoding, by using a slightly modified decoding scheme.

The proposed decoding algorithms may be attractive for practical implementation due to their low decoding complexities. Decoding involves an order of $n_r + n_c$ applications of a component code decoder. For comparison, a single iteration of a block turbo-decoding scheme requires an order of $O(n_r n_c)$ such applications. Also, due to their geometrical properties, the algorithms can be employed as stopping-criteria (within the framework of block turbo-decoding) for terminating the iterative process. Since these algorithms aim at reducing the probability of word error, they are good candidates for the decoding of coset product codes [4].

References

[1] O. Amrani, and Y. Be'ery, "Bounded-distance decoding: algorithms, decision regions, and pseudo nearest-neighbors," *IEEE Trans. Inform. Theory*, vol. IT-44, pp. 3072–3082, 1998.

[2] O. Amrani, and Y. Be'ery, "Soft decision decoding of binary product codes," submitted for publication *IEEE Trans. Inform. Theory*, Sept. 1999.

[3] P. Elias, "Error-free coding," *IRE Trans. Inform. Theory*, vol. PGIT-4, pp. 29–37, 1954.

[4] M. Goldberg, "Augmentation techniques for a class of product codes," *IEEE Trans. Inform. Theory*, vol. IT-19, pp. 666–672, 1973.

[5] J. Lodge, R. Young, P. Hoeher, and J. Hagenauer, "Separable MAP 'filters' for the decoding of product and concatenate codes," in *IEEE Int. Conf. Communications ICC'93*, pp. 1740–1745, 1993.

[6] S. M. Reddy and J. P. Robinson, "Random error and burst correction by iterated codes," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 182–185, 1972.

[7] P. Robertson, E. Villebrun, and P. Hoeher, "A comparison of optimal and sub-optimal MAP decoding algorithms operating in the Log domain," in *Proc. IEEE ICC'95*, Seattle, WA, pp. 1009–1013, 1995.

[8] C. C.H. Yu and D. J. Costello, Jr., "Generalized minimum distance decoding algorithms for Qary output Channels," *IEEE Trans. Inform. Theory*, vol. IT-26, pp. 238–243, 1980.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On Structure and Decoding of Product Codes

S. A. Miri[1]
Department of Mathematics
University of Toronto, Toronto
Ontario, Canada, M5S 3G3
samiri@math.utoronto.ca

A. K. Khandani
Dep. of Elect. & Comp. Eng.
University of Waterloo, Waterloo
Ontario, Canada, N2L 3G1
khandani@shannon.uwaterlo.ca

Abstract — **Product codes have been an effective coding method for communication channels where both random and burst error occur. In this paper, we present a new approach to the structure and Maximum Likelihood (ML) decoding of product codes using Tanner graphs. For product codes having a sub-code which is a product of simple parity codes and repetition codes, we show how to obtain a sub-code with an acyclic Tanner graph and the largest possible distance. We show that in all cases of interest, a n-dimensional product code has such a structure. Wagner rule decoding is used on this sub-code and its cosets to obtain an effective and efficient maximum-likelihood decoding of the given product code.**

I. Introduction

The product codes first proposed by Elias in the 1950's are multi-dimensional codes constructed by combining simpler component codes. Experience has shown that product codes generally have good random-error-correction and burst-error-correction capabilities. In [1], Tanner extended earlier works by Gallager on low-density parity-check codes to product codes using bipartite graphs, since known as Tanner graphs. It is well known that using this approach one can construct convergent decoding algorithms for codes with acyclic graphs. The question of which codes have acyclic Tanner graphs was answered categorically in [2]. In [3], it was shown that decomposition of a code into an acyclic sub-code and its cosets can provide an efficient method for the maximum-likelihood decoding of some of the best known linear block codes. In the present work, we concentrate on product codes for which the row and column codes are based on well known linear block codes such as Golay code and Reed-Muller codes. This assumption is justified by the fact that the minimum distance and dimension of a given product code is directly related to the distance and dimension of its component codes. For this reason, we are interested in product codes using good binary block codes as components. Extending the work in [3], we will provide a systematic way of obtaining an optimal sub-code with an acyclic, uniform Tanner graph with the largest possible distance such that the number of the corresponding cosets are minimized and decoding complexity is lowered.

II. Main

It is well known that the generator matrix for product of codes A and B is given by the Kronecker product of their generators, that is $G_A \otimes G_B$. It is also known that if two matrices G and G' differ by a permutation of row and columns, then their corresponding Tanner graphs are isomorphic. Allowing for row and column permutations, we will show that if C' and M' be sub-codes of codes C and M respectively, and the decomposition of corresponding generators be $G_C = G_{C'} + G_{C/C'}$ and $G_M = G_{M'} + G_{M/M'}$, then the product of C and M is equal to the union of the sub-code $C' \otimes M'$ and its cosets which can be easily calculated from appropriate products of C', M', C/C', and M/M'.

Consider an n-dimensional product of good codes. It was shown in [3] that each of these codes has an acyclic sub-code with a generator of the form $\mathcal{R}_m \otimes \mathcal{E}_n$ where $\mathcal{R}_m$, $\mathcal{E}_n$ are matrix generators of some repetition codes and simple-parity check codes of length m and n, respectively. Hence, an n-dimensional product code will have a sub-code of the form,

$$(\mathcal{R}_{j_1} \otimes \mathcal{E}_{i_1}) \otimes (\mathcal{R}_{j_2} \otimes \mathcal{E}_{i_2}) \otimes \cdots (\mathcal{R}_{j_n} \otimes \mathcal{E}_{i_n}).$$

Regrouping, and using the facts the Kronecker product is associative, and that the Kronecker product of repetition codes is simply another repetition code, this can be rewritten as

$$\mathcal{R}_L \otimes (((\mathcal{E}_{i_1} \otimes \mathcal{E}_{i_2}) \otimes \mathcal{E}_{i_3}) \cdots \mathcal{E}_{i_n}), \qquad \text{for some } \mathcal{R}_L.$$

We will show using the results of [2] that the product code given by the above equation always has cycles if it includes more than one parity check code. The aim is to show how to obtain an acyclic sub-code of the form $\mathcal{R} \otimes \mathcal{E}$ for these cases. We will first show how to find an optimal acyclic sub-code for the case of $\mathcal{E}_{i_1} \otimes \mathcal{E}_{i_2}$. We use this result to find an optimal acyclic sub-code for $\mathcal{E}_{i_1} \otimes \mathcal{E}_{i_2} \otimes \mathcal{E}_{i_3}$ in a recursive manner, since this product can be considered as $(\mathcal{E}_{i_1} \otimes \mathcal{E}_{i_2}) \otimes \mathcal{E}_{i_3}$ and it has a sub-code of the form $\mathcal{R} \otimes (\mathcal{E} \otimes \mathcal{E}_{i_3})$. Using this approach $n-1$ times, it follows that $(\mathcal{E}_{i_1} \otimes \mathcal{E}_{i_2} \otimes \cdots \mathcal{E}_{i_n})$, and consequently, the n-dimensional product code will have an acyclic sub-code of the form $\mathcal{R} \otimes \mathcal{E}$ of appropriate sizes. Finally, following earlier work in [3], the simple structure of $\mathcal{R} \otimes \mathcal{E}$ allows it to be easily decoded using the Wagner rule in conjunction with the trellis representation of the corresponding cosets.

References

[1] R. M. Tanner, "A Recursive Approach to Low Complexity Codes", *IEEE Trans. Inform. Theory*, Vol. IT-27, No. 5, pp. 533–547, September 1981.

[2] T. Etzion, A. trachtenberg, and A. Vardy, "Which Codes Have Cycle-Free Tanner Graphs?", *Proceedings of 1998 ISIT*, New York, NY, pp. 207.

[3] M. Esmaeili and A. K. Khandani, "Acyclic Tanner graphs and two-level decoding of linear block codes", *Proceedings of 1998 ISIT*, New York, NY, pp. 91.

[1]This work was supported in part by the Natural Sciences and Engineering Research Council of Canada and in part by Communications and Information Technology Ontario (CITO).

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Low Complexity Maximum-Likelihood Decoding of Product Codes

Omar Al-Askary[1]
Department of Electrical
Engineering
Linkpingsuniversitet
SE-581 83 Linkping
Sweden
e-mail: omar@isy.liu.se

Abstract — **Many block codes can be represented as an intersection of two or more easily decoded codes. We present a new decoding algorithm for decoding product codes that utilizes this property. It will be shown that this algorithm is maximum likelihood decoding. The complexity of the algorithm depends on the decoding complexity of the constituent codes and the quality of the channel.**

I. Summary

Let $\boldsymbol{x}$ and $\boldsymbol{y}$ be, respectively, the codeword representing the message and the output from the channel. Also, let $\hat{\boldsymbol{c}}$ be the codeword in $\mathcal{C}$ nearest to $\boldsymbol{y}$, i.e., the maximum likelihood estimation. Let $\mathcal{C}_1'$ and $\mathcal{C}_2'$ be, respectively, a (n_1, k_1, d_1) and a (n_2, k_2, d_2) codes over $\mathbb{F}_2$. Let the code $\mathcal{C}_1$ with parameters $(n_2 n_1, n_2 k_1, d_1)$ be defined as $\mathcal{C}_1 \triangleq \{\boldsymbol{u} | \boldsymbol{u} \in \mathbb{F}_2^{n_2 \times n_1}, \boldsymbol{u}_{i,\cdot} \in \mathcal{C}_1', i \in \{1, \ldots, n_2\}\}$, where $\boldsymbol{u}_{i,\cdot}$ is the i:th row in the $n_2 \times n_1$ matrix $\boldsymbol{u}$. In other words, $\mathcal{C}_1$ is the n_2 fold *direct sum*, see [1, page 76] over $\mathcal{C}_1'$. In a similar way, we can obtain the code $\mathcal{C}_2$ with parameters $(n_2 n_1, k_2 n_1, d_2)$ by the n_1 fold direct sum over the code $\mathcal{C}_2'$, column-wise. Let $\mathcal{C}$ be the product code obtained from $\mathcal{C}_1'$ and $\mathcal{C}_2'$, see [1, page 568]. Clearly the following is valid $\mathcal{C} = \mathcal{C}_1 \bigcap \mathcal{C}_2$. For each word $\boldsymbol{u}$ in $\mathbb{F}_2^{n_2 \times n_1}$, there might be more than one word at the same Hamming distance from $\boldsymbol{u}$. Therefore, we use a metric function $D(\cdot, \cdot)$ that solves such ties. In the case of soft decoding with high precision, the squared Euclidean distance can be used since the probability of ties would approach zero. Let $\mathcal{S}$ be a list of all the codewords in $\mathcal{C}_1$ with Hamming distances from $\boldsymbol{y}$ less than or equal to the covering radius of $\mathcal{C}$ listed in an ascending order using the distance $D(\cdot, \cdot)$ mentioned above. It is easy to see that $\hat{\boldsymbol{c}}$ will be a member of this list since $\hat{\boldsymbol{c}}$ is an element in $\mathcal{C}_1$ too. The list $\mathcal{T}$ can also be generated in a similar manner by list decoding on $\mathcal{C}_2$. The decoding commences by checking the words in $\mathcal{S}$ one by one beginning from the first word and downward to see if it is also a codeword in $\mathcal{C}_2$. The algorithm stops when $\hat{\boldsymbol{c}}$ is reached which is the first word that passes the check. An alternative method would be to jump between the two lists $\mathcal{S}$ and $\mathcal{T}$ checking the elements of these lists at increasing distance until $\hat{\boldsymbol{c}}$ is reached in either one of the two lists. It is clear from the discussion above that the algorithm is maximum likelihood. The bottle-neck part of the algorithm is the list decoding of $\mathcal{C}_1$ and $\mathcal{C}_2$. In the case of product codes, however, this problem is reduced to list decoding the rows or the columns, assuming that there exists an algorithm for list decoding of $\mathcal{C}_1'$ and $\mathcal{C}_2'$. A list decoder for $\mathcal{C}_1$ can be made by the direct sum of members of the list decoding of $\mathcal{C}_1'$. In a similar manner we can obtain the list decoding for $\mathcal{C}_2$ by list decoding the columns. Instead of generating the elements of the set $\mathcal{S}$, the elements of the list decoder for each row are stored with their respective distances from their corresponding rows in $\boldsymbol{y}$ At iteration l the decoder searches through the rows beginning from the first row using l elements only from each row to generate the l nearest different combinations of elements and discarding the rest until reaching the last row in the received matrix and the l:th member of the list $\mathcal{S}$ is thus generated to be checked to see if it was the required solution.

An important note is that a limited number of list elements in each row can generate a very large number of the elements in the list $\mathcal{S}$. This is the main argument for lower complexity decoding for such codes. If a large product code is implemented on a memoryless channel with transition probability slightly greater than $d_1/2n_1$, there will be, in average, a list of one solution for decoding each row that contains the correct solution, resulting in a very small list $\mathcal{S}$ that has to be checked. A GMD decoder, see [2], can not decode such error patterns correctly. When the transition probability exceeds d_1/n, however, the size of the list increases exponentially which makes the algorithm impractical. On the other hand, the minimal trellis complexity, taken as the maximum number of states in the trellis, of the same product code is of the order of $O(2^{\min\{k_1, n_1 - k_1, k_2, n_2 - k_2\}})$, see [3, page 76]. In order to evaluate the performance of the algorithm, many simulations were performed for different product codes with different rates. In all simulations a suboptimal algorithm that utilizes a Chase 3 decoder, see [4, page 76], was used to generate a list of at most two solutions to be used in the decoding for the rows or columns. In each iteration the result of the previous iteration is list decoded instead of decoding the original message. This is done in order to keep the complexity of the decoder to minimum comparable to bounded minimum distance decoding. In all simulations the new algorithm had a better decoding gain than the GMD decoder by circa 2 dB. The performance can be further increased with increasing complexity.

References

[1] MacWilliams and Sloane. *The Theory of Error Correcting Codes*, North Holland, New York, 1977.

[2] G.D. Forney Jr, *Generalized minimum distance decoding.* IEEE trans IT, vol. 12, pp.125-131, April 1966.

[3] A. Vardy, *Trellis Structure of Codes.* Handbook of Coding Theory, North Holland, pp. 1989–2118, 1998.

[4] D. Chase, *A class of algorithms for decoding block codes with channel measurement information.* IEEE trans IT, vol. 18, no. 1, pp.170-182, January 1972.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Randomly Interleaved SPC Product Codes

David Rankin
Dept. of Electrical and Electronic Engineering
University of Canterbury
Private Bag 4800
Christchurch
New Zealand
dmr43@elec.canterbury.ac.nz

Aaron Gulliver
Dept. of Electrical and Computer Engineering
University of Victoria
P.O. Box 3055 STN CSC
Victoria, B.C.
Canada V8W 3P6
agullive@ece.uvic.ca

Abstract — **This paper considers single parity check (SPC) product codes which are randomly interleaved between the encoding of each dimension. Using random interleaving reduces the number of low weight codewords and so improves performance.**

I. Encoding and Decoding

The encoding process is very simple, after every parity check equation is encoded in a single dimension the data (and possibly the parity bits) are interleaved before the next dimension is encoded. The component codes are equal length single parity check (SPC) codes and hence the code rate is $R = K/N$ where $N = n^d$, $K = (n-1)^d$, d is the number of dimensions, and n is the length of the component codes. Unlike the decoding of a traditional SPC product code, a randomly interleaved (RI) SPC product code must be decoded in the reverse order of the encoding process. Natur ally this code is very similar to a serially concatenated code with the appropriate interleaver size. The component decoders are *maximum a priori* (MAP) decoders in the log likelihood domain, hence the bit error probability in the component code is minimised. Furthermore the extrinsic information and received channel values are interleaved/de-interleaved as they are passed between the decoders in each dimension.

II. Low Weight Codewords

In [1] RI SPC product codes have been analysed in terms of *partial weight distributions* corresponding to the input-output weight distributions after the encoding of a single dimension. Therefore the expected weight distribution of the overall code can be calculated over the ensemble of random interleavers by considering each dimension to be independently encoded with the input weight equal to the output weight of the previous dimension (assuming both the data and parity checks are interleaved). The *partial* input-output weight enumerator function (IOWEF) for the code has been calculated by considering invariant (under permutation) input patterns of a given input weight. The expected weight distribution for three dimensional RI SPC product codes (interleaving both the data and parity bits) with $n = 8$ is given by

$$B_0 = 1, \quad B_2 = 0.3, \quad B_4 = 21.9, \quad B_6 = 160.4, \quad B_8 = 2668.5$$

compared to $B_0 = 1$ and $B_8 = 21952$ for a traditional SPC product code. This shows a trade-off between the reduced number of low weight codewords and the reduction in minimum distance. However as the number of dimensions increases the reduction in the number of low weight codewords more than offsets the possible reduction in the minimum distance of the code.

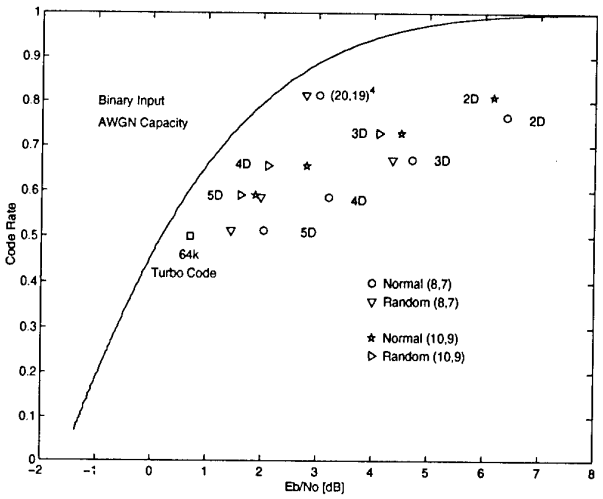


Figure 1: Performance of RI SPC Product Codes

III. Results

Simulation results for two- to five-dimensional RI SPC product codes with $n = 8$ and $n = 10$ are given in Fig. 1. The results are shown as code rate versus E_b/N_o for a probability of bit error equal to 10^{-5}. The performance of these very simple codes is quite exceptional, especially as the size of the component code increases and/or the number of dimensions increases. Note the four-dimensional $(20, 19)$ SPC code with rate .8145. Capacity of the binary input AWGN channel for this rate occurs at $E_b/N_O = 2.15$dB, therefore this code is only 0.63dB away from capacity at $P_b = 10^{-5}$. A disadvantage is the exponential increase in the blocklength as the number of dimensions (and the size of the component code) increases. It should be noted that the "error floor" predicted by the analysis typically becomes evident at $P_b \leq 10^{-5}$ for four- and five-dimensional codes. No attempt was made to optimize the interleavers, only randomly generated interleavers were used. Better interleaver design should improve the error floor.

IV. Summary

Randomly interleaved SPC product codes are extremely simple to encode and decode and yet perform surprisingly well due to the decrease in the number of low weight codewords.

References

[1] D.M. Rankin and T.A. Gulliver, "Single Parity Check Product Codes," *submitted to IEEE Trans. Commun.*

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Soft Decision Majority Decoding

Ilya Dumer[1]
College of Engineering
University of California at Riverside
Riverside, CA 92521, USA

Rafail Krichevskiy[1]
College of Engineering
University of California at Riverside
Riverside, CA 92521, USA

Abstract — **We present a new soft decision majority decoding algorithm for Reed-Muller codes $RM(r,m)$. First, the reliabilities of all received symbols are recalculated into the reliabilities of the parity checks that represent each information bit. In turn, information bits are obtained by the *weighted majority* that gives more weight to the more reliable parity checks. It is proven that for long low-rate codes $RM(r,m)$, our soft decision algorithm outperforms its conventional hard decision counterpart by $10\log_{10}(\pi/2) \approx 2$ dB at any given output bit error rate $\varepsilon < 1/2$.**

I. Introduction

Consider general Reed-Muller codes RM(r,m) [3] of length $n = 2^m$, dimension $k = \sum_{i=0}^{r}\binom{m}{i}$, and code distance $d = 2^{m-r}$. The *majority* algorithm [1] provides bounded distance decoding with complexity order of nk or less. Also, this decoding corrects many error patterns beyond the weight $d/2$ [2]. We consider majority decoding (see also [4]) for RM codes used over the channels with white Gaussian noise $\mathcal{N}(0,\sigma^2)$. The two symbols 0 and 1 are transmitted as $+1$ and -1. These two take arbitrary real values u at the receiver end with probability densities $g(u-1)$ and $g(u+1)$, where

$$g(u) = e^{-u^2/2\sigma^2}/\sqrt{2\pi}\sigma.$$

We wish to process further the likelihoods $p(0|u)$ and $p(1|u)$ while keeping the complexity $O(nk)$ of majority schemes. More specifically, the following questions arise:

- Can these likelihoods improve the performance of majority decoding ?
- How much can we reduce the possible S/N ratios?
- How many "hard decision" errors can we correct?

II. Decoding algorithm

The idea of our algorithm is as follows. Each information symbol of order r can be found from 2^{m-r} independent parity checks defined over disjoint subsets of 2^r code symbols. The simple majority of these checks is taken in hard-decision decoding. By contrast, in soft-decision decoding we use *weighted majority*. First, we recalculate the initial reliabilities of 2^r transmitted symbols into the reliability of the corresponding parity check. Second, the majority voting scheme accumulates all 2^{m-r} parity checks and gives more weight to the more reliable ones.

To estimate performance of a given code $RM(r,m)$, we fix an output bit error rate $\varepsilon < 1/2$. Then we introduce the *ε-sustainable* noise powers $\sigma_h^2(\varepsilon)$ and $\sigma_s^2(\varepsilon)$. These are the maximum noise powers that support BER ε in hard- and soft decision decoding, respectively. Similarly, we use the corresponding ε-sustainable transition error probabilities p_h and p_s. Our main theoretical result is that soft-decision decoding gains $10\log_{10}(\pi/2) \approx 2.0$ dB over conventional majority scheme for all long low-rate RM codes at any output error rate ε. We also keep the former complexity order of $O(nk)$. The results are summarized below.

Theorem 1 *For any output bit error probability ε, soft decision decoding of long codes $RM(r,m)$ of fixed order r increases $\pi/2$ times ε-sustainable noise power over hard decision decoding:*

$$\sigma_s^2/\sigma_h^2 \to \pi/2,\ m \to \infty.$$

For any output bit error probability ε, soft decision decoding of long codes $RM(r,m)$ of fixed code rate $R \in (0,1)$ increases $4/\pi$ times ε-sustainable transition error probability over hard decision decoding:

$$p_s/p_h \to 4/\pi,\ m \to \infty.$$

We also find the Euclidean weights of the error patterns correctable by our algorithm. The statement below shows that this algorithm exceeds about $2^{r/2}$ times the capacity $\sqrt{d}$ of bounded distance decoding.

Theorem 2 *For $m \to \infty$, soft decision majority decoding of codes $RM(r,m)$ corrects virtually all error patterns of Euclidean weight:*

$$\rho \le \sqrt{n}\,(d/2m)^{1/2^{r+1}}, \quad \textit{if } r = const,$$

$$\rho \le \sqrt{n/(m\ln 2)}, \qquad \textit{if } 0 < R < 1.$$

From the practical standpoint, we obtain *tight* numerical bounds on the output bit error rate for any code $RM(r,m)$. When these bounds were compared with simulation results, both turned out to be almost identical.

References

[1] I.S. Reed, "A class of multiple error correcting codes and the decoding scheme," *IEEE Trans. Info. Theory*, vol. IT-4, pp. 38-49, 1954.

[2] R.E. Krichevskiy, "On the number of Reed-Muller code correctable errors," *Dokl. Soviet Acad. Sciences*, vol. 191, pp. 541-547, 1970.

[3] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*. North Holland, Amsterdam, 1977.

[4] I. Dumer and R. Krichevskiy, "Soft Decision Majority Decoding of Reed-Muller Codes," *IEEE Trans. Info. Theory*, vol. 46, pp. 258-264, 2000.

[1] This work was supported by the NSF grant NCR-9703844.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

A* ML Decoding of Linear Block Codes on Band-Limited Channels

Svante Eriksson (svante.eriksson@space.se)
Saab Ericsson Space AB
SE-405 15 Göteborg, Sweden

Tor M. Aulin (tor@ce.chalmers.se)
Dept. of Computer Engineering, Telecommunication Theory
Chalmers Univ. of Technology, SE-412 96, Göteborg, Sweden

Abstract — **The A* algorithm is applied to soft-decision maximum-likelihood decoding (MLD) of linear block codes when intersymbol interference (ISI) is present. Results for a small set of channels and codes show that the chosen column permutation of the generator matrix for the code affects not only the decoding complexity, but also the error performance.**

I. Introduction

Consider a system where codewords from a block code are transmitted using linear modulation on a band-limited channel, such that ISI is present at the channel output, where white Gaussian noise is added. The decoding approach taken here is to treat the encoder and the discrete-time whitened matched filter (WMF) receiver [1] as a joint entity. Using finite-state machine (FSM) descriptions of the encoder and the channel, the state vector for a joint FSM describing the whole system is achieved by concatenating the state vectors of the component state machines [2]. MLD can then be stated as determining the most likely sequence of state transitions of the joint FSM, i.e., the optimal path through the joint trellis, given the received signal. A* is a heuristic graph algorithm [3] that can be used to perform that search.

II. Maximum-Likelihood Decoding

Let $\boldsymbol{a}_j \equiv (a_{jN}, \ldots, a_{(j+1)N-1})$ be a codeword $\boldsymbol{c}_j$ from a binary linear block code $\mathcal{C}$ and let $\boldsymbol{\alpha}_j \equiv (\alpha_{jN}, \ldots, \alpha_{(j+1)N-1})$ be the sequence of channel symbols corresponding to $\boldsymbol{a}_j$. The outputs of the WMF are then $s_n = \sum_{k=0}^{L-1} f_k \alpha_{n-k}$ [1]. For simplicity, assume that $\boldsymbol{a}_j = \boldsymbol{0}$ for $j \neq 0$.

Then $\boldsymbol{s}_0 \equiv (s_0, \ldots, s_{N+L-2})$ are the only filtered symbols affected by $\boldsymbol{a}_0$, and therefore $\boldsymbol{a}_0$, $\boldsymbol{\alpha}_0$ and $\boldsymbol{s}_0$ are mapped one-to-one. At the WMF output, zero-mean white Gaussian noise samples η_n with variance $\sigma_\eta^2 = N_0$ are added, yielding the received sequence $\boldsymbol{z}_0 \equiv (z_0, \ldots, z_{N+L-2}) = \boldsymbol{s}_0 + \boldsymbol{\eta}_0$.

The task of the joint ML decoder is to determine the codeword $\boldsymbol{a}_0'$ that maximizes the likelihood function $\mathbf{p}_{\boldsymbol{z}_0}(\boldsymbol{z}_0|\boldsymbol{a}_0')$. Due to WMF properties, this is equivalent to determining the codeword that minimizes the cost, the squared Euclidean distance between $\boldsymbol{z}_0$ and $\boldsymbol{s}_0'$, i.e. $\hat{\boldsymbol{a}}_0 \equiv \arg\min_{\boldsymbol{a}_0' \in \mathcal{C}} \|\boldsymbol{z}_0 - \boldsymbol{s}_0'\|^2$.

A coarse approximation of the word error probability for high SNRs is given by $\mathbf{P}_w \approx Q(\sqrt{d^2_{min} \frac{K}{N} \frac{\mathcal{E}_{ib}}{N_0}})$ [1], where $d^2_{\min}$ is the minimum distance between any two codewords at the filter output, ignoring the multiplicity of the error event.

The state of the ISI FSM is defined by the $(L-1)$ most recently transmitted symbols and the state of the encoder FSM at time i is defined by the $\rho_i \leq \rho_{\max} \leq \min(K, N-K)$ active information bits. Concatenating these state definitions, a $(\rho_{\max} + L - 1)$-bit joint state vector, $\boldsymbol{\sigma}_i$, is yielded.

A* needs an evaluation function, $f(\boldsymbol{\sigma}_i) \equiv g(\boldsymbol{\sigma}_i) + h(\boldsymbol{\sigma}_i)$ to be defined for each trellis state, $\boldsymbol{\sigma}_i$, associating with it an *underestimate* of the total cost of any path passing through it. $g(\boldsymbol{\sigma}_i)$ is defined as the actual cost of the path taken from the initial node, $\boldsymbol{\sigma}_0$, to reach $\boldsymbol{\sigma}_i$. The definition of $h(\boldsymbol{\sigma}_i)$ proposed here is the minimum cost of any length-$(N+L-1-i)$ path from $\boldsymbol{\sigma}_i$, *not necessarily consistent with the code.* This cost is easily determined with the Viterbi algorithm (VA).

III. Results and Conclusions

For simulations and $d^2_{\min}$-calculations, real-valued $(L=2)$-channels characterized by f_1/f_0 have been considered. The codes studied are different-complexity permutations of the extended Golay $(24, 12)$ code and various BCH and RM codes.

For the selected codes and channels, the lower complexity permutations have worse error performance than their higher-complexity counterparts in terms of $d^2_{\min}$ (see Fig. 1) though the decoding complexity in terms of expanded nodes and examined edges is lower. Simulation results support this for all considered different permutations of the same code. For the $\mathbf{P}_w$-simulation of the Golay codes on the $f_0 = f_1$ channel, the gain of the higher complexity permutation over the lower complexity permutation is more than 3 dB $\mathcal{E}_{ib}/N_0$ at $\mathbf{P}_w \approx 7 \times 10^{-4}$.

For all considered codes, the number of expanded nodes and considered edges approach constant values for very high and low SNRs. For high SNRs, the distribution of the number of expanded nodes becomes narrow, and an average of $(N+L-1)$ nodes are expanded. Detecting and ignoring repeatedly visited nodes yields only a negligible improvement on the decoding complexity.

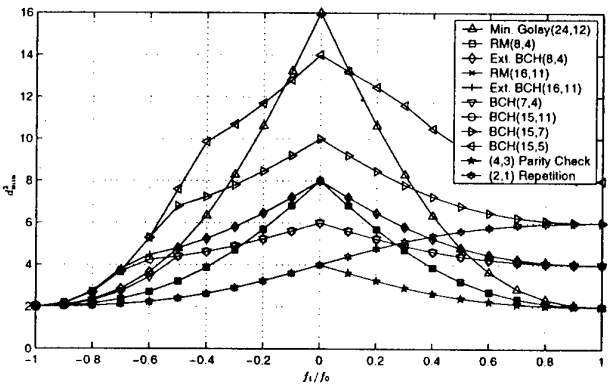


Fig. 1: $d^2_{\min}$ as function of f_1/f_0

References

[1] G. D. Forney, Jr., "Maximum-Likelihood Sequence Estimation of Digital Sequences in the Presence of Intersymbol Interference," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 363–378, May 1972.

[2] T. M. Aulin, "Breadth-First Maximum Likelihood Sequence Detection: Basics," *IEEE Trans. Commun.*, vol. COM-47, pp. 208–216, Feb. 1999.

[3] N. J. Nilsson, *Principles of Artificial Intelligence.* Symbolic Computation, Berlin: Springer Verlag, 1982.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Fast Soft-Decision Decoding of Linear Codes, Stochastic Resonance in Algorithms

Antoine Valembois[1]
Projet CODES
INRIA Rocquencourt
78153 Le Chesnay Cedex France
antoine.valembois@inria.fr

Abstract — **We propose a new soft decoding algorithm for long general binary linear codes, based on information set decoding. Its specificity is that it is derived from the fastest hard decoding algorithm for long codes, which explores successively information sets close to each other, and that the search is guided by the reliability values thanks to a technique inspired by stochastic resonance. It can reach for instance a bit error rate of 10^{-6} at 3 dB in a reasonable time.**

I. Introduction

General (random) binary linear codes provide correcting capacity depending on their length and rate. For a given channel and at a given rate (lower than the channel capacity), the decoding error probability decreases exponentially with the length of the code (cf. [1]). Unfortunately, the computation cost of complete decoding is also exponential in this length.

The decoding algorithms generally explore an exponential set (the set of codewords, of error patterns, of information sets of the code...), and, after an adjustable computational effort, return the best element they have found. When the computational effort tends to infinity, the decoding error probability tends to that of complete decoding. Beyond a given computational effort, they hence perform quasi-complete decoding.

In this context, soft decoding has two different advantages over hard decoding. The first one is provided by the greater accuracy of the distance between a received word and the possible codewords, which allows, for the same signal to noise ratio (SNR), to put up better performances in terms of residual error rate, or to decrease (by approximately 2 dB) the required SNR to achieve a given residual error rate.

The second one comes from the fact that the reliability informations may offer a guideline to the algorithms in their exploration of the set, and may consequently reduce importantly the search space required to achieve a residual error rate close to that of complete decoding.

This work is an adaptation to the soft decoding of what is supposed to be the fastest general quasi-complete hard decoding algorithm for long codes, in a way that intends to turn these two advantages to the best possible account.

II. How to guide Information Set Decoding

The above-mentioned hard decoding algorithm is a particular information set decoding algorithm designed by Canteaut, Chabanne and Chabaud in 94, in order to improve the attacks on cryptosystems based on error-correcting codes, like McEliece's cryptosystem (cf. [2]). In short, it searches for an information set with as few errors as possible, and when changing information set, an only information position is rejected out of it whereas a new one is admitted in it.

Since we want the information set to contain few errors, we can start the search (like in [3], [4]) with the most reliable basis, the set of the k most reliable independant positions.

To continue the search, a choice has to be made: which information position to reject and which new one to admit in the information set ? Determinist methods based on the reliability lead to a periodic exploration of the same information sets. Preventing this implies an additive cost in space and time that can be dramatically important for long codes.

Eventually, the chosen method is based on a controlled random: All the positions in (out of) the information set can be chosen to be rejected (admitted) with a probability that is a decreasing (increasing) function of their reliability.

By looking for the optimal probability distributions, we observe stochastic resonance phenomena: For a given set of reliability measures, certain probability distributions will make our algorithm much faster.

The concept of stochastic resonance has been introduced in 1981 (cf. [5]) in the study of the periodic variations of glacier. It is mentioned when a processing can turn a noise to advantage, and when the moments of this noise are adjusted to optimize this advantage. Such phenomenas have been observed in various areas (cf [6]), a main application being the improvement of lasers.

III. Results

The implemented version of the algorithm has been evaluated for a gaussian channel with antipodal modulation. For instance it performed quasi-complete decoding of a code of length 200 and dimension 100, reaching a bit error rate of 10^{-6} at 3 dB in a reasonable time.

[1]This work was supported by a grant from the D.G.A..

References

[1] Robert G. Gallager, "A simple derivation of the coding theorem and some applications" *IEEE Trans. on Inform. Theory*, vol. 11(1), pp. 3-18, Jan. 1965.

[2] A. Canteaut and F. Chabaud, "Improvements of the attacks on cryptosystems based on error-correcting codes," *Technical Report LIENS-95-21, Ecole Normale Supérieure*, July 1995.

[3] M. P. C. Fossorier and S. Lin, "Soft-Decision Decoding of Linear Block Codes based on Ordered Statistics," *IEEE Trans. on Inform. Theory*, vol. 41, pp. 1379-1396, Sept. 1995.

[4] D. Gazelle and J. Snyders, "Reliability-Based Code-Search Algorithms for Maximum-Likelihood Decoding of Block Codes," *IEEE Trans. on Inform. Theory*, vol. 43, pp. 239-249, Jan. 1997.

[5] R. Benzi, A. Sutera and A. Vulpiani, "The mechanism of Stochastic Resonance," *J. Phys. A: Math.*, Gen.14L 453, 1981.

[6] B. McNamara and K. Wiesenfeld, "Theory of Stochastic Resonance," *Phys. Rev.* A39 4854, 1989.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Minimum Norm Solution Based Approach to Decoding of Real Number BCH Codes

Nikola Rozic, Dinko Begusic, Marija Vrdoljak
University of Split, R.Boškovića bb., 21000 Split, Croatia, email: rozic@fesb.hr

Abstract - *In this paper we consider the special case of the underdetermined LS problem when the difference between the number of unknowns and the number of equations equals one. We propose a new method to improve the minimum norm solution based on using the estimate of the norm of the exact solution. The method is applied to the problem of syndrome based error control image coding over real fields. A series of computer simulations show the significant gain in output signal to noise ratio at high bit error rate in the channel.*

I. A NORM ESTIMATE BASED APPROACH TO IMPROVING THE MINIMUM NORM SOLUTION

Consider the special case of the rank *N-1* underdetermined LS system. It may be written in the following form

$$\mathbf{Y}_{N-1} = \mathbf{A}_{(N-1)\times N}\ \mathbf{X}_N \qquad (1)$$

where $\mathbf{Y}_{N-1}$ is an *N-1* dimensional vector of observations and $\mathbf{A}_{(N-1)xN}$ is an *(N-1)xN* coefficient matrix.

We can write the expression for the squared norm of the vector of *N* unknowns $\mathbf{X}_N$ in terms of the given quantities of the rank *N-1* system and the *N-th* unknown $\mathbf{x}_N$ as

$$\|\mathbf{X}_N\|^2 = a\mathbf{x}_N^2 + b\mathbf{x}_N + c \qquad (2)$$

where the coefficients *a, b,* and *c* are defined as follows

$$a = \left[-\mathbf{A}^{-}_{(N-1)\times(N-1)}\ \mathbf{A}_{N,N-1}\right]\left[-\mathbf{A}^{-}_{(N-1)\times(N-1)}\ \mathbf{A}_{N,N-1}\right] \qquad (3)$$

$$b = \left[\mathbf{A}^{-1}_{(N-1)\times(N-1)}\ \mathbf{Y}_{N-1}\right]\left[-\mathbf{A}^{-1}_{(N-1)\times(N-1)}\ \mathbf{A}_{N,N-1}\right] + \left[-\mathbf{A}^{-1}_{(N-1)\times(N-1)}\ \mathbf{A}_{N,N-1}\right]\left[\mathbf{A}^{-1}_{(N-1)\times(N-1)}\ \mathbf{Y}_{N-1}\right]; \qquad (4)$$

$$c = \left[\mathbf{A}^{-}_{(N-1)\times(N-1)}\ \mathbf{Y}_{N-1}\right]\mathbf{A}^{-}_{(N-1)\times(N-1)}\ \mathbf{Y}_{N-1} \qquad (5)$$

By solving equation (11) we can write the expression for the unknown $\mathbf{x}_N$ in terms of the norm of the vector of *N* unknowns $\mathbf{X}_N$ and the coefficients *a, b,* and *c* as

$$\mathbf{x}_N = \frac{-b \pm \sqrt{b^2 - 4a(c - \|\mathbf{X}_N\|^2)}}{2a} \qquad (6)$$

Equation (15) gives the relation between one unknown and the norm of the exact solution to the full rank LS system.

Norm estimation can be considered for certain conditions such as appearing in applications in image channel coding over the real fields [2]. In fact we estimate a norm ratio (NR) of exact norm N_1 and minimum norm N_0 i.e. N_1/N_0.

II. REAL NUMBER BCH (4,2) PRODUCT CODE

In [3], real-number codes based on the discrete Fourier transform (DFT) are defined. It is important for decoding that the last c elements of the error vector **e** present the syndrome vector **s** [4]. Based on **s**, error signals can be estimated as a solution to the standard least squares problem:

$$\mathbf{e}=\mathbf{A}^{-1}\mathbf{s} \qquad (7)$$

where **A** is a c x c data matrix.

As it is described in [2] for a (4,2) BCH code, almost all single errors under the background noise can be detected and corrected based on a syndrome $\mathbf{s}=(s_1,s_2)$. To deal with multiple errors, an approach based on norm estimation discussed in a preceding section has been considered. For the considered case of real number (4,2) BCH code it can be found for noise-free case the norm ratio (NR) is

$$\alpha_0 = NR_0 = \frac{N_1}{N_0} = \sqrt{1.333} = 1.1547$$

so that this value can be also used as optimal one in noisy cases, too. For noisy cases the ratio α is random variable. In addition, a correlation between a minimum norm N_0 and norm ratio NR_0 has been considered and negative correlation was identified so that an adaptive algorithm for α can be performed.

III. EXPERIMENTAL RESULTS

An autoregressive first order process AR(1) driven by a Gaussian noise has been quantized with $x \in \{0,1,...,255\}$ which fits data such as images and videos quite well. Pair of symbols are coded with (4,2) BCH code [2] and transmitted through an AWGN channel. Based on Eq. (7) all noise-free and single-error cases are decoded based on syndrome values s_1 and s_2. For all multiple error cases, a MNS solution is calculated and an SNR_0 defined by $SNR_0 = 10\log[\mathbf{x}/(\mathbf{x}-\mathbf{x}_0)],[dB]$ where $\mathbf{x}=(x_1,x_2)$ is a data vector and $\mathbf{x}_0=(x_{10},x_{20})$ is an MNS estimate.

Simulations performed in Matlab show a significant SNR gain for highly correlated sources. For a constant norm ratio $\alpha = 1.1547$ SNR gain was about 2.3dB. For an adaptive α an additional gain of about 1.5dB is obtained. It yields in total a gain of about 3.8dB.

IV. CONCLUSIONS

In this paper we propose a new method to improve the minimum norm solution to the special case of the underdetermined LS problem when the difference between the number of unknowns and the number of equations equals one. The approach is based on using the estimate of the norm of the exact solution to the full rank system. The method is applied to the problem of error control over real fields as an additional algorithm to the syndrome based error correction in multiple-error cases. Experimental results have shown significant gain in SNR.

REFERENCES

[1] G.H.Golub, C.F.VanLoan: *Matrix Computations*, Second Edition, The Johns Hopkins University Press, Baltimore, MD, USA, 1989.

[2] N.Rozic, D.Begusic, N.Pavesic,H.Dujmic: *Real (4,2) BCH Code for Image Communications,* in Proceedings of GLOBECOM'99, Rio de Janeiro, Brasil, Dec. 5-9, 1999.

[3] T.G. Marshall Jr.: "*Coding of Real-Number Sequences for Error Correction: A Digital Signal Processing Problem*", IEEE Journal on Select. Area in Commun., Vol. SAC-2, N0.2, March 1984, pp 381-392.

[4] R.E. Blahut: *Transform Techniques for Error Control Codes*, IBM J.Res.Develop., vol.32, May 1979, pp 299-315.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

The Construction and Free Distance Estimation of Generalized Woven Codes with Outer Warp

Matin Bossert, Walter Schnug
University of Ulm, Com. Eng.
Dept, Albert-Einstein-Allee 43,
89081 Ulm, Germany;
boss@it.e-technik.uni-ulm.de

Hans Dieterich
Siemens AG,
Lise-Meitner-Str. 5,
89081 Ulm, Germany;
Hans.Dieterich@icn.siemens.de

Sergo Shavgulidze
Dept. of Digital Com. Theory,
Georgian Technical University
380075 Tbilisi, Georgia;
sergo_130@hotmail.com

Abstract — **A new class of convolutional codes, namely generalized woven codes with outer warp is presented. The codes are based on nested classes of inner single convolutional code and many outer convolutional codes with different redundancies. We give a lower bound on free distance for these codes.**

I. Introduction

In 1997, Höst, Johannesson and Zyablov presented woven convolutional codes [1]. Here we extend these ideas and construct generalized woven convolutional codes with outer warp (GWOW). We use nested system of binary convolutional codes at the inner stage and binary convolutional codes with different rates as outer codes. The nested system of inner codes are constructed on the basis of partitioning of convolutional codes into subcodes. The partitioning principles for convolutional codes has been described in [2, 3, 4] and can be found in the full paper. Furthermore, we extend the active distance ideas proposed in [5] to the case of nested subcodes. Based on these results we determine the overall code rate and give the lower bound on the free distance for GWOW codes.

II. Generalized Woven Codes

Figure 1 shows the encoder of the proposed generalized woven codes with outer warp. As the inner code

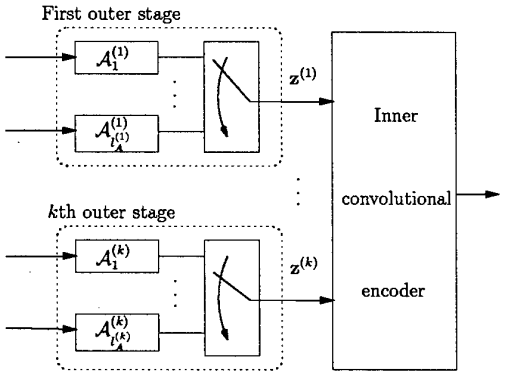


Figure 1: Encoding scheme of GWOW codes

a kth order partitioned convolutional code of rate R_B is used. We have kth outer stages, whereby each outer stage comprises of $l_A^{(j)}$, $j = 1, 2, ..., k$ interleaved parallel convolutional codes $A_i^{(j)}$, $i = 1, 2, ...l_A^{(j)}$. In each stage all outer codes have the same rate $R_A^{(j)}$ and they determine the sequences $z^{(j)}$ which are encoded by the inner partitioned convolutional code. The overall code rate $R_{GWOW} = R_B(\sum_{j=1}^{k} R_A^{(j)}/k)$.

The partitioning method introduces scrambler matrices to construct suitable equivalent encoding matrices for kth order partitioning. Therewith we obtain increasing free distances $d_B^{(j)}$, $j = 1, 2, ..., k$ in the subcodes. Furthermore, we also investigate the active row distances of subcodes. In general, active row distances of the jth subcode $B^{(j)}$ can be lower bounded by $a^{r(j)}(l) \geq \max(\alpha^{(j)} l + \beta^{r(j)}, d_B^{(j)})$ where $\alpha^{(j)} \geq 0$, $\alpha^{(j)}, \beta^{r(j)} \in \mathbb{R}$, $l = 0, 1, 2, ...$ Since $a^{r(j)}(l)$ is in general no increasing function we define $\widehat{a}^{r(j)}(l) \geq \min_{l' \geq l}(a^{r(j)}(l))$ which is an increasing function.

Theorem: Let $l_A^{(j)} \geq l^{r(j)}$ where $l^{r(j)}$ is the smallest l for which $\widehat{a}^{r(j)}(l) \geq 2d_B^{(j)}$ holds. Then the free distance of GWOW code is lower bounded by

$$d(GWOW) \geq (d_A^{(1)} d_B^{(1)}, ..., d_A^{(j)} d_B^{(j)}, ..., d_A^{(k)} d_B^{(k)}).$$

In the full paper with the help of examples we show that GWOW codes compared to the ordinary woven convolutional codes achieve larger free distances and/or higher code rates.

References

[1] S. Höst, R. Johannesson, and V. Zyablov, "A first encounter with binary woven convolutional codes," in *Proc. of the 4th International Symposium on Communication Theory and Applications*, Lake Districts, UK, July 1997.

[2] M. Bossert, H. Dieterich, and S. Shavgulidze, "Generalized concatenation of convolutional codes," *Eur. Trans. Telecommun.*, vol. 7, no. 6, pp. 483–492, Nov./Dec. 1996.

[3] —, "Partitioning of convolutional codes using a convolutional scrambler," *Electron. Lett.*, vol. 32, no. 4, pp. 1758–1760, Sept. 1996.

[4] —, "Generalized concatenated convolutional codes with systematic encoding of partitioned subcodes," *Int. Jour. of Elec. and Comm.*, vol. 53, no. 5, pp. 273–279, 1999.

[5] S. Höst, R. Johannesson, K. Zigangirov, and V. Zyablov, "Active distances for convolutional codes," *IEEE Trans. Inform. Theory*, vol. IT-45, pp. 658–669, March 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Woven Codes with Outer Block Codes

J. Freudenberger, M. Bossert
Dep. of Information Technology
University of Ulm
Albert-Einstein-Allee 43
D-89081 Ulm, Germany
e-mail: jfreuden@e-technik.uni-ulm.de
boss@e-technik.uni-ulm.de

V. Zyablov
Inst. for Problems of Information Transmission of the Russian Academy of Science
B. Karetnyi per., 19, GSP-4
Moscow, 101447 Russia e-mail:
zyablov@iitp.ru

S. Shavgulidze
Dep. of Digital Communication Theory
Georgian Technical University
Kostava str. 77
Tbilisi, 380075 Georgia
e-mail: sergo_130@hotmail.com

Abstract — **Woven codes with outer binary block codes and additional permutation are presented. This enables the construction of a new class of woven block codes, where the minimum distance is about twice the product of the minimum distances of the component codes.**

I. Introduction

Woven convolutional codes were introduced by Höst *et al.* in [1]. In this paper we present a new encoder construction of woven codes namely, woven codes with outer binary block codes and inner recursive convolutional encoders. We show that by employing designed permutations we can improve the distance properties of woven block codes. Moreover, in the full paper first simulation results for woven block codes are presented, where we employ outer single-parity-check codes.

II. Woven encoder

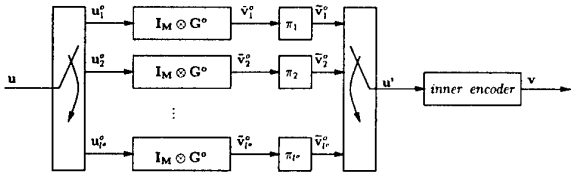


Figure 1: Woven encoder with permutation.

We use an encoder construction with l^o rows of outer encoders (see Figure 1), where we apply an unique permutation in each row. Each information sequence $\mathbf{u}_l^o$ is subdivided into M short blocks of length k^o. Each short block is encoded with the same generator matrix $\mathbf{G}^o$. We call a codeword encoded by $\mathbf{G}^o$ *basic codeword*. The sequence $\mathbf{v}_l^o$ consists of M basic codewords, each of length n^o, i.e. $N = Mn^o$ code bits. We obtain the output code sequence $\tilde{\mathbf{v}}_l^o$ of the lth row after permuting the code bits of $\mathbf{v}_l^o$. Using an $N \times N$ matrix $\mathbf{P}_l$ to describe the row-wise permutations we may express the encoding of the lth output sequence as $\tilde{\mathbf{v}}_l^o = \mathbf{u}_l^o (\mathbf{I}_M \otimes \mathbf{G}^o) \cdot \mathbf{P}_l$, where $\mathbf{I}_M$ is an $M \times M$ identity matrix and $\otimes$ denotes the Kronecker product. A permutation matrix $\mathbf{P}_l$ is a non-singular matrix with a single one in each row and each column, all other elements are zero. In the following we describe a permutation as a function $\pi(\cdot)$, where $\pi_l(i)$ denotes the position of the single one in the ith column of the permutation matrix $\mathbf{P}_l$.

III. Permutation Design

Let d^o and d_f^i denote the minimum distance and the free distance of the outer and inner codes, respectively. Let j_{min}^i denote the minimum j for which $j_{min}^i = \min_j\{j \mid \tilde{a}^{b,i}(j) \geq 2d_f^i\}$ holds, where $\tilde{a}^{b,i}(j)$ denotes the lower bound on the active burst distance of the inner encoder [2]. If we do not restrict the l_o permutations $\pi_l(\cdot)$ we obtain the following result.

Theorem 1. *The minimum distance of the woven code with $l^o \geq b^i j_{min}^i$ outer block codes satisfies the following inequality:*

$$d^w \geq d^o d_f^i. \tag{1}$$

In the following we consider designed permutations. Let $p = N+1$ be prime. We perform all multiplications in GF(p). For each lth row we use its own unique permutation $\pi_l(i) = i \cdot u_l,\ i \in \{1, \ldots, N\}$, where $l \in \{1, \ldots, l^o\}$. Each u_l is a fixed element of $GF(p)$ which satisfies the following conditions:

$$u_l \geq 2, \tag{2}$$

$$u_l \leq \frac{N}{n^o - 1}, \tag{3}$$

$$u_l^{-1} \geq n^o, \tag{4}$$

$$|\delta_1 u_l - \delta_2 u_j| \geq 3,\ \forall\ \delta_1, \delta_2 \in \{-n^o+1, \ldots, -1, 1, \ldots, n^o-1\} \text{ and for any pair } l \neq j;\ l, j \in \{1, \ldots, l^o\}. \tag{5}$$

Theorem 2. *The minimum distance of the woven code with $l^o \geq b^i j_{min}^i$ outer block codes (each encoded according to formulas (2) - (5)) satisfies:*

$$d^w \geq (2d^o - 1)d_f^i. \tag{6}$$

IV. Example

We construct a woven encoder with row-wise permutation, where we use $\mathbf{G}^i(D) = (1, \frac{1+D^2}{1+D+D^2})$ as inner generator matrix. We employ $l^o = 12$ rows of single parity check codes with $\mathbf{G}^o = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$. Each row consists of $M = 416$ basic codewords. For the permutations we use

$$u_l \in \{7, 10, 17, 23, 26, 29, 37, 40, 43, 49, 55, 61\}$$

which satisfy conditions (2) - (5). The resulting woven code has rate $R = 1/3$ and dimension $K = 9984$. With the minimum distances $d^o = 2$ and $d_f^i = 5$ we obtain $d^w \geq 15$.

References

[1] S. Höst, R. Johannesson, and V. Zyablov, "A first encounter with binary woven convolutional codes," in *Proc. International Symposium on Communication Theory and Applications, Lake District, UK*, July 1997.

[2] S. Höst, R. Johannesson, K. Zigangirov, and V. Zyablov, "Active distances for convolutional codes," *IEEE Trans. on Inform. Theory*, vol. IT-45, pp. 658–669, March 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Optimum Slope Convolutional Codes

R. Jordan, J. Freudenberger, V. Pavlouchkov, M. Bossert
Dep. of Information Technology
University of Ulm
Albert-Einstein-Allee 43
D-89081 Ulm, Germany
e-mail: {ralph.jordan, jfreuden, boss}
@e-technik.uni-ulm.de

V. Zyablov
Inst. for Problems of Information
Transmission of the Russian
Academy of Science
B. Karetnyi per., 19, GSP-4
Moscow, 101447 Russia
e-mail: zyablov@iitp.ru

Abstract — **A new family of binary convolutional codes is introduced: the maximum slope (MS) code family. MS codes are defined such, that there exist no other rate $R = b/c$ binary convolutional code with the same free distance d_f and overall constraint length ν, whose lower bounds on the active distance family exhibit a larger slope. Tables for the rate $R = 1/2$ maximum slope code family with memory $m = 1, 2, \ldots, 5$ are given. Furthermore, tables for new rate $R = (c-1)/c$, $c = 2, 3, \ldots, 5$, punctured convolutional codes with optimum free distance codes and MS mother codes are given.**
Simulation results for woven convolutional codes with MS component codes are presented. It is shown, that the component code choice makes a tradeoff between d_f and α.

I. Introduction

The active distance family was recently introduced in [1]. It is a new type of distance measure on binary convolutional codes. For example the active burst distance a_j^b is defined as the minimal Hamming weight among all c–tuple code sequences of length j that start and terminate in the all–zero state and do not have consecutive all–zero encoder state transitions associated with all–zero input. The active burst distance determines the error correcting capability of the code. All other active distances are defined in the same manner, but for different sets of start and terminal states. In [2] it is proven that asymptotically in j the minimum weight code sequence follows a cycle in the encoder state diagram. Hence, the minimum average weight growth is given by the cycle with smallest average weight and the active distances are lower bounded by linear increasing functions with slope α. Upper and lower bounds on α were derived in [3] and [4].

In [5, 6] encoding properties and decoding aspects of woven convolutional codes are discussed. The free distance and the slope of the component codes used in this construction essentially describe the woven convolutional code active distances. Furthermore, it is shown that the bit error rate performance of woven convolutional codes depend strongly on these parameters.

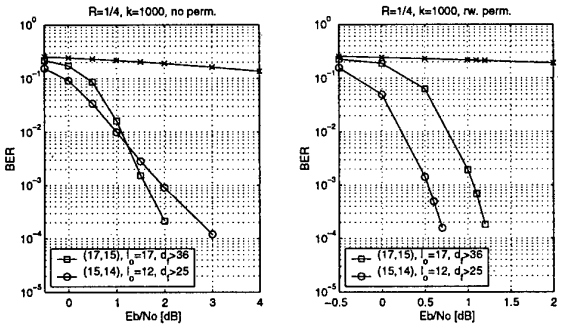
II. Maximum Slope Codes

The computation of the active distances is realized by using transfer function methods based on the encoder state transition matrix. An effective and efficient method to compute α for small overall constraint lengths is presented. Some rate $R = 1/2$ MS codes with memory $m = 2, \ldots, 5$ are given in the table below.

m	d_f	α	$G(D)$
2	4	2/3	(7 6)
	5	1/2	(7 5)
3	5	4/7	(15 14)
	6	1/2	(15 17)
4	7	3/8	(31 35)
5	7	4/9	(70 65)
	8	2/5	(76 65)

III. Simulation Results

The following figure depicts simulation results for the $R = 1/4$ terminated woven convolutional codes $(l_o, 1)$. On the left side no permutation was performed, on the right side row wise permutation was applied.



The bit error performance of serial concatenated Turbo codes show a similar behavior. Hence, the slope of the component codes is an important design parameter for serial concatenated codes with additional interleaving.

References

[1] S. Höst, R. Johannesson, K. Zigangirov, and V. Zyablov, "Active distances for convolutional codes," *IEEE Trans. on Inform. Theory*, vol. IT-45, pp. 658–669, March 1999.

[2] I. L. Traiger, A. Gill, "On an asymptotic optimization problem in finite directed weighted graphs," in *Information and Control*, vol. 13, pp. 527-533, March 1968.

[3] G. K. Huth, C. L. Weber, "Minimum weight convolutional codewords of finite length," in *IEEE Trans. on Inform. Theory*, vol. IT-22, pp. 243-246, March 1976.

[4] F. Hemmati, D. J. Costello, "Asymptotically catastrophic convolutional codes," in *IEEE Trans. on Inform. Theory*, vol. IT-26, pp. 298-304, May 1980.

[5] S. Höst, R. Johannesson, V. Zyablov, "Woven Convolutional Codes I: Encoder Properties," *submitted to IEEE Trans. on Inform. Theory*, 2000.

[6] M. Bossert, S. Höst, R. Jordan, R. Johannesson, V. Zyablov, "Woven Convolutional Codes II: Decoding Aspects," *In preparation*, 2000.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Decoding of Woven Convolutional Codes and Simulation Results

R. Jordan, W. Schnug, and M. Bossert
Dep. of Information Technology
University of Ulm
Albert-Einstein-Allee 43
D-89081 Ulm, Germany
e-mail: {ralph.jordan, walter.schnug, boss}@e-technik.uni-ulm.de

S. Höst and R. Johannesson
Dep. of Information Technology,
Information Theory Group
Lund University
P.O. Box 118
SE-221 00 Lund, Sweden
e-mail: {stefan.host, rolf}@it.lth.se

V. V. Zyablov
Inst. for Problems of Information
Transmission of the Russian
Academy of Science
B. Karetnyi per., 19, GSP-4
Moscow, 101447 Russia
e-mail: zyablov@iitp.ru

Abstract — **An iterative decoding scheme for woven convolutional codes is presented. It is called pipeline decoding and operates in a window sliding over the received sequence. This exploits the nature of convolutional codes as sequences and suits the concept of convolutional encoding and decoding as a continuous process. The pipeline decoder is analyzed in terms of decoding delay and decoding complexity.**

Additional interleaving for woven convolutional constructions is introduced by employing a convolutional scrambler. It is shown that some types of interleaving preserve the lower bound on the free distance of the original woven construction.

Simulation results for woven convolutional codes are presented.

I. Introduction

In [1, 2] three related woven constructions were introduced, viz.,

- woven convolutional codes with *outer* warp $(l_o, 1)$,
- woven convolutional codes with *inner* warp $(1, l_i)$,
- the *twill* (l_o, l_i),

where the (l_o, l_i) denotes the number of encoders in the outer and inner warps, respectively. The encoder for a woven convolutional code is represented by a serial concatenation of two warps both consisting of a set of parallel convolutional encoders, see Fig. 1. If l_o and l_i are relatively prime and large enough, the free distance of the woven convolutional code satisfies

$$d^w_{\text{free}} \geq d^o_{\text{free}} d^i_{\text{free}}, \tag{1}$$

where d^o_{free} and d^i_{free} denote the free distances of the outer and inner component code, respectively.

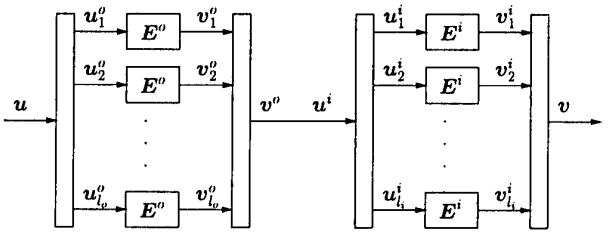


Fig. 1: Encoder for the twill.

II. Iterative Decoding

In contrast to the well known iterative decoding scheme of serially concatenated truncated convolutional codes [3, 4], the presented decoding scheme, called pipeline decoding, operates with a sliding window technique over the received sequence. For the symbol–by–symbol *a posteriori* decoding of the inner and outer component codes a sliding window version of the BCJR algorithm [5] is employed. The window is separated into one decision window of size w_d and one delay window of size w_b. Based on the sizes of these windows we analyze the decoding delay and the decoding complexity of the W–BCJR, as well as that of the pipeline decoder. Simulation results for the pipeline decoder are presented.

III. Additional Interleaving

Additional interleaving can significantly improve the bit error performance at low signal to noise ratios. To preserve the convolutional code structure of the overall code, we use convolutional scramblers for interleaving.

It is shown, that the woven construction can apply additional random interleaving without violating the lower bound on the free distance of the original construction (1). Furthermore, additional interleaving can be applied to reduce the number of encoders, l_o and l_i, while the lower bound (1) still holds.

IV. Simulation Results

Simulation results show that terminated woven convolutional codes are attractive alternatives to both parallel and serial concatenation of convolutional codes, e.g., Turbo codes.

References

[1] S. Höst, "On Woven Convolutional Codes," Ph.D. thesis, Lund University, Sweden, 1999, ISBN: 91-7167-016-5.

[2] S. Höst, R. Johannesson, and V. Zyablov, "Woven Convolutional Codes I: Encoder Properties," *submitted to IEEE Trans. on Inform. Theory*, Jan., 2000.

[3] J. Hagenauer, E. Offer, and L. Papke, "Iterative Decoding of Binary Block Codes and Convolutional Codes," *IEEE Trans. on Inform. Theory*, vol. IT-45, pp. 429–445, 1996.

[4] S. Benedetto and G. Montorsi, "Serial Concatenation of Interleaved Codes: Performance Analysis, Design, and Iterative Decoding," *IEEE Trans. on Inform. Theory*, vol. IT-44, pp. 909–926, 1998.

[5] L.R. Bahl, J. Cocke, F. Jelinek, and J. Raviv, "Optimal Decoding of Linear Codes for Minimum Symbol Error Rate," *IEEE Trans. on Inform. Theory*, vol. IT-20, pp. 284–287, 1974.

[6] M. Bossert, S. Höst, R. Jordan, R. Johannesson, and V. Zyablov, "Woven Convolutional Codes II: Decoding Aspects," *In preparation*, 2000.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Universal Prediction of Individual Binary Sequences in the Presence of Arbitrarily Varying, Memoryless Additive Noise[1]

Tsachy Weissman
tsachy@tx.technion.ac.il

Neri Merhav
merhav@ee.technion.ac.il

Abstract — **The problem of predicting the next outcome of an individual binary sequence, based on past observations which are corrupted by arbitrarily varying memoryless additive noise, is considered. The goal of the predictor is to perform, for each individual sequence, "almost" as well as the best in a set of experts, where performance is evaluated using a general loss function. This setting is a generalization of the original problem of universal prediction of individual sequences relative to a set of experts (cf., e.g., [2] and the many references therein).**

I. Introduction

The noise model considered in this work is that where the observation available to the predictor to make its prediction for time t is the vector $(y_1, \ldots, y_{t-1})$, where $y_i = x_i + r_i$, x_i is the clean bit at time i, and $r = \{r_t,\ t \geq 1\}$ is some arbitrarily varying memoryless noise process. The additive noise model considered in this work differs from the binary-valued noise model considered in [1], [3]-[5] (where the observed bit is the bitwise XOR of the clean bit and the noise bit) and joins it to give a more complete picture for the noisy setting [6]. It is shown that even in this noisy environment, when the information available regarding the past sequence is incomplete, a predictor can be guaranteed to successfully compete with a whole set of prediction schemes in considerably strong senses. Furthermore, these performance guarantees are valid for a very large family of noise processes, though the predictor itself does not depend on the statistical characterization of the particular active noise process within this class. In other words, it is *twofold universal* where, in this context, twofold universality stands for universality in the usual sense (w.r.t. the experts in the class and all possible sequences) *and* w.r.t. a family of noise distributions.

II. Statement of the Problem and Main Results

Let $L : \{0,1\} \times [0,1] \to [0,\infty]$ be a fixed *loss function*. A *predictor* (or an *expert*) $F = \{F_t\}_{t\geq 1}$ is a sequence of functions where $F_t : \mathbf{R}^{t-1} \to [0,1]$. We define the cumulative loss of the predictor F, fed by $y^n = (y_1, \ldots, y_n)$ and judged with respect to $x^n = (x_1, \ldots, x_n) \in \{0,1\}^n$ by $L_F(y^n, x^n) \stackrel{\text{def}}{=} \sum_{t=1}^n L(x_t, F_t(y^{t-1}))$. We consider the case where the noisy observation accessible to the predictor, $y = (y_1, y_2, \ldots) \in \mathbf{R}^\infty$ is given by $y_t = x_t + r_t$, $t \geq 1$, where $r = \{r_t, t \geq 1\}$ is a zero-mean, memoryless, arbitrarily varying process: for every n, the p.d.f. governing $r^n = (r_1, \ldots, r_n)$ is of the form: $f(r^n|s^n) = \prod_{i=1}^n f(r_i|s_i)$, where $s^n \in \mathcal{S}^n$ is some unknown *arbitrary* sequence of states, and $\mathcal{S}$, is some abstract state-space such that for all $\sigma \in \mathcal{S}$ we have $\int_{-\infty}^{\infty} r \cdot f(r|\sigma)dr = 0$.

Letting $L_F(x^n) \stackrel{\text{def}}{=} EL_F(y^n, x^n)$ denote the expected loss of F when the underlying individual sequence is x^n, we define the *worst-case relative expected loss* of a predictor P by $R_n(P, \mathcal{F}) \stackrel{\text{def}}{=} \max_{x^n \in \{0,1\}^n} (L_P(x^n) - \inf_{F\in\mathcal{F}} L_F(x^n))$. It is shown that, for a large class of loss functions, for any finite set of experts $\mathcal{F}$, there exists a predictor P such that $R_n(P, \mathcal{F}) = O((\ln n)^2 \cdot \ln|\mathcal{F}|)$, while for another class of loss functions we have $R_n(P, \mathcal{F}) = O(\sqrt{n \ln|\mathcal{F}|})$.

Further results show, however, that the prediction strategies that we suggest are guaranteed to be doing well in considerably stronger senses. It is shown that under some mild additional conditions on the noise process, the predictor P satisfies

$$\limsup_{n\to\infty} \frac{L_P(y^n, x^n) - \inf_{F\in\mathcal{F}} L_F(y^n, x^n)}{\sqrt{n \log\log n}} \leq c \quad \text{a.s.} \quad \forall x \in \{0,1\}^\infty,$$

for some deterministic constant c. It is further shown that, using this same predictor, we also have

$$\max_{x^n\in\{0,1\}^n} \Pr\{\frac{1}{n}[L_P(y^n, x^n) - \min_{\mathcal{F}} L_F(y^n, x^n)] > \epsilon\} \leq \exp\{-n(I(\epsilon, B) + o(n))\},$$

where, $I(\epsilon, B) > 0$, which lower bounds the possible exponential rate of the decay, is independent of the expert class $\mathcal{F}$.

The remarkable feature of the predictors that we employ is the strong sense in which they are twofold universal. The above described performance bounds hold with the *same* universal predictor P, regardless of the particular state sequence driving the noise process.

References

[1] A. Baruch, "Universal Algorithms for Sequential Decision in the Presence of Noisy Observations," submitted to the senate of the technion (Master's thesis), February 1999. (See also Proc. ISIT 98', p. 331, Cambridge, MA, August 1998.)

[2] D. Haussler, J. Kivinen, and M.K. Warmuth, "Sequential Prediction of Individual Sequences Under General Loss Functions," *IEEE Trans. Inform. Theory*, vol. 44, pp. 1906-1925, September 1998.

[3] T. Weissman and N. Merhav, "On Prediction in the Presence of Noise," unpublished manuscript, 1999 (preprint available).

[4] T. Weissman and N. Merhav, "On Prediction of Individual Sequences Relative to a Set of Experts in the Presence of Noise," in *Proc. 12th Annu. Workshop on Computational Learning Theory*, pp. 19-28, New York: ACM, 1999.

[5] T. Weissman, A. Baruch and N. Merhav, "Twofold Universal Prediction Schemes for Achieving the Finite-State Predictability of a Noisy Individual Binary Sequence," To be submitted to *IEEE Trans. Inform. Theory* (preprint available).

[6] T. Weissman and N. Merhav, "Universal Prediction of Individual Binary Sequences in the Presence of Noise," Submitted to *IEEE Trans. Inform. Theory*, Nov. 1999.

[1]The research, which is supported by the Israeli Science Foundation, is part of the D.Sc. dissertation of the first author. Both authors are with the Department of Electrical Engineering, Technion-Israel Institute of Technology, Haifa 32000, Israel.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Worst-case Bounds for the Redundancy of Sequential Lossless Codes and for the Logarithmic Loss of Predictors

Nicolò Cesa-Bianchi
Polo Didattico e di Ricerca,
University of Milano
Via Bramante 65,
26013 Crema, Italy
email:cesabian@dsi.unimi.it

Gábor Lugosi
Department of Economics
Pompeu Fabra University
Ramon Trias Fargas 25-27 08005
Barcelona, Spain
email: lugosi@upf.es

Abstract — **We investigate on-line prediction of individual sequences. Given a class of predictors, the goal is to predict as well as the best predictor in the class, where the loss is measured by the self information (logarithmic) loss function. The excess loss (regret) is closely related to the redundancy of the associated lossless universal code. Using Shtarkov's theorem [3] and tools from empirical process theory, we prove a general upper bound on the best possible (minimax) regret. The bound depends on certain metric properties of the class of predictors and is applicable to both parametric and nonparametric classes of predictors.**

I. Summary

Assume that elements of an arbitrary sequence $y_1, \ldots, y_n$ are revealed one by one, where the elements y_t belong to some set measurable $\mathcal{Y}$. At each time $t = 1, \ldots, n$, before revealing an element y_t, we are asked to assign a probability density p_t on $\mathcal{Y}$ and then observe y_t incurring the logarithmic loss $-\ln p_t(y_t)$. Our total loss at the end is the sum of the losses suffered at each round. As we know the prefix $y_1, \ldots, y_{t-1}$ before choosing each probability assignment p_t, we may view each p_t as the conditional $p(\cdot \mid y_1, \ldots, y_{t-1})$ of some joint distribution p that we choose before the game begins. We call p a *prediction strategy*. Any strategy for playing this game is equivalent to a probability distribution on $\mathcal{Y}^n$.

Our goal is to predict (almost) as well as the best strategy in a given "reference" set of strategies. We call "experts" the strategies in the reference set. In other words, we intend to accumulate a loss not much larger than that of the best expert, regardless of what the sequence $y_1, \ldots, y_n$ might be.

In this paper we investigate the minimum excess loss, with respect to the total loss of the best expert, achievable on any sequence. This quantity, known as minimax regret (under logarithmic loss), turns out to depend on certain metric properties of the class $\mathcal{F}$ of experts.

It is well-known that every sequential prediction strategy may be converted into a sequential lossless source code. Conversely, every uniquely decodable code over $\mathcal{Y}^n$ defines a probability distribution. Thus, the prediction problem under logarithmic loss is formally equivalent to the problem of sequential universal coding in data compression. In this context, the subject of our study is the smallest achievable worst-case redundancy of a sequential lossless code, with respect to a general class of reference codes.

This research was supported in part by ESPRIT Working Group EP 27150, Neural and Computational Learning II (NeuroCOLT II) and DGES grant PB96-0300. The first author was also partially supported by MURST project "Modelli di calcolo innovativi: metodi sintattici e combinatori".

Fix a class $\mathcal{F}$ of "reference" strategies, called here *experts*. The *worst-case regret* of a strategy p (with respect to the class $\mathcal{F}$) is defined by

$$R_n(p, \mathcal{F}) = \sup_{y^n} \ln \frac{\sup_{\mathcal{F}} f(y^n)}{p(y^n)} .$$

In other words, $R_n(p, \mathcal{F})$ is the worst-case difference between the log-likelihood of y^n under the density p and the log-likelihood of y^n under its maximum likelihood estimator in the class $\mathcal{F}$. The smallest worst-case regret achievable by any predictor is the *minimax regret*

$$R_n(\mathcal{F}) = \inf_{p} \sup_{y^n} \ln \frac{\sup_{\mathcal{F}} f(y^n)}{p(y^n)}$$

where the infimum is taken over all densities p on $\mathcal{Y}^n$.

To any class $\mathcal{F}$ of experts, we associate the metric d defined by

$$d(f, g) = \sqrt{\sum_{t=1}^{n} \sup_{y^t} \left(\ln f(y_t|y^{t-1}) - \ln g(y_t|y^{t-1})\right)^2} . \quad (1)$$

We use $N(\mathcal{F}, \varepsilon)$ to denote the ε-covering number of $\mathcal{F}$ under the metric d, that is, the cardinality of the smallest subset $\mathcal{F}' \subseteq \mathcal{F}$ such that

$$(\forall f \in \mathcal{F})(\exists g \in \mathcal{F}') \quad d(f, g) \le \varepsilon .$$

Our main result is the following:

Theorem 1 *For any class $\mathcal{F}$ of experts,*

$$R_n(\mathcal{F}) \le \inf_{\varepsilon > 0} \left(\ln N(\mathcal{F}, \varepsilon) + 24 \int_0^{\varepsilon} \sqrt{\ln N(\mathcal{F}, \delta)}\, d\delta \right) .$$

The theorem improves on previous general results in [1] and [2]. We may use the theorem to obtain tight upper bounds for $R_n(\mathcal{F})$ for both parametric and nonparametric classes. For example, for parametric classes we obtain:

Corollary 1 *Assume that there exist positive constants k and c such that for all $\varepsilon > 0$, $\ln N(\mathcal{F}, \varepsilon) \le k \ln \frac{c\sqrt{n}}{\varepsilon}$. Then*

$$R_n(\mathcal{F}) \le \frac{k}{2} \ln n + o(\ln n) .$$

References

[1] Opper, M. and D. Haussler: 1997, 'Worst Case Prediction over Sequences under Log Loss'. In: *The Mathematics of Information Coding, Extraction, and Distribution*. Springer Verlag.

[2] Rissanen, J.: 1996, 'Fischer Information and Stochastic Complexity'. *IEEE Transactions on Information Theory* **42**, 40–47.

[3] Shtarkov, Y.: 1987, 'Universal Sequential Coding of Single Messages'. Translated from: *Problems in Information Transmission* **23**(3), 3–17.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Filtering and Prediction of Individual Sequences Corrupted By Noise Using the Lempel-Ziv Algorithm

Anelia Baruch and Neri Merhav
Dpt. EE, Technion, Haifa Israel
anelia@tx.technion.ac.il
merhav@ee.technion.ac.il

Abstract — **We address the problem of filtering and prediction of an individual binary sequence based on its *noisy* past, as an extension to [1]. The performance criterion investigated is the expected fraction of errors. We propose algorithms and compare their performance to that of the best finite state machine (FSM). We improve on previous results [1] by showing that optimum performance can be achieved by Lempel-Ziv-based estimation algorithms.**

I. Introduction

Let $\theta_1, \theta_2, \ldots$ be an arbitrary binary sequence corrupted by a Bernoulli noise process $\nu_1, \nu_2, \ldots$ with $Pr\{\nu_i = 1\} \stackrel{\Delta}{=} p$. An observer accesses the noisy sequence $y_1, y_2, \ldots$, where $y_i = \theta_i \oplus \nu_i$, and $\oplus$ denotes addition modulo 2. The observer is interested in either estimating θ_i (filtering), or predicting θ_{i+1} (prediction), based on $y_1, y_2, \ldots, y_i$. We seek a universal estimator whose bit error probability is essentially as small as that of the best FSM, simultaneously for all θ. Previous work [3],[2] can be viewed as a special case of this filtering problem, where in [2] it was shown that there exists a sequential estimator whose asymptotic performance is as good as that of the best estimator that is implementable by a single-state machine. In [2], prediction without noise was considered and a sequential LZ-based predictor was shown to attain the finite state predictability of all infinite sequences. In this work, we improve on previous results of [1] where an asymptotically optimum sequential algorithm with growing memory was introduced. In this work we present a more practical, LZ-based algorithm that achieves the same goal.

A finite-state filter (FSF) with S states is a causal device that, upon receiving a sequence of observations $y_1, y_2, \ldots$, generates a sequence of estimates $\hat{\theta}_1, \hat{\theta}_2, \ldots$, while going through a sequence of states $s_1, s_2, \ldots$ that take on values in a finite set $\mathcal{S} = \{1, 2, \ldots, S\}$. The mechanism of the FSF is defined by a pair of deterministic functions f and g, where f is the *output function* that is given by $\hat{\theta}_i = f(s_i, y_i)$ for filtering and $\hat{\theta}_{i+1} = f(s_i)$ for prediction, and g is the *next-state function* that defines a recursive state update rule, according to $s_{i+1} = g(s_i, y_i)$. Let G_S be the set of all next-state functions of no more than S states. Henceforth, $x_i^j, i \le j$, generically designates $(x_i, x_{i+1}, \ldots, x_j)$. Also, denote by g_k the k-th order Markovian next-state function whose state at time instant t is defined by $s_t = y_{t-k}^{t-1}$. For a given (f, g), let $e(\theta_1^n, \nu_1^n, (f, g)) \stackrel{\Delta}{=} \frac{1}{n}\sum_{t=1}^{n} 1_{\{\hat{\theta}_t \neq \theta_t\}}$ be the fraction of errors attained when (f, g) is applied to y_1^n. Let $e_g(\theta_1^n) \stackrel{\Delta}{=} \min_f E\{e(\theta_1^n, \nu_1^n, (f, g))\}$, and define the *FS filterability* of an infinite sequence θ by $e(\theta) = \lim_{S\to\infty} \lim_{n\to\infty} \min_{g\in G_S} e_g(\theta_1^n)$. The *aperiodic FS filterability*, $\bar{e}(\theta)$, is defined similarly, with the exception that the minimization is over the class of aperiodic machines, and the *Markovian filterability*, $\mu(\theta)$, is defined by $\lim_{k\to\infty} \lim_{n\to\infty} e_{g_k}(\theta_1^n)$.

[1] This work was supported by the ISF administered by the Israeli Academy of Sciences and Humanities.

II. Main Results

Our main result is a derivation of a scheme that asymptotically achieves $e(\theta)$. This scheme is based on the incremental parsing (IP) procedure of the LZ '78 algorithm, and can be viewed as a Markovian machine of increasing order. The transition between states is identical to that of the equivalent scheme in [2], apart of the fact that it is the noisy sequence $\{y_t\}$ which determines the states sequence rather than the clean one. The state at time instant t is the string of bits observed since the last phrase has terminated.

The estimation is as follows: denote by $N_t^y(s,x) = \sum_{i=1}^{t-1} 1_{\{s_i=s, y_{i+1}=x\}}$ the joint count of state s and the value of the *next noisy* bit being x, and let $\tilde{N}_t^y(s,x)$ be a randomized version of it, i.e., $\tilde{N}_t^y(s,x) = N_t^y(s,x) + z_x(t)\,(N_t(s))^{1/2}$ where $\{z_x(t)\}_{t=1}^n, x \in \{0,1\}$, are independent r.v.'s uniformly distributed over the interval $[0,1]$ and $N_t(s) = \sum_{i=1}^{t} 1_{\{s_i=s\}}$.

Let $N_t^\theta(s,x) = \sum_{i=1}^{t-1} 1_{\{s_i=s, \theta_i=x\}}$ be the joint count of state s and the value of the *current clean* bit being x. Now, an estimation of $N_t^\theta(s,x)$ is performed: $\hat{N}_t^\theta(s,x) = \frac{1}{1-2p}\sum_{i=1}^{t-1} 1_{\{s_i=s, y_i=x\}} - \frac{2p}{1-2p} N_t(s)$, and some auxiliary randomization is introduced which results in $\tilde{N}_t^\theta(s,x) = \hat{N}_t^\theta(s,x) + z_x(t)\,(N_t(s))^{1/2}$.

For prediction, the decision rule is $\hat{\theta}_{t+1} = x$ if $\tilde{N}_t^y(s_t,x) > \tilde{N}_t^y(s_t, 1-x)$. For filtering, the decision rule is $\hat{\theta}_t = x$ if $\tilde{N}_t^\theta(s_t,x) > \frac{p}{1-p}\tilde{N}_t^\theta(s_t, 1-x)$, and otherwise $\hat{\theta}_t = y_t$, where ties are broken arbitrarily. Denote by $e^{IP}(\theta_1^n)$ the expected fraction of errors made by this scheme.

Our first result is that, when prediction is concerned $e_{g_k}(\theta_1^n) - \min_{g\in G_S} e_g(\theta_1^n) \le \frac{1}{1-2p}\sqrt{\frac{\ln S}{2(k+1)}}$ and therefore $\mu(\theta) = e(\theta)$. When both filtering and prediction are concerned we show that $e_{g_k}(\theta_1^n) - \min_{g\in G_s, g\ aperiodic} e_g(\theta_1^n) \le O(\alpha(S,p))^k + \frac{k}{n}$ where $|\alpha(S,p)| < 1$ which implies that $\mu(\theta) \le \bar{e}(\theta)$ for filtering. We further show that $e^{IP}(\theta_1^n) - e_{g_k}(\theta_1^n) \le O\left(\frac{1}{\sqrt{\log n}}\right) + O\left(\frac{k}{\log n}\right)$. Combining these two observations it follows that the above described scheme achieves the FS filterability.

References

[1] A. Baruch, N. Merhav "Universal Filtering of Individual Sequences Corrupted by Noise", *Proc. ISIT 1998* p. 331 .

[2] M. Feder, N. Merhav and M. Gutman, "Universal Prediction of Individual Sequences," *IEEE Trans. Inform. Theory*, vol. 38, pp. 1258–1270, July 1992.

[3] J. V. Ryzin, "Asymptotic solutions of the sequential compound decision problem," *Ann.Math. Statist.*, vol. 37, pp. 954-975, 1966.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Iterative Correction of ISI via Equalization and Decoding with Priors

Michael Tüchler[1], Ralf Koetter, Andrew Singer
University of Illinois at Urbana-Champaign
e-mail: {tuechler,koetter,acsinger}@uiuc.edu

Abstract — **An iterative algorithm is presented for joint equalization and decoding of data that has been transmitted over intersymbol interference (ISI) channels. This differs from well-known "turbo equalization" (TEQ) methods, in that the ISI is removed with a soft-input soft-output (SISO) equalizer via linear or decision feedback equalization (DFE). The data is encoded with a convolutional code and interleaved prior to transmission over the channel. At the receiver, symbol estimates are successively refined by passing extrinsic information, in the form of priors over the symbols, between the SISO equalizer and a SISO decoder based on maximum-aposteriori-probability (MAP) symbol estimation. The low complexity of this algorithm make it a practical alternative to existing methods, without sacrificing bit error rate (BER) performance.**

I. Introduction

Data transmission over ISI channels is a classical problem in communication scenarios. Conventional approaches implement an equalizer to remove ISI or use MAP or maximum likelihood (ML) detection. Data reliability can be enhanced using coding, where the data is encoded in the transmitter prior to transmission. For reasons of complexity, the receiver then typically performs separate equalization and decoding of the data. Significant performance gains can be achieved through joint equalization and decoding at the cost of added complexity. A recent approach that significantly reduces the complexity of joint equalization and decoding is the so-called "turbo equalization" algorithm, where MAP/ML detection and decoding are performed iteratively on the same set of received data [4, 5]. It has recently been shown that passing soft information, the use of interleaving, and the controlled feedback of soft information are essential requirements to achieve performance gains with an iterative system [1]. Various algorithms similar to TEQ have been proposed to overcome the complexity of the MAP/ML algorithms, especially in the detector, where complexity is exponential in the channel delay spread [2, 3].

An algorithm that is a practical alternative to turbo equalization is presented in this paper. In an approach similar to that of Wang and Poor [2], the MAP/ML detector in the TEQ setup is replaced by a linear equalizer (LE) or DFE. The filter coefficients are selected according to a minimum mean squared error criterion (MMSE), taken over both the statistics of the noise and the prior over the symbols.

II. Concepts

A block diagram of the data transmission system is shown in Figure 1. In the receiver, the SISO equalizer and SISO decoder exchange priors over the possible values of each code symbol c_n. The SISO equalizer consists of an estimator, providing

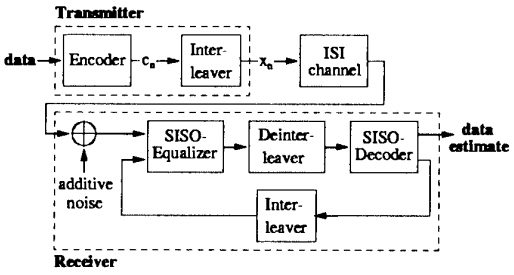


Figure 1: *Data Transmission System*

the estimates $\hat{x}_n$ of the transmitted symbols x_n, followed by a mapping that transforms $\hat{x}_n$ to a prior over the transmitted symbol at time n. The SISO decoder uses this soft information to decode the data and produce an additional prior over the symbols, which can be interpreted as soft feedback information for the equalizer. The SISO equalizer minimizes the MMSE cost function $E\{|x_n - \hat{x}_n|^2\}$ using the time varying statistics $E\{x_n\}$ and $Cov\{x_n x_m^*\}$, which are computed for each received symbol using the soft feedback information [1].

For the SISO equalizer, a time-recursive update algorithm with $O(N^2+M^2)$ (exact implementation) and $O(N+M)$ (approximate) complexity per received symbol and iteration was developed [1], where M is the ISI channel length and N the length of the equalization filter. Both implementations yield significant savings in the computational complexity compared to MAP/ML-based detectors with $O(q^M)$ complexity, where q is the size of the alphabet of the transmitted symbols x_n.

III. Results

From the set of possible equalizer implementations, the exact implementation of the LE-based SISO equalizer performs best in terms of BER and can match or beat the performance of the approach in [3] and even the MAP-based TEQU approach in [5]. The DFE-based solutions are shown to perform worse than LE-based solutions [1]. The performance improvements of the proposed algorithm over that of the TEQ approach, for certain ISI channels and data block lengths, demonstrates that BER-optimum SISO receiver elements (detector, decoder) are not necessarily optimum in an iterative setup [1].

[1] This work was supported by NSF Grant CCR 99-79381.

References

[1] Michael Tüchler, "Iterative equalization using priors," M.S. thesis, University of Illinois, Urbana-Champaign, IL, U.S.A., 2000.

[2] X. Wang and H.V. Poor, "Turbo multiuser detection and equalization for coded CDMA in multipath channels," in *IEEE Int. Conf. on Universal Press Comm.*, vol. 2, 1998, pp. 1123-1127.

[3] A. Glavieux, C. Laot, and J. Labat, "Turbo equalization over a frequency selective channel," *Int. Symp. on Turbo codes & related topics*, pp. 96-102, September 1997.

[4] C. Douillard et al., "Iterative correction of intersymbol interference: turbo equalization," *Europ. Trans. on Tel.*, vol. 6, no. 5, pp. 507-511, Sept.-Oct. 1995.

[5] G. Bauch and V. Franz, "A somparison of soft-in/soft-out algorithms for "turbo-detection"," in *Proc. on the Int. Conf. on Tel.*, June 1998, pp. 259-263.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Use of the List Viterbi Algorithm to Compute the Distance Spectrum of Trellis Codes and ISI Channels

Sabah Badri-Hoeher
Wireless Telecommun. and Multimedia Technology
Fraunhofer Gesellschaft (FhG)
Am Weichselgarten 3, D-91058 Erlangen, Germany
e-mail: bar@iis.fhg.de

Peter Hoeher
Information and Coding Theory Lab
University of Kiel
Kaiserstr. 2, D-24143 Kiel, Germany
e-mail: ph@techfak.uni-kiel.de

Abstract — **We propose to compute the distance spectrum of arbitrary trellis codes (including convolutional codes, trellis-coded modulation, continuous phase modulation, etc.) and intersymbol-interference (ISI) channels by means of a modified list Viterbi algorithm (LVA). This search procedure is (i) computationally efficient, (ii) is applicable to linear as well as nonlinear codes, (iii) can be applied to arbitrary distance measures, (iv) can be used for MLSE as well as RSSE or related techniques, and (v) guarantees that an ordered list of the N nearest error paths is produced. A sample results illustrates the distance spectra of linear ISI channels, both for MLSE and ideal RSSE receivers.**

I. Introduction

Prior solutions to compute the free distance of nonlinear codes include sequential algorithms, the Viterbi algorithm, and the Dijkstra algorithm. Solutions to compute the distance spectrum include sequential algorithms, transfer function methods, and a modified Viterbi algorithm with state-splitting and multiple passes, among other techniques. For special applications and particularly in the case of linear codes extensive simplifications are possible.

In the present paper, we propose to apply a modified LVA for the purpose of computing the distance spectrum of arbitrary trellises. LVAs compute an ordered list of the N best paths. Serial and parallel LVAs have extensively been investigated in [1] and the references therein in the context of decoding and related applications, but, to our best knowledge, not for distance calculations.

II. Distance Calculation using an LVA

Throughout this paper, we assume the existence of a trellis with a finite number of states. We consider a linear code first. In order to compute the distance spectrum with N error paths, it is sufficient to design a modified LVA for the *original trellis* taking the N best survivors into account, and to apply this LVA given noise-free channel outputs. An ordered list of the N nearest error paths is produced, if the following modifications are done:

1. All error paths taken into account must diverge from the transmitted sequence at time $k = 0$ and re-merge at time $k' > 0$. All other paths must be excluded, particularly the ML path and all paths that diverge more than once from the transmitted path.
2. Instead of outputting the N most likely information sequences [1], we output the accumulated path metrics (i.e., the distances) and the corresponding path weight (multiplicity) a_d and/or information weight c_d.

Without loss of generality, the transmitted sequence may be the all-zero sequence. Then, the all-zero path (i.e., the ML path) may be eliminated by setting the N accumulated distances of the all-zero state at the second interval of the trellis to infinity. The number of spectral lines is less than the number of error paths N actually computed, when the multiplicity $a_d > 1$ for at least one distance d. Whether a serial or a parallel type of LVA should be accomplished depends on memory and complexity constraints, among others. If the trellis is of finite length, the LVA may operate on the full trellis, otherwise a stop criterion must be applied.

These general design criteria also hold for nonlinear codes, which are discussed next. In the general case, we design the LVA to operate on the *product trellis* in order to take all error events into account. If the error events depend on difference symbols only, we may use the *difference trellis* instead. This is the case of linear ISI channels and CPM, e.g. In any case the symmetry of the error states has to be taken into account, either by eliminating redundant error events or by reducing the number of states.

For illustration, consider a time-invariant linear ISI channel with binary inputs $a_k \in \{\pm 1\}$ and channel coefficients h_l, $0 \le l \le L$. The difference symbols, $d_k = a_k - \tilde{a}_k$, take the values $\{-2, 0, +2\}$. In case of MLSE, the difference trellis has 3^L states, whereas the original trellis has 2^L states. However, due to the symmetry of the error states, we can use an equivalent difference trellis that has only $(3^L + 1)/2$ states Without loss of generality, we may assume that the all-zero difference sequence has been transmitted. A new spectral line is computed whenever an error path re-merges the all-zero difference path. In case of reduced-state sequence estimation (RSSE), the original trellis has 2^K states, where $0 < K \le L$. A new spectral line is computed whenever an error path merges in one of the $(3^{L-K} + 1)/2$ hyper states. Otherwise, the search algorithm is the same as described above.

Fig. 1 shows the (truncated) distance spectrum for an ISI channel given MLSE and ideal RSSE. (Ideal RSSE does not take error propagation into account.) The information weight is moderate for error paths with small distance, whereas larger spectral lines have a larger multiplicity and are less spread out.

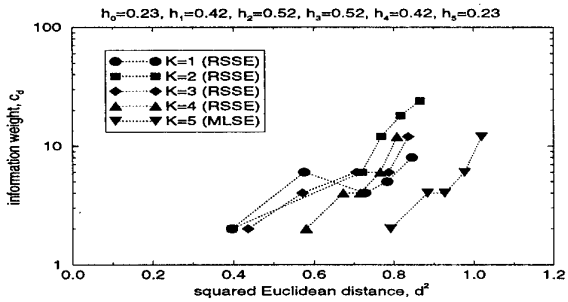


Fig. 1: Distance spectrum for MLSE and ideal RSSE for a binary, linear, time-invariant ISI channel with 32 states.

Reference

[1] N. Seshadri and C-E.W. Sundberg, "List Viterbi decoding algorithms with applications," *IEEE Trans. Commun.*, vol. 42, pp. 313-323, Feb./Mar./Apr. 1994.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

A New Successively Decodable Coding Technique for Intersymbol-Interference Channels[1]

Tommy Guess
Dept. EE, Univ. of Virginia
Charlottesville, VA 22904-4743

Mahesh K. Varanasi
Dept. ECE, Univ. of Colorado
Boulder, CO 80309-0425

Abstract — **For the Gaussian channel with intersymbol-interference (ISI), it is known that there is no loss in channel capacity if the receiver is an ideal minimum mean-squared error (MMSE) decision-feedback equalizer (DFE) with error-free feedback. However, combining the DFE with channel coding is problematic. Transmitter precoding and reduced-state sequence estimation are two common approaches (cf. [1] and references therein). This paper introduces a new successively-decodable coding technique that effectively combines channel coding with decision-feedback that is housed in the receiver.**

I. The Channel Model

Consider the real-valued discrete-time Gaussian channel with intersymbol interference (ISI) represented by

$$y_k = \sum_{j=0}^{M-1} h_j x_{k-j} + n_k, \qquad (1)$$

where $\{x_k\}$ is a sequence of zero-mean, independent identically-distributed (i.i.d.) transmitted symbols with power $E[x_k^2] = p$, $\{h_k\}_{k=0}^{M-1}$ is the finite-tap discrete-time, post-cursor channel response, and $\{n_k\}$ is an i.i.d. sequence of zero-mean Gaussian noise samples with variance $E[n_k^2] = \sigma^2$. The average mutual information of the channel (bits per channel use) is maximized when the symbol distributions are zero-mean Gaussian random variables with power p.

II. Successively Decodable Coding Technique

We describe the two-level successive decoder for the ISI channel from which the corresponding coding technique is easily inferred. Begin by blocking the channel output sequence into vectors of length L. We view this vector output sequence as N distinct vector channels, the n-th of which is given by

$$\left\{ \left[\; y_{(kN+n-1)L+1} \quad \cdots \quad y_{(kN+n)L} \; \right]^T \right\}_{k=-\infty}^{\infty}. \qquad (2)$$

Note that y_k is statistically independent of y_{k-M}. Therefore, if $N \geq \lceil \frac{M+L-1}{L} \rceil$, then the output sequence of the n-th channel is the output sequence of a memoryless vector channel. Thus, we have decomposed the ISI channel into N memoryless vector channels that are statistically related to each other.

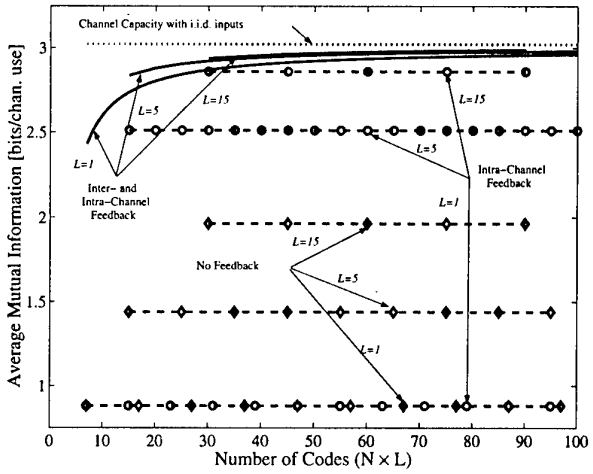
Outer-level coding allows the N vector channels to be decoded one at a time, starting with channel 1 and ending with channel N. If, when decoding the n-th channel, we make use of symbol decisions from the channels that have already been decoded (i. e., vector channels 1 through $n-1$), we refer to this as inter-channel feedback. Clearly, the potential advantage of inter-channel feedback increases with N, the number of vector channels.

Inner-level coding addresses each vector channel by viewing it as consisting of L scalar sub-channels that are successively decoded with single-user coders and decoders. If, when decoding the l-th sub-channel of a particular vector channel, we make use of symbol decisions from sub-channels that have already been decoded (i. e., sub-channels 1 through $l-1$), we refer to this as intra-channel feedback. Since this vector channel can be cast as a memoryless multiple-access channel, the optimal successive-decoding technique developed in [2] can be implemented. For any given vector channel, performance potential will improve as L, the block size, increases.

Hence, the original ISI channel is treated as a composition of NL sub-channels which are to be coded and decoded successively using single-user codes, with or without inter- and intra-channel feedback.

III. Example

Consider the response of the 2 kft-AWG26 channel (i. e., $h_0 = 1$, $h_1 = -0.6$, $h_2 = -0.15$, $h_3 = -0.12$, $h_4 = -0.05$, $h_5 = 0.00$, and $h_6 = 0.05$) [1], which is operating at a coded-symbol signal-to- noise ratio of $p/\sigma^2 = 18.0$ dB. The following figure compares the theoretical rate of information transmission for several schemes. The average mutual information is plotted as a function of the total number of sub-channels, NL. It is evident that increasing the vector length L can provide substantial gains for each scheme presented and that there is an advantage in implementing inter-channel feedback in addition to intra-channel feedback.



References

[1] D. Yellin, V. Vardy, and O. Amrani, "Joint Equalization and Coding for Intersymbol Interference Channels," *IEEE Trans. Inform. Theory*, vol. IT-43, pp. 409–425, Mar. 1997.

[2] M. K. Varanasi and T. Guess, " Optimum Decision Feedback Multiuser Equalization with Successive Decoding Achieves the Total Capacity of the Gaussian Multiple-Access Channel ," in *Proc. Thirty-First Asilomar Conf. Signals, Systems, and Computers* , pp. 1405–1409, Nov. 1997.

[1]This work was supported by NSF grant NCR-9725778 and the Colorado Center for Information Storage, University of Colorado, Boulder, CO 80309.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Partitioning for SA(B,C) detectors on ISI AWGN channels

Andreas Cedergren[1] and Tor M. Aulin
Dept. of Computer Engineering
Chalmers University of Technology
SE-412 96 Göteborg, Sweden
{andreasc, tor}@ce.chalmers.se

Abstract — **In this paper partitioning for the SA(B,C) algorithm on intersymbol interference (ISI) channels is considered. Substantial savings in complexity can be made by using the SA(B,C), while achieving almost optimal error performance.**

I. Introduction

A receiver that uses the SA(B,C) algorithm [2] for intersymbol interference (ISI) additive white gaussian noise (AWGN) channels is considered. SA stands for Search Algorithm. The SA(B,C) partitions the states in the trellis into C state classes. Then proceeding breadth first in the trellis, the detector selects B paths closest to the received signal for each state class. The number of computations per released symbol, which is to be minimized, is proportional to BC, the number of paths traced. The SA(B,C) family of algorithms perform maximum likelihood sequence detection (MLSD) under given structural and complexity constraints [2]. The Viterbi algorithm (VA) [1] performs complexity unconstrained MLSD. The performance of the SA(B,C) detector is here required to be asymptotically optimal (AO) [2], [3], i.e. the error event probability should approach unconstrained MLSD when the signal to noise ratio (SNR) $\rightarrow \infty$. Given the parameter B, there will be constraints on how to construct the partition i.e., which states that can belong to the same state class. To find an optimum partition is in its general form an NP-hard problem, e.g., when $B = 1$ the problem is equivalent to the graph coloring problem [3]. Here the size of the problem of finding a partition is limited by imposing structural constraints on the partition.

The cases $B < S; C = 1$ and $B = 1; C \leq S$ are considered in [2] and [3], respectively. S is the number of states in the trellis. The case $B < S; C = 1$ is optimal with respect to complexity [2]. Here the results in [2] and [3] are generalized to the case $B = 2; C \geq 1$. This method can be generalized to apply for an arbitrary B.

II. System Description

The message to be sent over an ISI AWGN channel is a sequence $\mathbf{a}_N = \{a_0, a_1, \ldots, a_{N-1}\}$ of statistically independent equally probable data symbols drawn from an M-ary alphabet. The MLSD finds the candidate sequence having the minimum log likelihood metric given the received sequence. This can be calculated recursively using the VA or the SA(B,C). The states in the trellis, which the detectors operate in, are given by $\sigma_n = (a_{n-1}, \ldots, a_{n-L+1})$ where $L-1$ is the memory of the channel. For large SNR the error event probability of the SA(B,C) detector can be approximated as [2]

$$\Pr(error) \approx K_1 Q\left(\sqrt{d^2_{\min} SNR}\right) + K_2 Q\left(\sqrt{d^2_{l,\min} SNR}\right)$$

where $d^2_{l,\min}$ is the minimum vector Euclidean distance and $d^2_{\min}$ is the minimum Euclidean distance for the VA, K_1 and K_2 are constants. By requiring that $d^2_{l,\min} \geq d^2_{\min}$, the SA($B$,$C$) detector will be AO.

III. Partitioning

To find a constrained partition, consider the states written on the form $\sigma_n = (a_{n-1}, a_{n-2}, \ldots, a_{n-L+1})$. Next, define the partition vector [3] $\mathbf{\Gamma} = (\Gamma_1, \Gamma_2, \ldots, \Gamma_{L-1})$ where Γ_k, $1 \leq k \leq L-1$, denotes a partition of the symbol alphabet for the kth position in the state vector. Let γ_k be the number of subsets defined by partition Γ_k. Each subset is identified by a label in the range $0, 1, \ldots, \gamma_k - 1$. No connection is assumed between the partitions Γ_k. The partition vector may be employed to map every state σ_n into a corresponding vector of subset labels $\lambda_n^{(i)} = (\lambda_{n1}, \lambda_{n2}, \ldots, \lambda_{nL-1})$, where λ_{nk}, $1 \leq k \leq L-1$, is the subset label of a_{n-k} in the partition Γ_k. A state-class is defined as the set of states that map onto the same subset vector: $\Omega^{(i)} = \left\{\sigma : \sigma \rightarrow \lambda^{(i)}\right\}$, $i = 1, 2, \ldots, C$.

The first step in constructing a partition is to obtain some finite set, P, of alphabet partitions from which the partition vector is to be constructed. Finding P is a problem that only has to be solved once for each alphabet. This can be done by imposing a certain degree of regularity on the alphabet partitions, by considering rotational invariance and difference symbols [3]. The next step is to find the states that has to be partitioned into different state classes. The final step is to perform a search for a minimum partition vector $\mathbf{\Gamma}$ among the set of vectors $(\Gamma_1, \Gamma_2, \ldots, \Gamma_{L-1})$ with elements $\Gamma_k \in P$ for the given constraints. This can done by either performing an exhaustive search or a tree search, since the sequences of $\Gamma_1, \Gamma_2, \ldots, \Gamma_{L-1}$ can be represented by a tree, where every node in the tree represents a unique partition, since e.g. $(\Gamma_1, \Gamma_2) = (\Gamma_1, \Gamma_2, 0)$. The complexity BC for some channels of various lengths for the 8PSK alphabet are shown in table 1, using the VA and the SA(B,C) resulting in AO.

Tab. 1: The complexity for partitions resulting in AO for 8PSK.

$F(z)$	S	$1 \cdot C[3]$	$2 \cdot C$	$B \cdot 1$
$1 + z^{-1}$	8	2	2	2
$(1 + z^{-1})^2$	64	16	8	6
$(1 + z^{-1})^3$	512	64	32	9
$(1 + z^{-1})^4$	4096	128	32	12

[1] This work was supported by TFR under Grant 96-396.

References

[1] T. Aulin, "Breadth first maximum likelihood sequence detection: Basics," *IEEE Trans. Commun.*, vol. COM-47, pp. 208-216, Feb. 1999.

[2] G. D. Forney, "Maximum-likelihood sequence estimation of digital sequences in the presence of intersymbol interference," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 363-378, May 1972.

[3] T. Larsson, *A State-Space Partitioning Approach to Trellis Decoding*. Technical Report No. 222, Ph.D. thesis, Chalmers University of Technology, 1991.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Modeling of the LAN Traffic Microstructure Based on the Class A Noise Model

X.S. Yang, A.P. Petropulu[1]
ECE Dept., Drexel University
Philadelphia, PA 19104, USA
yxs,athina@ece.drexel.edu

David Middleton
127 E. 91st Street, New York,
NY 10128-1601, USA

Abstract — **We propose to model the packets activity of single IP address by the Middleton class A noise model. Theoretical results and numerical simulations indicate that the class A noise model captures well the inter-arrival properties of packets, especially in terms of long-range dependence (LRD), which is widely observed in computer network traffic.**

In this paper we consider the micro-structure of Local Area Network (LAN) traffic, that is, the single user network traffic up to the packet level. An accurate model for traffic is a valuable tool in queuing theory studies.

Recent results based on high-definition network traffic records suggest that high-speed data networks traffic exhibits LRD. Network traffic models can be divided into two categories. The first category considers the macro-structure of traffic. In this class, the mathematical models are fitted to the network traffic statistics, without considering the detail data stream structure. Examples include the fluid flow model, and the fractal On/Off models. In the second category, the network traffic is viewed as a point processes that models the data stream at the packet level. Various Markov-modulated Poisson processes belong to this category. We refer this kind of modeling as micro-structure modeling. The proposed model belongs to the second class.

Our statistical model is based on standard renewal processes (SRP). A SRP is characterized by the characteristics of the inter-events distribution. The events are the arriving packets in the network pipeline. The inter-event times are independent random variables drawn from Middleton's class A noise envelope. The motivation to investigate that kind of model in the context of LAN traffic came from the distinctive appearance of graphs corresponding to traffic data, and in particular, time intervals between packet arrivals. (see Fig.1) We were able to show analytically that, such a model results in a process with LRD, thus capturing the essential characteristic of real traffic. In the sequel, we outlined the proof of the main result of the paper, that is, a standard renewal processes with inter-event times modeled as class A noise envelope exhibits LRD. By LRD, we here refer to the definition proposed in [1], according to which the power spectrum density of the process, if it exists, can be approximated by a power-law function.

The *pdf* of class A noise envelop equals

$$w_1(\epsilon)_A \cong e^{-A_A} \sum_{m=0}^{\infty} \frac{{A_A}^m \epsilon e^{-\epsilon^2/2\hat{\sigma}^2_{mA}}}{m!{\sigma_{mA}}^2}, \quad 0 \le \epsilon < \infty \qquad (1)$$

Here, ϵ, ϵ_0 are normalized envelopes The parameters $(A_A, \Gamma_A', \Omega_{2A})$ are called *global parameters*. In practice, they all have physical meaning.

Let

$$\begin{cases} Z_i = \sum_{m=0}^{\infty} \frac{{A_A}^m \hat{\sigma}_{mA} e^{-\frac{1}{2}\hat{\sigma}^2_{mA}\omega^2}}{m!} \mathrm{Erfi}\left[\frac{\hat{\sigma}_{mA}\omega}{\sqrt{2}}\right] \\ Z_q = \sum_{m=0}^{\infty} \frac{{A_A}^m \hat{\sigma}_{mA} e^{-\frac{1}{2}\hat{\sigma}^2_{mA}\omega^2}}{m!} \end{cases}, \qquad (2)$$

the power spectrum of the SRP becomes:

$$S_N(\omega) = \mu^2\delta(\omega/2\pi) + \frac{2\sqrt{2}Z_i}{\sqrt{\pi}e^{A_A}\omega(Z_i^2 + Z_q^2)} - 1 \qquad (3)$$

where μ is the inverse of the class A noise envelop mean value.

Although the power spectrum density cannot be obtained in closed form, it can be numerically established that for small ω's (around unit frequency) the power spectrum density behaves like a power law function. When using Middleton's class A noise to model inter-packet times, we will need the non-normalized version of the model. The above presented results can be easily extended to the scaled version. The estimation of class A model parameters from real data is discussed in, for example [2].

Based on extensive studies involving real network traffic data, not included here due lack of space, it appears that the class A noise model can capture well the packet level activity of a single user in a local area high speed network. Given the adjustable class A noise parameters, one can synthesize the desired network traffic load traces, which have the same characteristics as real world traffic data.

[1]This work was supported by NSF under grant MIP-9553227.

References

[1] D. R. Cox and P. A. W. Lewis, *The Statistical Analysis of Series of Events*, London: Methuen, 1966.

[2] D. Middleton, "Procedure for Determining the Parameters of the First-Order Canonical Models of Class A and Class B Electromagnetic Interference", *IEEE Transactions on Electromagnetic Compatibility*, Vol. EMC-21, Aug. 1979.

[3] D. Middleton, "Non-Gaussian Noise Models in Signal Processing for Telecommunications: New Methods and Results for Class A and Class B Noise Models", *IEEE Transactions on Information Theory*, Vol.45, No.4, May 1999.

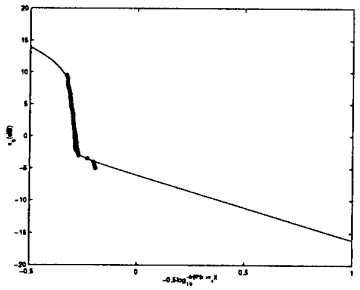


Figure 1: Inter-packet distribution [prob($t > t_0$)] obtained from single user qin.ece.drexel.edu, comparing with Middleton class A noise, with parameters $A_A = 0.02$ and $\Gamma_A' = 0.03$. X-axis is by $-0.5\log(-\log[])$, Y-axis is by $10\log[]$, i.e. dB.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Statistical Multiplexing of Many Independent ATM-Streams with Temporally Constrained Long-Range Dependence

Sándor Csibi[1]
Dept. of Telecommunications
Budapest Univ. of Technology and
Economics
Stoczek u. 2
H-1111 Budapest
Hungary
e-mail: csibi@hit.bme.hu

Abstract — **The broader design possibilities for statistical multiplexing are of our interest provided the *ATM* streams to be merged are not just independent but also many.**

I. Introduction and Notations

Statistical multiplexing of n independent input streams each of line rate r and mean activity m is considered, each being long range dependent at the same extent. Slotwise cyclic scanning of the input streams is assumed at a rate nr, and a single common output stream of line rate $R = lr < nr$. ($\lambda := \frac{l}{n} < 1$.) For fairness a single cyclic shift per scanning cycle of the stream scanned initially is assumed.

Upper and lower bounds are given on the total probability p_T of overflow (of cells from any stream, Theorem 1, [1]) for any scanning cycle initiating an *isolated* burst of overflowing cells only. (For *isolated* see [1].) The impact of merging many streams is investigated for multiplexing by scanning, and doing nothing else (Version (ii)), and for multiplexing as usual, including also a leaky bucket of length $\tilde{l}$ next to scanning (Version (i)). Instead of investigating the relation between the long range dependence at the input and the burst length at the output, a broad class of appropriate Pareto-kind template distributions of overflowing cells are considered. A member of this class is chosen in a best way (in a sense defined in [1]) to overbound the probability estimate that the burst length of lost cells is exceeded. (For such an estimate observations should be available on the cells stored in the course of each scanning.)

II. Main Results

Given $p_T < 1$, a pair of m and λ jointly admissible, denote by $n_0(p_T)$ the least admissible number of the input streams n, from which upwards the total probability of any scanning cycle, intitiating an *isolated* burst of overflowing cells, does not exceed p_T. From Theorem 1 ([1]) follows:

$$n_{LB}(p_T) < n_0(p_T) < n_{UB}(p_T).$$

Here $n_{UB}(p_T) := \lceil u \rceil$. u stands for a positive real, being the solution of the following equation:

$$\lg p_T^{-1} = u\,(\mathbf{D}(\mathcal{P} \,||\, \mathcal{Q}) - \epsilon_S(u) - \epsilon_{LB}(u)).$$

The the relative entropy underlying our present model is denoted by

$$\mathbf{D}(\mathcal{P} \,||\, \mathcal{Q}) = \lambda\frac{\lambda}{m} + (1-\lambda)\frac{(1-\lambda)}{(1-m)}.$$

$\mathcal{P} := (\lambda, 1-\lambda)$, and $\mathcal{Q} := (m, 1-m)$ are the underlying binary probability distributions. $\epsilon_s(n)$, $\epsilon_{LB}(n)$ and $\epsilon_{UB}(n)$ are positive, each decreasing with increasing n and approaching 0 as $n \to \infty$ (each precisely given in [1]). $\lg x$ stands for the logarithm of $x > 0$ of base 10. For $n_{LB}(p_T) \geq 0$ see [1]. For the probability p per input stream, corresponding to p_T, the following equation holds: $p = \frac{m}{n} p_T$ (Proposition 2, [1]). For Version (i) the following upper bound is given on the total probability $\tilde{p}_T$ of ATM cell loss due to leaky bucket saturation, provided experience on the cell bursts is available (Proposition 4 [1]):

$$\tilde{p}_T < p_T\, \bar{p}_{TUB}(\tilde{l}).$$

$\bar{p}_{TUB}(\tilde{l})$ stands for the upper bound on the total conditional probability estimate of cell loss, given event Θ, estimated by a member of the Pareto-kind distribution class, selected according to Section I. Θ occurs if the just considered scanning cycle is initiating an *isolated* burst of overflowing cells. The probability of cell loss $\tilde{p}$ per stream is related, under a realistic assumption, to $\tilde{p}_T$ as p to p_T (Proposition 5, [1]). Let $n = 2^\nu$ ($\nu = 1, 2, \ldots$). Denote by γ the at most admitted per stream probability and by γ_T that of the the total probability of the cell loss. Let $\gamma = 10^{-9}$, and $\gamma_T = 10^{-7}$ (assuming $n \geq 100$). Then the least number of input streams still admitted is $n = 2^8 > n_{UB}$ for $p_T \leq \gamma_T = 10^{-7}$, for a design with scanning only. However, even $n = 2^7$ might be admissible, even with $p_T = 10^{-4} < \gamma_T$, for a design with a leaky bucket next to scanning. This might be so if (i) not only the estimate on the conditional probability (given Θ) of the cell loss due to bucket saturation can be overbounded by $\bar{p}_{TUB}(\tilde{l}) < 10^{-3}$, but (ii) the upper bound can also be tolerated on the conditional probability estimate (given Θ) that a still tolerable burst length of cells, lost during bucket saturation, is exceeded. Single- and bi-variate large deviation relations are considered for finite many terms in Theorem 1 and Proposition 4. Obviously a study in finite terms is indispensible for estimating $n_0(p_T)$. One might expect, under two realistic assummptions, Version (i) to offer, even for $n \geq n_{UB}(\gamma_T)$, more room for bearing long-range dependence. (For background references and acknowledgements, and for notions, assumptions, and all proofs see [1].)

[1]This work was supported in part by the European Copernicus Project No. COP579 (1995-1999), the Hungarian Telcomm. Foundation, Grant No. 109 (1999), and a research professor visit of the author, at the CATSS, UTDallas, TX, USA, Feb/March 1999.

References

[1] S. Cs., *Prepint* under the same title.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Delay analysis for prioritized service of variable rate regenerative traffic sources

Michael Shalmon

ABSTRACT NOT AVAILABLE AT THE TIME OF PRINT

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Scheduling for Fair Allocation of Rates in Multirate Multicast Networks

Saswati Sarkar and *Leandros Tassiulas*
Dept. of Electrical and Computer Engineering and Institute for Systems Research
University of Maryland, College Park, MD, USA
email addresses: swati@eng.umd.edu, leandros@isr.umd.edu

I. Extended Summary

We study fair allocation of service rates for real time loss tolerant traffic in arbitrary networks with multicast capabilities. Multicasting poses some specific fairness challenges. The fairness objective is that every receiver receives service at a rate commensurate with its capability and the capacity of the path from the source. Hence, different receivers should receive information at different rates. The source encodes the signal into several layers that can be incrementally combined to provide progressive refinement. Every receiver must receive the most significant layer (layer 1) for basic information. If a receiver has additional bandwidth, it can subscribe to other layers for better reception quality. A layer carries meaningful information, only when all the more significant layers have been successfully decoded. Thus the objective is to provide fair rates of service to the receivers, and to limit the packet losses to the less significant layers.

We have previously proposed distributed algorithms for computing the fair rate allocation[1]. Once the fair rates are known, many congestion control policies such as fair queueing can be used to attain the computed rates. However, rate computation requires the exact knowledge of system parameters, such as link bandwidths. In general, the schedulers at the nodes may not have exact knowledge of this link capacity. It is also necessary to exchange messages between neighboring nodes. This increases information overhead. We propose a scheduling policy which attains the maxmin fair rates without computing them beforehand. In addition to guaranteeing fairness, this policy confines packet losses to less significant layers, and protects the more important layers, when there is shortage of bandwidth. Furthermore, this policy does not require any knowledge of traffic statistics, is computationally simple, and is essentially local information based.

II. Scheduling Policy

We propose a scheduling policy based on prioritized round robin with window flow control for multirate multicast networks. Let session i traverse through link l. Then, the "logical buffers" $B_{(i,k,l)}(t)$ denotes the number of layer k packets of session i waiting for transmission in link l at time t. Logical buffers $B_{(i,k,l)}(t)$s are monitored at each node, for every session i traversing the node (Figure 1). A window parameter (W) is associated with the policy.

All sessions traversing a link are sampled in round robin order. Consider a session i traversing link l. When session i is sampled, it first tries to send a packet of the most significant layer (layer 1). If it does not succeed, it tries to send the second most significant layer packet (layer 2), and so on. If all layers of session i are exhausted, the scheduler switches to the next session in the round robin order. Let $\tau_i(l)$ be the set of links originating from the destination of link l that lie on the path of session i. A $k-$layer packet of session i will be successfully transmitted at time t if

1. no session i packet from layers $1, \ldots, k-1$, can be transmitted,
2. a $k-$layer session i packet is waiting at the source node of the link, for transmission in the link ($B_{(i,k,l)}(t) > 0$) and
3. at least one of the logical buffers for the kth layer of session i at the destination node of the link has less than W packets (i.e., $\min_{l' \in \tau_i(l)} B_{(i,k,l')}(t) < W$).

Refer to figure 1 for an illustrative example. We have proved that for all sufficiently large window and physical buffer sizes, this policy allocates the maxmin fair rates to all receivers of all sessions. Note that congestion related packet loss is possible at any node. The policy offers an inherent priority to more significant layers of a session at every node. Thus the presence of less significant layers is transparent to more significant layers. In fact we have shown analytically that the more significant layers suffer negligible packet loss, and the packet losses are confined to the least significant layer served.

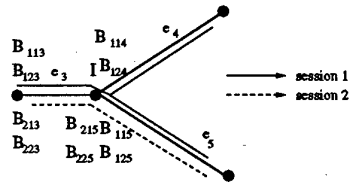


Fig. 1. Each session transmits two layers only. We show the logical buffers associated with source and destination of link e_3. For example, B_{124} consists of session 1 layer 2 packets waiting for transmission in link e_4. Consider the scheduling of link e_3. Here, $\tau_1(e_3) = \{e_4, e_5\}$ and $\tau_2(e_3) = \{e_5\}$. Session 1 and 2 are sampled in round robin order. When session 1 is sampled, it sends the most significant layer (layer 1) packet, if $B_{113}(t) > 0$, and $\min(B_{114}(t), B_{115}(t)) < W$. Otherwise, it tries to send a layer 2 packet. It sends a layer 2 packet if $B_{123}(t) > 0$, and $\min(B_{124}(t), B_{125}(t)) < W$. If it can not send a layer 2 packet, it passes its chance to session 2. Now session 2 tries to send a lowest layer packet first, and so on. Let $W = 5$, $B_{113}(t) = 2$, $B_{123}(t) = 1$, $B_{114}(t) = 5$, $B_{124}(t) = 2$, $B_{115}(t) = 7$, $B_{125}(t) = 6$. In this case, session 1 is not able to transmit a layer 1 packet. However, session 1 transmits a layer 2 packet.

References

[1] S. Sarkar and L. Tassiulas: Distributed Algorithms for Computation of Fair Rates in Multirate Multicast Trees *Proceedings of IEEE INFOCOM'* 2000, Tel Aviv, Israel, March' 2000

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Optimal Group-theoretic Methods for Selective Motion Analysis: Detection, Estimation, Filtering and Reconstruction with Continuous and Discrete Spatio-Temporal Wavelets

Jean-Pierre Leduc[1]
Washington University in Saint
Louis, Department of Mathematics,
One Brookings Drive, Campus Box
1146, Saint Louis, MO 63130
Email : leduc@math.wustl.edu

Abstract — **This work addresses the analysis of motion embedded in spatio-temporal digital signals as well as motion taking place in the outer space $\mathbb{R}^3 \times \mathbb{R}$. Three categories of motion are considered and referred to as translational, rotational or deformational. In each category, motion parameters are defined from all the temporal derivatives i.e. position, velocity and accelerations. Motion analysis means not only detection, estimation, interpolation, and tracking but also motion-compensated filtering, signal decomposition, and selective reconstruction. In this context, we show how all motion models can be derived from Lie groups and how group representations define continuous wavelets in the functional space of the signals. Motion detection, estimation and interpolation are based on continuous wavelet transforms. Selective motion tracking is based on the adjunction of a variational principle of optimality. The optimality principle defines the trajectory or the geodesic and provides the appropriate PDE of wavelet motion, the tracking equation (ODE), the selective constants of motion to be tracked, and all the symmetries to be imposed on the system. The Green functions of these PDE's give rise to the converse operators i.e. wavelet propagators and kernels of integral equations. These integral equations have several applications: (1). put a still wavelet on a trajectory to perform velocity or motion-oriented filtering, (2). achieve the motion compensation of a signal. This work investigates in fact the harmonic analysis associated with motion groups which leads to special functions, spectral signatures, propagators and yields motion-based detection and velocity or motion-oriented filtering. This motion analysis fits to both deterministic and stochastic processes. Eventually, spatio-temporal discrete wavelets can be derived from their continuous cognates as the orthonormal bases that perform signal decompositions along the trajectory and achieve selective reconstructions of moving patterns of interest.**

I. Motion Models and Assumptions

The entire construction for this signal analysis lies on defining a Lie group or a Lie algebra of transformation and an Euler-Lagrange equation. In short, three assumption have to be given as a law of composition and its inverse and a principle of optimality from calculus of variations. For each class of motion transformations, we consider the parameters of position, velocity and accelerations. For translational motion, the spatial position, velocity and accelerations are considered along with the temporal translation. For (circular) rotational motion in two-dimensional space, the parameters of angular position, velocity and accelerations will be denoted in the order of the Taylor expansion $\theta_i \in \mathbb{R};\ i \in \mathbb{Z}^+$. A variant of circular rotation is hyperbolic rotation which is denoted by ϕ_i instead of θ_i. The rotations are expressed through unitary matrices of transformation namely $R(\theta_i\tau^i) = \begin{pmatrix} cos(\theta_i\tau^i) & -sin(\theta_i\tau^i) \\ sin(\theta_i\tau^i) & cos(\theta_i\tau^i) \end{pmatrix}$ with the $x_1^2 + x_2^2$-invariance for circular rotations. For deformational transformation, the parameters of velocity and accelerations will be taken into account. The zero-order deformation is the most important. This is the scale which provides multiresolution analyses on space and time respectively. The matrix of deformation is defined as $\mathcal{A} = \begin{pmatrix} e^{a_i\tau^i} & 0 \\ 0 & e^{a_i\tau^i} \end{pmatrix}$ in $\mathbb{R}^2$. In case of general transformations taking place in $\mathbb{R}^n$ on homogeneous surfaces (spheres, hyperboloids) or on smooth manifolds, the scale parameter becomes a matrix A. These transformations rely on groups within $GL(m, \mathbb{R})$.

[1]This research work is supported by the AFOSR grant No. F49620-99-1-0068

References

[1] M. Kong, J.-P. Leduc, B. Ghosh, J. Corbett, V. Wickerhauser, "Wavelet based Analysis of Rotational Motion in Digital Image Sequences", *ICASSP-98, May 12-15, 1998, pp. 2781-2784.*

[2] J.-P. Leduc, F. Mujica, R. Murenzi, M. J. S. Smith, "Spatio-Temporal Wavelet Transforms for motion tracking", *ICASSP-97, Munich, 20-24 April 1997, Vol. 4, pp. 3013-3017.*

[3] J.-P. Leduc, J. Corbett, M. Kong, V. M. Wickerhauser, B. K. Ghosh, "Accelerated Spatio-temporal Wavelet Transforms: an Iterative Trajectory Estimation", *IEEE ICASSP, Vol. 5, 1998, pp. 2777-2780.*

[4] J.-P. Leduc, J.-M. Odobez and C. Labit, "Adaptive Motion-Compensated Wavelet Filtering for Image Sequence Coding", *IEEE Transactions on Image processing, Vol. 6, No. 6, pp. 862-878, June 1997.*

[5] J.-P. Leduc and J. Corbett, "Spatio-Temporal Continuous Wavelets for the Analysis of Motion on Manifolds", *IEEE-SP International Symposium on Time-Frequency and Time-Scale Analysis, Pittsburgh, October 6-9, 1998, pp. 57-60.*

[6] J.-P. Leduc, F. Mujica, R. Murenzi, and M. Smith, "Spatio-Temporal Wavelets: a Group-Theoretic Construction for Motion Estimation and Tracking", *to appear in SIAM Journal of Applied Mathematics.*

[7] F. Mujica, J.-P. Leduc, R. Murenzi, M. Smith, "A New Parameter Estimation Algorithm Based on the Continuous Wavelet Transform", *to appear in IEEE Trans. on Image Processing.*

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Channel Quality Estimation with Channel Error Counts for Adaptive Signaling in Wireless Communications

Michael B. Pursley[1]
Electrical and Computer Engineering
Clemson University
303 Fluor Daniel EIB
Clemson, SC 29634-0915
e-mail: pursley@eng.clemson.edu

John M. Shea
Electrical and Computer Engineering
University of Florida
439 ENG Bldg. #33, PO Box 116130
Gainesville, FL 32611-6130
e-mail: jshea@ece.ufl.edu

Abstract — **Accurate channel-quality estimates are needed for a variety of reasons in wireless communication systems, such as for power control and for adaptive transmission and routing. Channel-quality information can be derived from many sources at the receiver, including statistical characterizations of the channel, information from the demodulation process, and information from the error-correcting and error-detecting codes. One simple method for estimating the channel-quality is to estimate the channel error rate by re-encoding the outputs of the error-correcting code and comparing the re-encoded symbols to hard decisions at the demodulator output. In the presentation, we will present analysis and simulation results for several different channel quality estimates derived from estimates of the channel error rate.**

I. Introduction

In this paper we consider channel quality estimates based on estimates of the channel error rate. An estimate of the channel error rate for a system employing error-correcting codes can be determined from comparing hard-decision outputs of the demodulator to re-encoded symbols from the output of the decoder [1],[2]. We consider the performance of such estimates for convolutionally encoded data transmitted with binary phase-shift-keying. Consider a system that uses binary transmission over an additive white Gaussian noise channel. The information to be transmitted is convolutionally encoded and transmitted in blocks of N bits. The channel causes $B \geq 0$ channel symbol errors to occur, as measured by hard-decisions at the output of the demodulator. The receiver re-encodes the output of a Viterbi decoder and compares it to hard-decisions at the output of the demodulator. The number of differences between these encoded streams is labeled B' and is an estimate of B, and thus can be used to estimate the channel error rate. If no errors occur at the output of a Viterbi decoder, $B' = B$. If errors do occur at the output of the decoder, $B' \neq B$, and B' may not give an accurate count of the number of channel symbol errors that occurred. The probability of a block having multiple event errors is much higher for systems that employ adaptive transmission techniques or have highly dynamic channels than for other systems. For many systems, additional information is available to determine whether the output of the Viterbi decoder is in error. For instance, error-detecting codes are often necessary to validate that the received block is correct. This additional information can be used to improve the accuracy of the error counts.

The number of bit errors that occur in a block can be used to generate several different estimates of channel quality, including estimates of the channel error rate, estimates of the signal-to-noise ratio, or other estimates. In this summary, we consider estimates for the bit energy-to-noise density ratio based on error counts from comparing the re-encoded outputs of a Viterbi decoder to hard-decision outputs of the demodulator. The estimates also employ knowledge from an error-detecting code about whether the block was successfully decoded. The estimates of the bit energy-to-noise density ratio that we consider are of the form $\mathcal{E} = f(b)$, where b denotes the counted number of differences between the hard decision demodulator outputs and the re-encoded decoder outputs for a packet. For instance, for the *maximum a posteriori* (MAP) estimate,

$$\mathcal{E}_{MAP} = \underset{e}{\text{argmax}}\, P(\varepsilon = e \,|B' = b).$$

For the minimum mean-square error (MMSE) estimate,

$$\mathcal{E}_{MMSE} = E\{\varepsilon \,|B' = b\}.$$

We use several analytical techniques to determine approximations for these estimates. For instance, it is intractable to consider all of the possible multiple-event errors, so we use the approach taken in the analysis of turbo codes and determine a weight profile for the equivalent block code [3]. Our approach also requires the the probability that an event error occurs given that a certain number of the decision statistics are in error. This involves calculating the probability that a sum of non-Gaussian decision statistics is less than zero. Our approach is to use a Gaussian approximation for the sum, and simulations show that this approximation provides sufficient accuracy for many cases.

II. Conclusions

In the presentation, we will present results for channel quality estimates derived from error counts from re-encoding the output of an error-correcting decoder. We consider estimates that also employ information from an error-detecting code that provides information about whether the packet decoded correctly. A framework for analyzing the accuracy of such estimators for convolutionally encoded data is derived, and results are presented that illustrate the accuracy of several different types of estimators for different channels. Our results indicate that for the minimum mean-square estimate of the signal-to-noise ratio, channel error counts of the type discussed in this paper yield mean squared errors in the 0.5 dB to 2.5 dB range depending on the range and distribution of the actual signal-to-noise ratios. We will also illustrate the performance of these estimates for some example adaptive signaling schemes.

References

[1] C. D. Frank and M. B. Pursley, "Concatenated coding alternatives for frequency-hop packet radio," *IEICE Trans. Commun.*, vol. E76-B, pp. 863–873, Aug. 1993.

[2] S. Souissi and S. B. Wicker, "Diversity combining DS/CDMA system with convolutional encoding and Viterbi decoding," *IEEE Trans. Vehic. Technol.*, vol. 44, pp. 304–312, May 1995.

[3] S. Benedetto and G. Montorsi, "Unveiling turbo codes: Some results on parallel concatenated coding schemes," *IEEE Trans. Inform. Theory*, vol. 42, pp. 409–428, Mar. 1996.

[1]This research was supported by the U.S. Army Research Office under grants DAAH04-95-1-0247 and DAAG55-98-1-0013.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Least Mean-Squared Error Polynomial Estimation in Systems with Uncertain Observations [1]

Raquel Caballero-Águila
Dpto. Estadística e I. O.
Universidad de Jaén
Paraje Las Lagunillas, s/n
23071 Jaén, Spain
e-mail: raguila@ujaen.es

Aurora Hermoso-Carazo
Dpto. Estadística e I. O.
Universidad de Granada
Campus Fuentenueva, s/n
18071 Granada, Spain
e-mail: ahermoso@ugr.es

Josefa Linares-Pérez
Dpto. Estadística e I. O.
Universidad de Granada
Campus Fuentenueva, s/n
18071 Granada, Spain
e-mail: jlinares@ugr.es

Abstract — **In this paper, we consider a kind of discrete-time linear systems with uncertain observations, in which the additive noises of the state and observation equations are correlated with each other. By using the Orthogonal Projection Theorem, a recursive algorithm to obtain the least mean-squared error polynomial estimator for the state of these systems is proposed.**

I. Introduction

In the estimation theory developed by Kalman, it is assumed that, at any time, the signal to be estimated is contained in the observations. However, in many practical situations, such as communication systems, there may be a nonzero probability (false alarm probability) that any observation consists of noise alone; this may be caused by an intermittent failure in the observation mechanisms.

These situations are described by a system whose observation equation includes not only an additive noise, but also a multiplicative noise component, modelled by a sequence of Bernoulli random variables. These systems have been investigated under the topic of *Systems with Uncertain Observations*. In these systems, even if the noises are gaussian, the conditional expectation is not a linear function of the observations and it requires an exponentially growing memory for its computation (Jaffer and Gupta [2]). Consequently, for this class of systems, attention has been directed to suboptimal estimators.

The linear estimation problem in systems with uncertain observations, when the interruption process is a binary independent sequence, was treated by Nahi [4]. Later on, Hermoso and Linares [3] extended the results of Nahi for the case when the state and measurement noises are correlated at consecutive instants of time.

More recently, García-Ligero et al. [1] have studied the quadratic estimation problem in systems with uncertain observations under the hypothesis of mutual independence of the noise and the initial state.

In this paper we consider systems with uncertain observations when the additive noises of the state and the observation are correlated at the same instant of time. At an earlier stage, we proposed to approach the linear estimation problem in these systems, which still had not been studied, to subsequently obtain estimators which improved the linear one. Finally, we have approached the least mean-squared error polynomial estimation problem in these systems as a whole.

[1]This work has been supported by the "Comisión Interministerial de Ciencia y Tecnología" under contract PB98-1286.

This study generalizes the work of García-Ligero et al. [1] in two directions: on the one hand, the independence hypothesis of the noises is weakened and, on the other hand, polynomial estimators of an arbitrary order ν ($\nu \geq 1$) are considered.

II. Polynomial Estimation Problem

In order to approach the aforementioned optimal νth-order polynomial estimation problem, we define a new system (*augmented system*), whose state and observation vectors are obtained as the aggregate of the original vectors and their Kronecker powers up to the νth-order. Thus the least mean-squared error linear estimator of the augmented state based on the augmented observations provides the optimal polynomial estimator for the state of the original system.

Then the problem is reduced to obtain the least mean-squared error linear estimator for the state of the augmented system. This system has uncertain observations, and the state and observation noises are correlated with each other. Hence, the recursive algorithms proposed by Nahi [4] and Hermoso and Linares [3] cannot be applied since the augmented system does not satisfy the required conditions for their application.

By using the Orthogonal Projection Theorem, a recursive algorithm to obtain the optimal linear estimator for the state of the augmented system is proposed. This algorithm, that generalizes the Nahi algorithm, sets up recursive equations which allow us to obtain the linear filter as a function of the linear predictor and reciprocally. It should also be noted that the computation of the error covariance matrices is independent of the estimators computation. This allows us to quantify the goodness of the estimation without having to calculate the estimators explicitly.

Finally, as we have indicated above, the optimal polynomial estimator for the state of the original system is obtained from optimal linear estimator for the state of the augmented system.

References

[1] M. J. García-Ligero, A. Hermoso and J. Linares, "Second Order Polynomial Filtering for Discrete Systems with Uncertain Observation", *VIII International Symposium on Applied Stochastic Models and Data Analysis*, pp. 157–162, 1997.

[2] A. G. Jaffer and S. C. Gupta, "Recursive Bayesian Estimation with Uncertain Observation", *IEEE Transactions on Information Theory*, vol. IT-17, pp. 614–616, 1971.

[3] A. Hermoso and J. Linares, "Linear Estimation for Discrete-Time Systems in the Presence of Time-Correlated Disturbances and Uncertain Observations", *IEEE Transactions on Automatic Control*, vol. AC-39, no. 8, pp. 1636–1638, 1994.

[4] N. E. Nahi, "Optimal Recursive Estimation with Uncertain Observation", *IEEE Transactions on Information Theory* vol. IT-15, no. 4, pp. 457–462, 1969.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Asymptotics of the Bayesian Estimator of Hidden Markov Models

Laurent Mevel
IRISA/INRIA
Campus de Beaulieu
35042 Rennes Cedex, France
e-mail: lmevel@irisa.fr

Lorenzo Finesso
LADSEB-CNR
Corso Stati Uniti, 4
35127 Padova, Italy
e-mail: finesso@ladseb.pd.cnr.it

Abstract — **We study the asymptotic behavior of the Bayesian estimator of the parameters of a Hidden Markov Model (HMM) with continuous or finite observations and finite state space.**

I. Introduction

Maximum Likelihood (ML) is still the most popular approach to parameter estimation for HMM's. The established technique for the computation of the ML is the use of an algorithm of the EM type, which has poor convergence properties and is computationally expensive. In this paper we consider the optimal mean square (Bayesian) estimator as a possible alternative to ML. We study the asymptotic properties of the Bayesian estimator and prove its consistency under standard hypotheses of identifiability of the model class and of positivity of the prior probability. We briefly consider the algorithmic aspects and provide an explicit formula for the case of finitely valued observations. Whether Bayesian estimators constitute, from the computational point of view, a viable alternative to ML is a question that still has to be settled.

II. Statistical Model

Let $\{X_n\,,\, n \geq 0\}$ and $\{Y_n\,,\, n \geq 0\}$ be two sequences, defined on a probability space $(\Omega, \mathcal{F}, \mathbf{P})$, with values in the finite set $S = \{1, \cdots, N\}$ and $\mathbf{R}^d$ respectively. The statistical model is a parametric class of HMM's defined as follows. On the space $(\Omega, \mathcal{F})$ we consider a family $(\mathbf{P}^\theta\,,\, \theta \in \Theta)$ of probability measures, with Θ compact subset of $\mathbf{R}^p$, such that under $\mathbf{P}^\theta$ the unobserved (hidden) state sequence X_n is a Markov chain with transition probability matrix (t.p.m.) $Q^\theta = (q^\theta_{i,j})$, i.e. $q^\theta_{i,j} = \mathbf{P}^\theta[X_{n+1} = j \mid X_n = i]$, and initial probability distribution $\pi_0 = (\pi^i_0)$ independent of $\theta \in \Theta$, and possibly different from the *true* probability distribution π of X_0. The observations Y_n are mutually independent given the sequence of states, i.e. $\mathbf{P}^\theta[Y_n \in dy_n..Y_0 \in dy_0 \mid X_0 = i_0, ..X_n = i_n] = \prod_{k=0}^n \mathbf{P}^\theta[Y_k \in dy_k \mid X_k = i_k]$. We assume, moreover, that the model set contains $\mathbf{P}$, the *true* measure, i.e. that there exists $\alpha \in \Theta$ such that $\mathbf{P} = \mathbf{P}^\alpha$.

III. Bayesian Estimation

In the Bayesian approach to estimation a prior distribution, with density say $\nu(\cdot)$, is assigned on the parameter space Θ. The Bayesian (optimal m.s.e.) estimator is given by $\widehat{\theta}^B_n = E[\theta|Y^n]$ where the expectation is computed with respect to the posterior density $p(\theta|Y^n)$. Our main theorem generalizes to HMM's a classical result on the asymptotic behavior of the posterior density [4]. Let us define $\ell(\theta) \stackrel{\Delta}{=} \lim \frac{1}{n+1} \log p^\theta(y^n_0)$.

Theorem *If $\ell(\cdot)$ has a unique maximum at α, and if the prior density $\nu(\cdot) > 0$ everywhere then*

$$\widehat{\theta}^B_n \to \alpha\,, \quad \mathbf{P}^\alpha\text{-}a.s.$$

The proof is an application of the Laplace expansion technique, and requires the development of a uniform version of the Shannon-McMillan-Breiman Theorem for HMM's, which is of independent interest. Heuristically one can observe that, for any $\varepsilon > 0$, asymptotically the estimator $\widehat{\theta}^B_n$ is well approximated by

$$\frac{\int \theta \exp n(\ell(\theta) + \epsilon)\nu(\theta)d\theta}{\int \exp n(\ell(\theta) + \epsilon)\nu(\theta)d\theta}.$$

The limit for $n \to \infty$ can be identified using the Laplace asymptotic expansion of the integrals. The assumption that $\ell(\theta)$ has a unique maximum at α (identifiability assumption), allows us to conclude that $\widehat{\theta}^B_n$ is consistent. The technical results on which the proof is based can be found in [1], [2], [3].

IV. Explicit Form of the Estimator

A more explicit expression of the Bayesian estimator can be given, properly choosing the prior density $\nu(\cdot)$. In the special case of finitely valued observations and parameter θ coinciding with the t.p.m. Q^θ of X_n, one can adopt the Dirichlet prior [5], $\nu_D(\theta) \stackrel{\Delta}{=} \prod_i \left[\frac{\Gamma(k/2)}{\Gamma(1/2)^k} \prod_j q_{ij}^{-\frac{1}{2}}\right]$, where $\Gamma(\cdot)$ denotes the Gamma function. A long but straightforward algebraic manipulation gives

Lemma *The estimator $\widehat{\theta}^B_n$ corresponding to $\nu_D(\theta)$ is given, componentwise, by*

$$E[q_{ij}|Y^n_1] = E_Q\left[\frac{N_{ij}(X^n_1) + 1/2}{N_i(X^n_1) + k/2} \mid Y^n_1\right]$$

where $Q(X^n_1, Y^n_1)$ is the a-posteriori *measure, i.e.*

$$Q(X^n_1, Y^n_1) = \int P_\theta(X^n_1, Y^n_1)\nu_D(\theta)d\theta.$$

and $N_{ij}(X^n_1)$ denotes the number of transitions $i \to j$ in X^n_1.

References

[1] Le Gland F., Mevel L. *Asymptotic behaviour of the MLE in hidden Markov models.* Proc. 4th European Control Conference, Bruxelles, Belgium, Paper FRA–F6, 1997.

[2] Le Gland F. and Mevel L. *Exponential forgetting and geometric ergodicity in HMM's.* To appear in MCSS

[3] Mevel L. *Statistique asymptotique pour les modèles de Markov cachés.* Thèse de Doctorat, Université de Rennes 1, 1997.

[4] Berk R.H. *Consistency a posteriori.* Annals of Math. Stat., Vol.41, pp.894-906, 1970.

[5] Finesso L., Liu C.C. and Narayan P. *The optimal error exponent for Markov order estimation.* IEEE Trans. Information Theory, Vol.42, pp.1488–1497, 1996.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

A class of Sudan-decodable codes

R. Refslund Nielsen
Dep. of Mathematics, Bldg. 303
Technical University of Denmark
DK-2800 Lyngby, Denmark
e-mail: r.r.nielsen@mat.dtu.dk

Abstract — **In this paper Sudan's algorithm is modified into an efficient method to list-decode a class of codes which can be seen as a generalization of Reed-Solomon codes. The algorithm is specialized into a very efficient method for unique decoding. The code construction can be generalized based on algebraic-geometry codes and the decoding algorithms are generalized accordingly. Comparisons with Reed-Solomon and Hermitian codes are made.**

I. Introduction

The minimum distance is not the only measure of the usability of a code. For practical purposes it is important that there exist an efficient decoding method to make use of the error-correcting capability, and it is important that error-patterns which are likely to occur in the actual application are usually corrected by the decoder.

In [1] a series of new distance functions on vectors over finite sets is introduced and some codes which are good with respect to this distance are constructed. However, decoding methods are not discussed. This paper provides efficient methods for unique decoding and for list-decoding of the codes presented in [1] which are based on Reed-Solomon and algebraic-geometry codes. The methods are based on Sudan's improved algorithm (see [2]).

II. The codes

Let $\mathbb{F}_q$ denote a finite field with q elements and suppose that

$$P := \{P_1, \ldots, P_n\} \subseteq \mathbb{F}_q \text{ with } |P| = n \qquad (1)$$

Consider a polynomial, $f \in \mathbb{F}_q[x]$. Given some $P_i \in P$ we can write

$$f = \sum_{j=0}^{\deg(f)} f_{j,i}(x - P_i)^j \text{ with } f_{j,i} \in \mathbb{F}_q$$

Definition 1 *Let r be a positive integer and let $0 < k \leq rn$. Then define the following error-correcting code:*

$$C(P, r, k) = \{f(P, r) \mid \deg(f) < k\}$$

with P being as in (1) and

$$f(P, r) := (f_{0,1}, \ldots, f_{r-1,1}; f_{0,2}, \ldots, f_{r-1,2}; \ldots; f_{0,n}, \ldots, f_{r-1,n})$$

III. The distance

In $C(P, r, k)$ codewords consists of n chunks of r field elements where each chunk corresponds to an element in P. This structure is reflected in the following definition of r-distance:

Definition 2 *Let r be a positive integer and let $u, v \in \mathbb{F}_q^{rn}$ with $u = (u_0, \ldots, u_{rn-1})$ and $v = (v_0, \ldots, v_{rn-1})$. For $i \in \{0, \ldots, n-1\}$ define the r-distance, $d_r(u, v, i)$, between u and v with respect to the i'th chunk as follows:*

$$d_r(u, v, i) := r - \min\{j \geq 0 \mid j = r \vee u_{ir+j} \neq v_{ir+j}\}$$

Furthermore, define the r-distance, $d_r(u, v)$, between u and v:

$$d_r(u, v) := \sum_{i=0}^{n-1} d_r(u, v, i)$$

The following theorem (a special case of [1], Theorem 6]) gives the main parameters of the code $C(P, r, k)$:

Theorem 3 *$C(P, r, k)$ is a linear code of length rn and dimension k. Furthermore, the minimum r-distance between two different codewords in $C(P, r, k)$ is $rn - k + 1$.*

IV. Decoding

In the paper Sudan's improved algorithm is modified to decode the code $C(P, r, k)$ beyond half the minimum r-distance. The following theorem holds:

Theorem 4 *Let $s \geq 1$ be a given parameter and let b_s satisfy*

$$\binom{b_s}{2} \leq \frac{rn\binom{s+1}{2}}{k-1} < \binom{b_s+1}{2}$$

Then the algorithm finds a list of all codewords within r-distance τ_s from the received word, where $\tau_s = rn - \lfloor \ell_s/s \rfloor - 1$ with $\ell_s := \lfloor (rns(s-1)+(k-1)b_s(b_s-1))/(2b_s) \rfloor$. Furthermore, the number of codewords on the list is at most $b_s - 1$.

For sufficiently large s it can be seen that $\tau_s \approx rn(1 - \sqrt{k/(rn)})$.

V. Conclusion

In [4] the code construction and decoding algorithm are generalized to a setting resembling algebraic geometry one-point codes. The generalization make use of so-called increasing zero bases (see [3], Theorem 1) giving a code construction slightly different from [1].

References

[1] M. Yu. Rosenbloom and M. A. Tsfasman, "Codes for the m-metric" *Problems of Information Transmission*, vol. 33, no. 1, pp. 45-52, 1997.

[2] Venkatesan Guruswami and Madhu Sudan, "Improved Decoding of Reed-Solomon and Algebraic-Geometric Codes" *IEEE Transactions on Information Theory*, vol. 45, no. 6, pp. 1757-1767, 1999.

[3] T. Høholdt and R. Refslund Nielsen, "Decoding Hermitian Codes with Sudan's Algorithm" *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC-13*, LNCS, No. 1719, pp. 260-270, 1999.

[4] R. Refslund Nielsen, "A class of Sudan-decodable codes" *IEEE Transactions on Information Theory*, to appear.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Enumeration And Construction Of All Binary Duadic Codes

Xin Li[1], Wei Sun, Yixian Yang,
and Zhengtao Zhang
P. O. Box 126, Information
Security Center
Beijing University of Posts and
Telecommunications
100876 Beijing, China
e-mail: yxyang@bupt.edu.cn

Abstract — **In this paper we give a construction of all binary duadic codes of length $n = {p_1}^{m_1}{p_2}^{m_2}\cdots{p_r}^{m_r}$, by which all binary duadic codes of given length can be enumerated.**

I. Introduction

Quadratic residue (Q.R.) codes are error-correcting codes with good performance [5]. Leon et al. [3] introduced a new family of binary cyclic codes, called duadic codes, which not only include Q.R. codes as subsets, but also have analogous properties to that of Q.R. codes. Leon et al. [3] also proved that binary duadic codes of length n exist if and only if $n = \prod_i p_i^{m_i}$, where each $p_i \equiv \pm 1 \pmod 8$ (see [3, 4]). Ding et al. [1] constructed and enumerated all of the binary duadic codes of prime length by presenting a cyclotomy to a prime $p \equiv \pm 1 \pmod 8$, and Ding [2] gave the construction and enumeration of all binary duadic codes of length p^m. However, the problem of constructing and enumerating the duadic codes with length $n = {p_1}^{m_1}{p_2}^{m_2}\cdots{p_r}^{m_r}$ remains open up to now. In this paper, we will completely solve this problem.

II. Main result

In the sequel, we use $\delta_n(a)$ to denote the multiplicative order of a modulo n.

We present a cyclotomic approach to the construction of all binary duadic codes of length p^m, by which the number of all binary duadic codes of length p^m is given.

Result 1 *Let $p \equiv \pm 1 \pmod 8$ be a prime, and $p \in P_{e_1} = \{p : (p-1)/\delta_p(2) = 2e_1\}$, $e_1 = 2^s e_0$, e_0 is odd, and let m be a positive integer. Then the number of splittings of p^m is*

$$N(p^m) = \sum_{j=0}^{s} 2^{-1}\left(2^{2^j e_0}\right)^{e/e_1},$$

where $e_k = \phi(p^k)/2\delta_{p^k}(2)$, $e = \sum_{k=1}^{m} e_k$. Thus the number of duadic codes of length p^m is $4N(p^m)$.

Furthermore, we give a construction of all binary duadic codes of length $n = {p_1}^{m_1}{p_2}^{m_2}\cdots{p_r}^{m_r}$, by which all binary duadic codes of given length can be enumerated.

Let $2T(l)$ denote the number of non-zero 2-cyclotomic cosets of ${p_1}^{m_1}{p_2}^{m_2}\cdots{p_l}^{m_l}$, and $2t_i$ denote the number of non-zero 2-cyclotomic cosets of ${p_i}^{m_i}$.

For any $l \geq 1$, if $\gcd(\delta_{p_i}(2), \delta_{p_j}(2)) = 1$ for $i \neq j$, $i, j \in \{1, 2, \cdots, l\}$, then

$$\begin{aligned} T(l) &= \sum_{i_1} t_{i_1} + 2\sum_{i_1<i_2} t_{i_1}t_{i_2} + 2^2 \sum_{i_1<i_2<i_3} t_{i_1}t_{i_2}t_{i_3} \\ &\quad + \cdots + 2^{l-1} t_1 t_2 \cdots t_l \\ &= \sum_{k=1}^{l}\left(2^{k-1}\sum_{i_1<i_2<\cdots<i_k} t_{i_1}t_{i_2}\cdots t_{i_k}\right) \end{aligned} \quad (1)$$

where $i_j \in \{1, 2, \cdots, l\}$ for $j = 1, 2, \cdots, l$.

Result 2 *Let $n = {p_1}^{m_1}{p_2}^{m_2}\cdots{p_r}^{m_r}$, $p_i \equiv \pm 1 \pmod 8$ a prime for $i = 1, 2, \cdots, r$, $N(x)$ denote the number of the splittings of x, $2t_i$ denote the number of non-zero 2-cyclotomic cosets of ${p_i}^{m_i}$, $2T(l)$ denote the number of non-zero 2-cyclotomic cosets of ${p_1}^{m_1}{p_2}^{m_2}\cdots{p_l}^{m_l}$, $T = \sum_{l=1}^{r-1}(T(l)t_{l+1} - 1)$. Then*

$$N(n) \geq \left(2^T\right)^2 \cdot 8^{r-1} \cdot N({p_1}^{m_1}) \cdot N({p_2}^{m_2}) \cdots N({p_r}^{m_r})$$

and the number of duadic codes of length n is at least $4N(n)$, where the equality is achieved if $\gcd(\delta_{p_i}(2), \delta_{p_j}(2)) = 1$ for $i \neq j$, in this case $T(l)$ can be obtained from Equation (1) for $l = 1, 2, \cdots, r-1$. In fact, $N({p_i}^{m_i})$ can be obtained from Result 1.

Acknowledgments

The authors wish to thank C. Ding for his valuable comments and suggestions.

References

[1] C. Ding and V. Pless, "Cyclotomy and duadic codes of prime lengths," *IEEE Trans. Inform. Theory*, Vol. 45, pp. 453–466, 1999.

[2] C. Ding, "Construction and enumeration of all binary duadic codes of length p^m," *Fundamental Informaticae*, Vol.38, No.1-2, pp. 149–161, April 1999.

[3] J. S. Leon, J. M. Masley, and V. Pless, "Duadic Codes," *IEEE Trans. Inform. Theory*, Vol. IT-30, pp. 709–714, 1984.

[4] V. Pless, J. M. Masley, and J. S. Leon, "On Weights in duadic codes," *J. Comb. Theory*, Vol. A-44, pp. 6–21, 1987.

[5] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, Amsterdam, The Netherlands: North-Holland, 1978.

[6] R. Lidl and H. Niederreiter, *Finite Fields*, Vol. 20 of Encyclopedia of Mathematics and its Applications. Reading, MA:Addison-wesley, 1980.

[1]This work was supported by National Natural Sicence Foundation of China(No. 69802002, 69882002 and 69772035), and by National "863" (No. 863-306-ZT05-05-2).

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Extremal Doubly-even Self-dual Cocyclic [40,20] Codes

A. Baliga
Department of Mathematics,
RMIT University
GPO Box 2476V
Melbourne, VIC 3001, Australia
e-mail: asha@rmit.edu.au

Abstract — **The structure of cocyclic Hadamard matrices allows us a much faster and more systematic search for binary, self-dual codes.The search for binary self-dual [40,20] codes from $\mathbf{Z}_5 \times \mathbf{Z}_2^2$ - cocyclic Hadamard matrices and two types of $\mathbf{D}_{20}$ - cocyclic Hadamard matrices resulted in 25 equivalence classes of extremal doubly-even codes. It is worth noting that the equivalence classes found in each case were disjoint, emphasising the importance of the cocyclic structure of the Hadamard matrices used.**

I. Introduction

Given a Hadamard matrix H of order $n = 8s + 4$, if the number of $+1$'s in each row and column of H is $\equiv 3 \pmod 4$ then the matrix $[I, \bar{H}]$ generates a binary, doubly-even, self-dual $[2n, n]$ code C, where $\bar{H} = (H + J)/2$, I is the identity matrix, J is the all 1's matrix of order n (see [4]).

If in addition H is of the shape

$$\begin{bmatrix} -1 & 1 \ldots 1 \\ 1 & \\ \vdots & H' \\ 1 & \end{bmatrix} \quad (1)$$

then H' is an $(+1,-1)$-incidence matrix of a symmetric Hadamard $2-(n-1, n/2, n/4)$ design, thus satisfying for $n > 4$ the condition required to produce doubly-even codes.

II. Self-dual codes from $\mathbf{Z}_5 \times \mathbf{Z}_2^2$ cocyclic Hadamard matrices

Here we consider H to be a $\mathbf{Z}_5 \times \mathbf{Z}_2^2$ - cocyclic Hadamard matrix.

From [2] the structure of a $\mathbf{Z}_t \times \mathbf{Z}_2^2$ - cocyclic matrix, t odd, is $\sim_h$ to a $t \times t$ block-backcirculant matrix W with top row $W_1, W_2, \ldots, W_t$, where

$$W_i = \begin{bmatrix} n_i & x_i & y_i & z_i \\ x_i & An_i & z_i & Ay_i \\ y_i & Kz_i & Bn_i & BKx_i \\ z_i & AKy_i & Bx_i & ABKn_i \end{bmatrix}, \quad 1 \le i \le t. \quad (2)$$

[1] gives the conditions which make the search for self-dual codes more efficient that any known searches. [1] also includes a list of codes obtained from a preliminary search from these Hadamard matrices.

The Hadamard matrices were also converted into the equivalent (1) form and used to produce more codes from $\mathbf{Z}_5 \times \mathbf{Z}_2^2$ - cocyclic Hadamard matrices. Two equivalence classes of extremal doubly-even $\mathbf{Z}_5 \times \mathbf{Z}_2^2$- cocyclic[40,20] codes were found, one using the 1 form.

III. Self-dual codes from D_{4t}

In [3] Flannery details the conditions for the existence of a Hadamard matrix cocyclic over D_{4t}, the dihedral group of order $4t, t \ge 1$, given by the presentation

$$< a, b | a^{2t} = b^2 = (ab)^2 = 1 >$$

Cocyclic Hadamard matrices developed over D_{4t} exist only in the case $(A, B, K) = (1,-1,1), (1,-1,-1), (-1,1,1)$ for t odd, where A and B are the inflation variables and K is the transgression variable. The matrices for $(A, B, K) = (1,-1,1)$ and $(1,-1,-1)$ possess the most tractable block structure and are the only cases dealt with here.

In the case $(A, B, K) = (1,-1,1)$, if there is a cocyclic Hadamard matrix associated with a cocycle in this class, then t is the sum of two squares. The cocyclic Hadamard matrices have the form $\begin{pmatrix} M & N \\ NC_{2t} & -MC_{2t} \end{pmatrix}$ where the matrices M and N are $2t \times 2t$ back circulant matrices and C_{2t} is the back circulant $2t \times 2t$ permutation matrix with first row 1 0 0 0... 0..

The case $(A, B, K) = (1,-1,-1)$ is very prolific, giving more Hadamard matrices cocyclic over D_{4t} for t odd, than the case above. The cocyclic Hadamard matrices are of the form $\begin{pmatrix} M & N \\ ND & -MD \end{pmatrix}$, where the $2t \times 2t$ matrices M and N are each the entrywise product of a back circulant and back negacyclic matrix (hence are symmetric), and D is the $2t \times 2t$ matrix obtained by negating every noninitial row of C_{2t}.

Generating matrices using both the cocyclic forms and the (1) form were used. Again it was seen that other equivalence classes were obtained by using the (1) form. In general it was found that there were more equivalence classes obtained from the Dihedral construction than the $\mathbf{Z}_5 \times \mathbf{Z}_2^2$ construction.

In the case $(A, B, K) = (1,-1,1)$ there were two equivalence classes, one obtained by using the (1) form, with 6400 codes in each class.

In the case $(A, B, K) = (1,-1,-1)$ a total of 5621 extremal codes were found divided into 21 equivalence classes. Usage of the (1) form resulted in 11200 codes in another two equivalence classes.

References

[1] A. Baliga, New self-dual codes from cocyclic Hadamard matrices, J. Combin. maths. Combin. Comput., 28 (1998) pp. 7-14.

[2] A. Baliga and K.J. Horadam, Cocyclic Hadamard matrices over $\mathbf{Z}_t \times \mathbf{Z}_2^2$, Australas. J. Combin., 11 (1995) pp. 123-134.

[3] D.L. Flannery, Cocyclic Hadamard matrices and Hadamard groups are equivalent, J. Algebra, 192 (1997), pp 749-779.

[4] V.D. Tonchev, Self-orthogonal designs and extremal doubly-even codes, J. Combin. Theory, Ser A 52,(1989), 197-205.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

A New Family of Optimal Codes Correcting Term Rank Errors

David Lund
Dept. Communication Systems
Lancaster University
Lancaster
LA1 4YR, UK
e-mail: d.j.lund@lancaster.ac.uk

Ernst. M. Gabidulin
Moscow Institute of Physics and Technology
Dept. of Radio Engineering, Head
Institutskii per., 9
141700 Dolgoprudny, Russia
e-mail: gab@jane.telecom.mipt.ru

Bahram Honary
Dept. Communication Systems
Lancaster University
Lancaster
LA1 4YR, UK
e-mail: b.honary@lancaster.ac.uk

Abstract — **We consider messages represented as matrices. The term rank norm of a matrix is defined as minimal number of lines (rows and coulmns) which cover all the non zero entries of a matrix. We propose a family of codes correcting term rank errors. These codes are optimal since they reach the Singleton-type bound.**

I. Introduction

In digital communication, messages are often represented as matrices. For example, in FDMA or OFDM systems, information is transmitted through a system of parallel channels. A message can be considered an $N \times n$ matrix where N is the number of channels and n is the duration of transmission in number of symbols.

The model in which the most probable event is a corruption of a row or a column is considered. A formal description of such errors is given.

For simplicity we restrict our consideration to the binary case. Let X be an $N \times n$ binary matrix. Let $w(X)$ be the minimal number of lines (rows or columns) which cover all the non zero entries of the matrix. The number $w(X)$ is known as the term rank of the matrix X. This notation is introduced and used in combinatorial matrix theory [3]. The term rank function $w(X)$ on the set of all matrices of the given size is in fact the norm function.

The concept of term rank distance for coding theory was introduced in 1971 (see, [1][2]. The term "lattice-pattern errors" was used that here instead of "term rank errors".)

The maximal norm is $w_{\max} = \min\{N, n\}$. The *term rank distance* between X and Y is defined as $d(X,Y) = w(X-Y)$. Let C be a code, i.e., any set of matrices of given size. The term rank distance of a code is defined as

$$d = d(C) := \min_{M_i \neq M_j} \{w(M_i - M_j) | M_i \in C, M_j \in C\}$$

A code with term rank distance d can correct up to $(d-1)/2$ term rank errors.

Let $M = |C|$ be the cardinality of the code C. The rate of the code is defined as $R := \frac{\log_2 M}{Nn}$.

The next Lemma gives the Singleton-type upper bound.

Lemma 1: Let C be a matrix code of size $N \times n$, rate R, and term rank distance d. Then

$$R \leq 1 - \frac{d-1}{w_{\max}} = 1 - \frac{d-1}{\min\{N,n\}}. \qquad (1)$$

A code C is said to be the *Maximal Term Rank Distance* (MTRD) code if it satisfies the equation (1) with the equality sign.

It can be easily shown that codes for rectangular matrices can be derived from codes for square matrices.

II. Construction of Codes

Note: Rank codes proposed in [4] can correct also term rank errors. We consider more general codes which are not rank codes.

A. Known Codes of Term Rank Distance n and 2.

The codes descirbed here are proposed in [1] & [2].

B. New Optimal Codes of Term Rank Distance 3 and n − 1

We generalise properties of previous codes in this case.

Lemma 2: A Code C is a MTRD $[n, n-2, 3]$ code if and only if any $n-2$ rows of the general code matrix can be considered as information rows *and* any $n-2$ columns of the general code matrix can be considered as information columns.

Let $C^{\perp}$ be the dual code of C.

Lemma 3: A code $C^{\perp}$ is a MTRD $[n, 2, n-1]$ code.

The general code matrix of a MTRD $[n, n-2, 3]$ code can be represented in two equivelent forms. The full construction is given and illustrated by example.

III. Decoding

We discuss also decoding methods including the majority decoding and soft decision decoding based on the method of trellis decoding similar to those described in [5].

References

[1] E. M. Gabidulin, "A Class of Two-Dimensional Codes Correcting Lattice Pattern Errors", Proceedings of the 2nd International Symposium on Information Theory, pp. 44-47, 1971.
[2] E. M. Gabidulin, V. I. Korzhik, "Codes Correcting Lattice Pattern Errors", Izvestia VUZov MVSSO SSSR - Radioelectronika, v. 15, No. 4, pp. 492-498, 1972 (In Russian).
[3] R. A. Brualdi, H. J. Ryser, "Combinatorial Matrix Theory", Encyclopaedia of Mathematics and its applications, Cambridge University Press, 1991.
[4] E. M. Gabidulin, "Theory of Codes with Maximal Rank Distance", Problems of Information Transmission, v. 21, No. 1, pp 3-14, 1985.
[5] Honary B., Markarian G., "Trellis Decoding of Block Codes", Kluwer Academic Publishers 1997.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Subcode Graphs of Linear Block Codes

Thomas Mittelholzer
IBM Zurich Research Laboratory
Säumerstrasse 4
CH-8803 Rueschlikon, Switzerland
e-mail: tmi@zurich.ibm.com

Abstract — **The Hamming-distance related lattice of subcodes of a linear code C is represented by a subcode graph. The dimensions of these subcodes and the dimensions of the subcodes of the dual are related by MacWilliams-like identities. The coordinate permutation problem for minimum trellis-complexity is approached by introducing suitable vertex functions on the subcode graph that reflects the trellis-complexity measure. This approach gives a simple new proof for well-known results on maximum-distance separable (MDS) codes and a slight sharpening of the Wolf bound for a large class of binary codes.**

I. The Subcode Graph

Let $C \subset \mathbf{F}^n$ be a linear (n,k) block code over a field $\mathbf{F}$. For each subset $s = \{s_1, \ldots, s_\ell\}$ of the codeword components $\{1, \ldots, n\} \triangleq I$ of cardinality ℓ, we consider the ℓ-dimensional subspace $F_s \subset \mathbf{F}^n$ with support in s and the subcode with support in s, $C_s = C \cap F_s$. If $s' \subset s$, then there is an inclusion map $i_{s',s} : C_{s'} \to C_s$. The lattice structure of the subcodes C_s can be illustrated by a *subcode graph*, which is defined as follows. The vertices of the graph are the subspaces C_s. There is a directed edge from vertex C'_s to vertex C_s, whenever $s' \subset s$ and the cardinalities of the two sets satisfy $|s'|+1 = |s|$. Note that the subcode graph is actually a trellis with n trellis sections, where $|s| = \ell$ represents the time index.

II. MacWilliams-like Identities

Using the techniques of the original proof No. 1 of the MacWilliams Identity [1], one can derive some simple MacWilliams-like identities, which hold for arbitrary fields.

In analogy to the full weight enumerator of a linear (n,k) code [2], we define the *full dimension enumerator* by

$$\alpha(\mathbf{Y},\mathbf{Z}) = \alpha(Y_1,\ldots,Y_n,Z_1,\ldots,Z_n) = \sum_{s \subset I} \dim(C \cap F_s) Y_s Z_{I \setminus s}$$

where s runs through all subsets of cardinality $\ell = 0,1,\ldots,n$ and Y_s and $Z_{I\setminus s}$ denote the monomials $Y_{s_1}\cdots Y_{s_\ell}$ and $Z_{t_1}\cdots Z_{t_{n-\ell}}$, $t_i \in I \setminus s$, resp. The *dimension enumerator* of the code C is defined by

$$\tilde{\alpha}(Y) = \sum_s \dim(C \cap F_s) Y^{|s|}.$$

Theorem 1 *Let $\tilde{\alpha}(Y)$ and $\tilde{\beta}(Y)$ ($\alpha(\mathbf{Y},\mathbf{Z})$ and $\beta(\mathbf{Y},\mathbf{Z})$) be the (full) dimension enumerators of a linear (n,k)-code C and its dual $C^\perp$, resp. Then, the following identities hold*

$$Y^n \tilde{\beta}(Y^{-1}) = \tilde{\alpha}(Y) + \sum_{\ell=0}^{n} (n-k-\ell) \binom{n}{\ell} Y^\ell$$

$$\beta(\mathbf{Z},\mathbf{Y}) = \sum_{\ell=0}^{n} (n-k-\ell) \sum_{s,\,|s|=\ell} Y_s Z_{I\setminus s} + \alpha(\mathbf{Y},\mathbf{Z}).$$

Remarks: 1.) Theorem 1 holds for any field and can be extended to codes that are projective modules over abelian artinian rings. 2.) The lowest degree nonzero term of the dimension enumerator specifies the minimum distance d_{min} and the corresponding codeword multiplicity μ_{min}.

III. The Permutation Problem

For a generic linear block code it is computationally difficult to find a permutation of the codeword components that results in a minimal trellis [3], [4]. We will approach the permutation problem by introducing suitable vertex functions on the subcode trellis:

- the *dimension vertex function* is given by $k(C_s) = \dim C_s + \dim C_{I\setminus s}$, and
- (in case of a finite field) the *enumerator vertex function* is given by $e(C_s) = |C_s| \cdot |C_{I\setminus s}|$.

Each path from the starting node to the ending node in the subcode trellis corresponds to a chain of support sets $\emptyset = s^{(0)} \subset s^{(1)} \subset \ldots \subset s^{(n)} = I$ and this determines an ordering of the codeword components. Thus, permutation problems for a given linear block code can be transformed into a path search problem on the subcode trellis. E.g., looking for an optimal permutation of the coordinates that minimizes the maximum state space complexity is equivalent to finding a path through the subcode trellis, which goes through a vertex with maximum value $k(C_s)$ of the dimension vertex function.

This approach allows one to give a simple alternative proof, using Theorem 1, to show that permuting the codeword components of an MDS code does not change the dimension of the state spaces of its minimal trellis, which is well-known [4]. Moreover, for a large class of codes, the Wolf bound (Theorem 5.5 in [4]) can be slightly sharpened as follows.

Proposition 1 *Let C be a binary linear (n,k) code. If either*

(i) $2 \le k \le n/2$ and the all-one word is in C, or

(ii) $n/2 \le k \le n-2$ and the all-one word is in $C^\perp$

then the maximum state complexity K_s is upper bounded by

$$K_s \le \min\{k, n-k\} - 1.$$

References

[1] J. MacWilliams, "A theorem on the distribution of weights in a systematic code," *Bell Syst. Tech. J.*, vol. 42, pp. 79–94, 1963.

[2] E.M. Rains, N.J.A. Sloane, *Self-Dual Codes* in *Handbook of Coding Theory, Part I*, Eds. V.S. Pless and W.C. Huffman. North-Holland, Elsevier Science, 1998.

[3] G.B. Horn, F.R. Kschischang, "On the Intractability of Permuting a Block Code to Minimize Trellis Complexity," *IEEE Trans. Information Th.*, Vol. 42, No. 6, Nov 1996, pp. 2042 – 2048.

[4] A. Vardy, *Trellis Structure of Codes*, in *Handbook of Coding Theory, Part II*, Eds. V.S. Pless and W.C. Huffman. North-Holland, Elsevier Science, 1998.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

General Structure and Construction of Tail Biting Trellises for Linear Block Codes

Shu Lin
University of California, Davis
Davis, CA 95616
e-mail:shulin@ece.ucdavis.edu

Rose Y. Shao
Quantum Corporation
Shrewsbury, MA 01545
e-mail:rose.shao@quantum.com

I. Introduction

A tail biting trellis for a code is a trellis with multiple starting and ending states which has the following structures: (1) the starting and ending state spaces are identical; (2) every starting state has a unique ending state and they are the same state; and (3) a path in the trellis is a valid codeword if and only if its starting and ending states are identical [1, 2]. For a block code, tail biting trellis representation may result in a significant reduction in trellis complexity [2].

II. General Structure

The general structure of an L-section tail biting trellis T for an (n, k) linear block code C is depicted in Figure 1. Let $\{0, 1, ..., L\}$ denote the set of state boundary locations. Suppose T consists of 2^m starting states and 2^m ending states. We may view T as a union of 2^m isomorphic subtrellises which share a common part from boundary location(BL)-t_1 to BL-t_2, where $t_1 < t_2$. Each subtrellis consists of those paths in T that connect a state at BL-0 to the same state at BL-L, and it has three parts, the header, the center span and the tail. The center span is shared by every subtrellis. For $1 \leq i \leq 2^m$, let T_i denote the subtrellis whose starting and ending states are $s_0^{(i)}$ and $s_L^{(i)}$, respectively. Assume that T_1 contains the all-zero path. Then the paths in T_1 form an $(n, k-m)$ linear subcode of C, denoted C_1, and the paths in any other subtrellis form a coset of C_1 in C. Let $\mathbf{v} = (v_1, v_2, \cdots, v_n)$ be a codeword in C. Since all the subtrellises have the same common span from BL-t_1 to BL-t_2, there must be a codeword $\mathbf{w} = (w_1, w_2, ..., w_n)$ in each subtrellis whose components from location-$(t_1 + 1)$ to location-t_2 are zeros. For convenience, we call the part of first t_1 components of $\mathbf{w}$ the header, the part of last $n - t_2$ components of $\mathbf{w}$ the tail. Adding $\mathbf{w}$ to each path in T_1 results in a subtrellis which is isomorphic to T_1 and is identical to T_1 from BL-t_1 to BL-t_2. The header and the tail of this subtrellis are obtained by adding the header and the tail of $\mathbf{w}$ to the header and the tail of T_1, respectively. This subtrellis is the trellis for the coset $\mathbf{w} + C_1$ of C_1 and $\mathbf{w}$ is the coset representative.

Although all the subtrellises share a common span from BL-t_1 to BL-t_2. Two individual subtrellises may share a longer span starting from BL-i to BL-j with $0 < i \leq t_1$ and $t_2 \leq j < L$. For $0 < i < j < L$, let $[i, j]$ denote the interval $\{i, i+1, \cdots, j\}$. The zero-span of an n-tuple $\mathbf{v} = (v_1, v_2, \cdots, v_n)$ is defined as the largest interval $[i, j]$ such that $v_{i+1} = v_{i+2} = \cdots = v_j = 0$. This definition implies that $v_i = v_{j+1} = 1$. Let $\mathbf{v}$ be a codeword in C but not in C_1 whose zero-span is $[i, j]$ with $0 < i \leq t_1$ and $t_2 \leq j < L$. It is clear that $[t_1, t_2] \subseteq [i, j]$. Let $T_1(\mathbf{v})$ denote the subtrellis for the coset $\mathbf{v} + C_1$ obtained by adding $\mathbf{v}$ to every path in T_1. Then $T_1(\mathbf{v})$ and T_1 have a common span from BL-i to BL-j. Let $\mathbf{v}$ and $\mathbf{w}$ be codewords in two different cosets of the partition C/C_1. Let $[i_1, j_1]$ and $[i_2, j_2]$ be the zero-spans of $\mathbf{v}$ and $\mathbf{w}$, respectively. Let $[i_3, j_3] = [i_1, j_1] \cap [i_2, j_2]$. Then the co-subtrellises, $T_1(\mathbf{v})$ and $T_1(\mathbf{w})$, are isomorphic and have a common span from BL-i_3 to BL-j_3.

III. Construction

For $0 < t_1 < t_2 < L$, let $C(t_1, t_2)$ denote the set of codewords in C which satisfy the following conditions: (1) each nonzero codeword $\mathbf{v}$ in $C(t_1, t_2)$ has zero components from location-$(t_1 + 1)$ to location-t_2, i.e., $v_{t_1+1} = v_{t_1+2} = \cdots = v_{t_2} = 0$, and (2) the part of first t_1 components of $\mathbf{v}$ contains at least one nonzero component and the part of last $n - t_2$ components of $\mathbf{v}$ contains at least one nonzero component. Then $C(t_1, t_2)$ is a linear subcode of C. The zero-span of each codeword in $C(t_1, t_2)$ contains $[t_1, t_2]$ as a subinterval. Let m be the dimension of $C(t_1, t_2)$. There exists an $(n, k-m)$ linear subcode C_1 in C such that C is the direct sum of C_1 and $C(t_1, t_2)$. Let C/C_1 denote the partition of C modulo C_1. Then the vectors in $C(t_1, t_2)$ can be used as the coset representatives of the coset in C/C_1.

Let T_1 be the minimal conventional bit-level trellis for C_1. Form all the co-trellises $T_1(\mathbf{v})$ of T_1 with $\mathbf{v} \in C(t_1, t_2)$. All these co-trellises have a common span from BL-t_1 to BL-t_2. Putting all these co-trellises together and sharing maximum common spans between them, we obtain a tail biting trellis with 2^m starting states and 2^m ending states. The overall complexity of this tail biting trellis depends on the length of common span of the co-trellises, the choice of the boundary locations, t_1 and t_2, of the common span. These parameters should be chosen to minimize the trellis complexity.

References

[1] G. Solomon and H. C. A van Tilborg, " A connection between block and convolutional codes", *SIAM J. Appl. Math.*, Vol. 37, No. 2, pp. 358-369, Oct. 1979.

[2] A. R. Calderbank, G. D. Forney Jr. and A. Vardy, "Minimal Tail-Biting Trellises: Golay Code and More," *IEEE Trans. Inform. Theory*, Vol.45, No.5, pp. 1435-1455. July 1999.

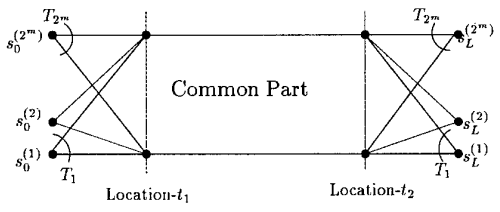


Figure 1: General structure of a tail biting trellis.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Minimal Tail-Biting Trellises for Linear MDS Codes over F_{p^m}

B.Sundar Rajan[1]
Department of Electrical Communication Engineering
Indian Institute of Science
Bangalore 560 012, India
bsrajan@ece.iisc.ernet.in

G.Viswanath
Department of Electrical Communication Engineering
Indian Institute of Science
Bangalore 560 012, India
gviswa@protocol.ece.iisc.ernet.in

Abstract — **For all linear (n,k,d) MDS over finite fields F_{p^m}, we identity a generator matrix with the property that the product of trellises of rows of the generator matrix will give a minimal tail-biting linear trellis, and viewing the code as a group code, identify a set of generators, product of whose trellises will give a minimal tail biting group trellis. We also give the necessary and sufficient condition for the existence of flat minimal linear and group tail-biting trellises.**

I. Introduction

Trellis representation of block codes illuminate the structure of the code and also useful for efficient decoding. Recently, unconventional "Tail-biting trellises" (TBT) have been studied for well known codes like (24,12,8) Golay code, hexacode and few other short codes [1].

Minimal Tail-Biting Trellis: A tail-biting trellis with minimum maximum number of states along with the minimum product of all state space sizes, among all tail-biting trellises for the code under all possible coordinate permutations is called a minimal tail-biting trellis for the code.

The total span bound: [1] If C is an (n,k,d) linear code over F_q, then any n-section linear tail-biting trellis for C satisfies

$$\prod_{j=0}^{n-1} |S_j| \geq q^{k(d-1)} \tag{1}$$

$$S_{max} \geq q^{\frac{k}{n}(d-1)} \tag{2}$$

If $q = p^m$, then for group trellises we have

$$S_{max} \geq p^{\frac{mk}{n}(d-1)} \tag{3}$$

Flat Trellis: A tail-biting trellis is said to be flat if it has a constant state complexity profile.

It is well known that any k coordinates of a MDS code can be taken as information positions. This means that minimum weight vectors (of weight $n-k+1$) with circular span $n-k$ can be obtained such that the successive $n-k+1$ nonzero components start from any specified coordinate position from $\{0,1,...,(n-1)\}$. It can be shown that any k such vectors starting from different coordinate positions will constitute a generator matrix for the code. Using these results in the next section we specify the generator matrices that give minimal tail-biting trellises in terms of these k coordinate positions.

II. Minimal Circular Span Generator Matrices

Theorem 1: For a (n,k) linear MDS code over F_{p^m}, let $e = gcd(n,k)$, $n' = \frac{n}{e}$, $k' = \frac{k}{e}$ and $n' = \alpha k' + \beta$, where α and β are integers. The generator matrix which has only minimum weight vectors with consecutive nonzeros and with nonzeros starting from the indices given by the set I given below gives a minimal linear tail-biting trellis when product of trellises corresponding to each row vector is obtained:

$$\begin{aligned} I = \; & \{[\{jn' + i(\alpha+1) | i = 0,1,\ldots,\beta\} \cup \\ & \{jn' + \beta(\alpha+1) + (i-\beta)\alpha | i = \beta+1,\ldots,k'-1\}] \\ & j = 0,1,...,(e-1).\} \end{aligned} \tag{4}$$

Theorem 2: A necessary and sufficient condition for an (n,k) linear MDS code over any finite field to admit a minimal linear flat-trellis is that "n divides k^2".

Notice that the condition in Theorem 2 is independent of the size of the field.

Theorem 3: For a (n,k) linear MDS code over F_{p^m}, let $e = gcd(n,mk)$, $n' = \frac{n}{e}$, $k' = \frac{mk}{e}$. Also, let $k' = an' + k''$ where $0 \leq k'' < n'$ and $n' = \alpha k'' + \beta$, where $0 \leq \beta < k''$ and a and α are integers. The group-generator matrix which has $a+1$ minimum weight vectors with consecutive nonzeros with nonzeros starting from the indices given by the set I given below and a minimum weight vectors with consecutive nonzeros with nonzeros starting at all other time indices gives a minimal group tail-biting trellis when product of trellises corresponding to each row vector is obtained, if the rows starting at the same index are p-linearly independent (which can always be achieved):

$$\begin{aligned} I = \; & \{[\{jn' + i(\alpha+1) | i = 0,1,\ldots,\beta\} \cup \\ & \{jn' + \beta(\alpha+1) + (i-\beta)\alpha | i = \beta+1,\ldots,k''-1\}] \\ & j = 0,1,...,(e-1).\} \end{aligned} \tag{5}$$

Theorem 4: A necessary and sufficient condition for a linear (n,k) MDS code over F_{p^m} to admit a minimal group flat-trellis is that "n divides mk^2".

Observe that the condition in Theorem 4 depends only on m and not on the characteristic of the field.

Acknowledgments

B.S.Rajan gratefully acknowledges IBM India Research Lab, for the travel support to present this paper.

References

[1] A.R.Calderbank, G.D.Forney and A.Vardy, "Minimal Tail-Biting Trellises: The Golay Code and More", *IEEE Trans. on Information Theory*, Vol.45, No.5, pp.1435-1455, July 1999.

[2] F.R.Kschischang and V.Sorokine, "On the trellis structure of Block codes ", *IEEE Trans. Information Theory*, Vol.41, pp.1924-1937, Nov. 1995.

[1]This work was partly supported by CSIR, India, through Research Grants (No:25(0086)/97/EMRI-II) and (22(0298)/99/EMR-II) to B.S.Rajan

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Uniformly Efficient Trellises for Self-Dual Codes

Houshou Chen
Dept. of EE, National Chi-Nan University, Nantou, Taiwan 545.
e-mail: houshou@ncnu.edu.tw

John T. Coffey[1]
Dept. Of EECS, University of Michigan, Ann Arbor, MI, USA.
e-mail: scoffey@eecs.umich.edu

Abstract — **Uniformly efficient trellis decoders are known for very few codes, and no general method is known that can decide whether such a decoder exists. It is shown that this question is substantially simplifiable in the case of self-dual codes, when certain subcodes meet the Griesmer bound with equality. Furthermore, in many cases the result makes it possible to count the number of uniformly efficient permutations. In some cases the existence and number of uniformly efficient trellises may be deduced directly from the parameters of the code. Among the codes that meet the criterion are the $[24, 12, 8]$ Golay code, for which the number of uniformly efficient permutations is derived, four of the $[32, 16, 8]$ doubly even codes, and the $[48, 24, 12]$ quadratic residue code, for which a lower bound on the number of uniformly efficient permutations is derived.**

I. Introduction

We consider the *permutation* problem for trellis decoders for block codes. For all necessary definitions, background, and references, we refer to Vardy's chapter [4], in particular Section 5.

For any fixed ordering of a code, a minimal trellis may be found efficiently. However, an equivalent code will have its own minimal trellis, which may be of substantially lower complexity. As there is no useful distinction between two equivalent codes for many purposes, the problem is to find a permutation that minimizes the complexity in some sense.

Various definitions of optimality may be used; here we are concerned with one of the strongest: that of "uniform efficiency." A permutation is uniformly efficient if the minimal trellis for the corresponding code minimizes the state complexity at each time unit simultaneously, i.e., if $s_i(\pi^*(C)) \leq s_i(\pi(C))$ for all permutations π and all i. Such a permutation may or may not exist.

There are very few codes for which such permutations are known. These include the binary Reed-Muller codes, MDS codes, the $[24, 12, 8]$ Golay code, the $[48, 24, 12]$ quadratic residue code, and the $[16, 7, 6]$ lexicode [4]. Classification of the existence or nonexistence question for short self-dual codes has been carried out by Encheva and Cohen [2, 3].

Here we consider self-dual codes. Our main result, when it applies, provides a way of demonstrating the existence of a uniformly efficient permutation and of counting all such permutations. This resolves a question posed by McEliece for the case of the $[24, 12, 8]$ Golay code.

II. Main result

Theorem. *Let C be a self-dual code. Suppose $k_{n/2}(C)$ is such that $n/2 = g_q(k_{n/2}, d)$, where $g_q(k, d) \equiv \sum_{i=0}^{k-1} \lceil d/q^i \rceil$ is the Griesmer bound function. Then:*

(a) *the code satisfies the double chain condition;*

(b) *the code meets the DLP bound;*

(c) *the code has the smallest state complexity in each component among all self-dual codes of the same length and dimension, and at least the same distance;*

(d) *the optimum state complexity profile is $s_i = i - 2g_q^{-1}(i, d)$ for $i \leq n/2$, and $s_{n-i} = s_i$, where $g^{-1}(i, d) = \max\{j | i \geq g(j, d)\}$;*

(e) *a permutation is uniformly efficient if and only if it is of the form*

$$G = \begin{bmatrix} G_1 & 0 \\ 0 & \tau(G_2) \\ E & F \end{bmatrix}, \qquad (1)$$

where $C_1 = \langle G_1 \rangle$ is a length $n/2$, distance d code that meets the Griesmer bound with equality, and is in chain condition order; and where G_2 generates a code with the same parameters as C_1, and is in chain condition order; and where $\tau(G_2)$ is the column reverse of G_2.

III. Application

The main result applies to the following self-dual codes: the binary $[8, 4, 4]$, $[12, 6, 4]$, $[14, 7, 4]$, and $[24, 12, 8]$ codes, one of the $[16, 8, 4]$ codes, four of the eight $[32, 16, 8]$ codes, and the $[48, 24, 12]$ quadratic residue code; the ternary $[12, 6, 6]$ Golay code, and both ternary $[24, 12, 9]$ codes. The results for three of the $[32, 16, 8]$ binary codes and both ternary $[24, 12, 9]$ codes are new. In addition, using part (e), we may in some cases easily find the number of uniformly efficient permutations: this happens for the binary $[12, 6, 4]$, $[14, 7, 4]$, $[16, 8, 4]$, and $[24, 12, 8]$ codes, and the ternary $[12, 6, 6]$ and $[24, 12, 9]$ codes. The number of uniformly efficient permutations for the $[24, 12, 8]$ Golay code is, from part (e), equal to the number of X_{12}'s times the square of the number of chain condition orderings of a $[12, 2, 8]$ code, i.e., $35420(3 \cdot 8! \cdot 4!)^2$ permutations out of all $24!$, a fraction of approximately 4.81×10^{-7} of all permutations.

The main result may be generalized at the cost of a nontrivial increase in the difficulty of application [1]; the generalization applies to many more self-dual codes.

[1]This work was supported in part by the U. S. Army Research Office under Grant DAAH04-96-1-0377.

References

[1] H. Chen and J. T. Coffey, "Trellis structure and higher weights of extremal self-dual codes," submitted to *Designs, Codes and Cryptography*, Sep. 1999.

[2] S. B. Encheva and G. D. Cohen, "Self-orthogonal codes and their coordinate ordering," *IEICE Trans. Fundamentals*, vol. E80-A, no. 11, pp. 2256–2259, 1997.

[3] S. B. Encheva and G. D. Cohen, "On the state complexities of ternary codes", Proc. AAECC 13, Honolulu, Hawaii, Nov. 15–19, 1999, pp. 454–461.

[4] A. Vardy, "Trellis structure of codes," in *Handbook of Coding Theory, Volume II*, V. S. Pless and W. C. Huffman, editors, North-Holland, Amsterdam, The Netherlands, 1998.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

General Coding Theorems for Turbo-like codes[1]

Hui Jin
Dept. of Electrical Engineering
California Institute of Technology
Pasadena, California, USA
e-mail: hui@systems.caltech.edu

Robert J. McEliece
Dept. of Electrical Engineering
California Institute of Technology
Pasadena, California, USA
e-mail: rjm@systems.caltech.edu

Abstract — **In this paper we prove that for general memoryless binary input channels, most ensembles of parallel and serial turbo codes, with fixed component codes, are "good" in the sense that with maximum likelihood decoding, their word (or bit) error probability decreases to zero as the block length increases, provided the noise is below a finite threshold. Our proof uses the classical union bound, which shows that under very general conditions, if the noise is below a certain threshold, the word (or bit) error probability is controlled by the low-weight codewords as the block length approaches infinity. Our main coding theorems then follow from a study of the low weight terms in the ensemble weight enumerator. Using this methodology, we can prove that the threshold is finite for most ensembles of parallel and serial turbo codes.**

I. Introduction

This paper addresses the basic question as to whether turbo codes, both parallel and serial, are "good" in the sense of MacKay [5]. The earliest work on this problem is in [1, 2], where "interleaving gain" was first proposed and investigated, but this was not fully rigorous.

In this paper, we restrict ourselves to memoryless binary input channels with maximum likelihood decoding. Our specific goal is to prove a general coding theorem for ensembles of parallel or serial concatenated convolutional codes, where the ensemble is taken with respect ot all possible interleavers. The tools we use are the union bound and the ensemble weight enumerator. Previously, in [3], we analyzed RA codes on AWGN channels, by deriving the input-output weight enumerator (IOWE), from which we could compute a signal-to-noise ratio threshold above which the ensemble is "good." This technique fails for complex component codes, because calculation of the IOWE is intractable. Fortunately, to prove coding theoremd, the exact IOWE isn't indispensable. Instead, a good upper bound of that proves to be sufficient.

II. Union Bounds

Consider a linear (n, N) block code C with rate $R_c = N/n$. The union bound on the word error probability P_W of the code C over a memoryless binary input channel, using ML decoding has the form:

$$P_W \leq \sum_{h=1}^{n} A_h e^{-\alpha h}, \tag{1}$$

where A_h denotes the number of codewords in C with output weight h. The parameter α is determined by channel.

[1]This work was supported by NSF grant no. CCR-9804793, and grants from Sony and Qualcomm.

III. Main Result

Theorem 1 *For an ensemble of a parallel concatenated convolutional code with recursive components, if the number of recursive parallel branches is $k \geq 2$, then there exists a positive number γ_o, such that for any fixed $\alpha > \gamma_o$,*

$$P_W = O(n^{-k+2+\epsilon}) \tag{2}$$

$$P_b = O(n^{-k+1+\epsilon}) \tag{3}$$

for arbitrary $\epsilon > 0$.

Theorem 2 *For an ensemble of a serial concatenated convolutional code with recursive inner code, if the free distance of the outer code d_o^* is at least 3, then there exists a positive number γ_o, such that for any fixed $\alpha > \gamma_o$,*

$$P_W = O(n^{-\lfloor \frac{d_o^*-1}{2} \rfloor + \epsilon}). \tag{4}$$

$$P_b = O(n^{-\lfloor \frac{d_o^*+1}{2} \rfloor + \epsilon}). \tag{5}$$

for arbitrary $\epsilon > 0$.

IV. Remarks

The thresholds derived by classical union bound are by no means the best possible. In the following table, we compare those thresholds for RA codes over BSC derived by union bound with those by typical set decoder bound [6].

q	R	UB:γ_q	TD:γ_q	Capacity
3	1/3	0.091	0.132	0.174
4	1/4	0.132	0.191	0.215
5	1/5	0.163	0.228	0.243

References

[1] S. Benedetto. D. Divsalar, G. Montorsi, and F. Pollara, "Serial Concatenation of interleaved codes: Performance analysis, design, and iterative decoding," *IEEE Trans. on Info. Theory*, vol. 44, pp. 909–926, 1998.

[2] S. Benedetto and G. Montorsi, "Unveiling turbo codes: some results on parallel concatenated coding schemes, " *IEEE Trans. on Info. Theory*, vol. 42, pp. 409-428, 1996.

[3] D. Divsalar, H. Jin, and R. J. McEliece, "Coding theorems for 'turbo-like' codes," in *Proc. 36th Allerton Conf. on Communication, Control and Computing*, pp. 201-210, 1998.

[4] N. Kahale and R. Urbanke, "On the minimum distance of parallel and serial concatenated codes," in *Proc. ISIT 1998* , p. 31, 1998.

[5] D. J. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Trans. Info. Theory*, vol. 45, pp. 399-431, 1999.

[6] S. Aji, H. Jin, R. J. McEliece, and D. MacKay, "BSC Thresholds for code ensembles based on 'Typical Pairs' Decoding, " submitted to *Proc. of IMA workshop 1999*.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Irregular Turbocodes

Brendan J. Frey, Computer Science, University of Waterloo, http://www.cs.uwaterloo.ca/~frey
David J. C. MacKay, Physics, Cambridge University, http://wol.ra.phy.cam.ac.uk/mackay

Abstract— **We construct irregular turbocodes with systematic bits that participate in varying numbers of trellis sections. By making the original rate 1/2 turbocode of Berrou *et al.* slightly irregular, we obtain a coding gain of 0.15 dB at BER = 10^{-4}.**

I. Irregular turbocodes

Recently, significant coding gains have been obtained by making the codeword bits of low density parity check codes participate in varying numbers of parity checks (c.f. [1, 2]).

What we call an *irregular turbocode* [3] has the form shown in Fig. 1, which is a type of "trellis-constrained code" [3]. One way to describe the code is by a *degree profile*, $f_d \in [0, 1], d \in \{1, 2, \ldots, D\}$, where f_d is the fraction of codeword bits that have degree d and D is the maximum degree. Each codeword bit with degree d is repeated d times before being permuted and connected to the trellis for a convolutional code. If the bits in the convolutional code are partitioned into "systematic bits" and "parity bits", then by connecting each parity bit to a degree 1 codeword bit, we can encode in linear time by copying, permuting and encoding the systematic bits.

The overall rate R of an irregular turbocode is related to the rate R' of the convolutional code and the average degree $\bar{d}$ by $\bar{d}(1 - R') = 1 - R$. So, if the average degree is increased, the rate of the convolutional code must also be increased (*e.g.*, by puncturing or redesign) to keep the overall rate constant.

II. Decoding irregular turbocodes

Fig. 1 can be interpreted as the graphical model (factor graph, Bayesian network, *etc.*) [4, 5] for the irregular turbocode. Decoding consists of applying the sum-product algorithm (a generalized form of turbodecoding) in this graph.

The decoder first computes the N channel output log-likelihood ratios $L_1^0, \ldots, L_N^0$, and then repeats each log-likelihood ratio appropriately. For bit i with degree d_i, set $L_{i,1} \leftarrow L_i^0, \ldots, L_{i,d} \leftarrow L_i^0$. Next, the log-likelihood ratios are permuted and fed into the BCJR algorithm for the convolutional code, which, for bit i, produces d *a posteriori* log-probability ratios, $L'_{i,1}, \ldots, L'_{i,d}$. The current estimate of the log-probability ratio for bit i is $\hat{L}_i \leftarrow L_i^0 + \sum_{k=1}^{d}(L'_{i,k} - L_{i,k})$. The inputs to the BCJR algorithm for the next iteration, are computed by subtracting off the corresponding outputs from the BCJR algorithm produced by the previous iteration: $L_{i,k} \leftarrow \hat{L}_i - L'_{i,k}$.

III. Discussion

Fig. 2 shows the simulated BER-E_b/N_0 curves for the original regular turbocode and an irregular turbocode that we came up with by making 5% of the codeword bits in the original turbocode have degree 10 The irregular turbocode clearly performs better than the regular turbocode for BER $> 10^{-4}$.

For high E_b/N_0, most of the errors for the irregular turbocode were due to low-weight codewords. Our permuter was drawn from a uniform distribution over permuters, but we expect the BER "flattening" effect can be significantly reduced by carefully designing the permuter and the convolutional code, possibly by extending the method of "density evolution" to convolutional codes. We are also studying ways of constraining the degree 1 "parity" bits (*i.e.*, increasing their degree) to eliminate low-weight codewords.

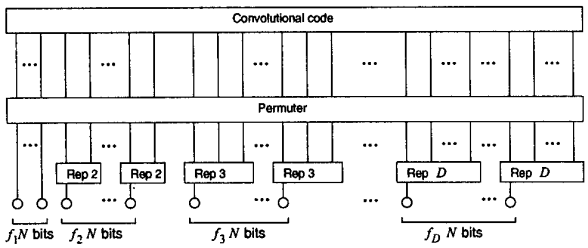


Figure 1: A general *irregular turbocode*. For $d = 1, \ldots, D$, fraction f_d of the codeword bits are repeated d times, permuted and connected to a convolutional code.

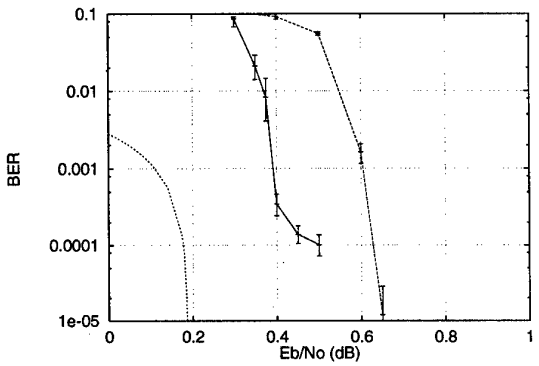


Figure 2: Performances of the original block length $N = 131,072$ turbocode (dashed line) and one of its irregular cousins (solid line).

For BER $> 10^{-4}$ this irregular turbocode performs in the same regime as the best known irregular Gallager code [2]. We expect the improvement in performance to be even more significant for lower-rate codes, since the constituent convolutional code can have lower-rate, thus eliminating many low-weight codewords while retaining the benefit of irregularity.

References

[1] D. J. C. MacKay, S. T. Wilson, and M. C. Davey, "Comparison of constructions of irregular Gallager codes," *IEEE Transactions on Communications*, vol. 47, October 1999.

[2] T. Richardson, A. Shokrollahi, and R. Urbanke, "Design of provably good low density parity check codes." Submitted to *IEEE Transactions on Information Theory*, July 1999.

[3] B. J. Frey and D. J. C. MacKay, "Irregular turbocodes," in *Proceedings of the 37th Allerton Conference on Communication, Control and Computing 1999*.

[4] B. J. Frey, *Graphical Models for Machine Learning and Digital Communication*. Cambridge MA.: MIT Press, 1998.

[5] F. R. Kschischang and B. J. Frey, "Iterative decoding of compound codes by probability propagation in graphical models," *IEEE Journal on Selected Areas in Communications*, vol. 16, pp. 219–230, February 1998.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Contradicting a Myth: Good Turbo Codes With Large Memory Order

Peter C. Massey
University of Notre Dame
email: pmassey@nd.edu

Oscar Y. Takeshita
Ohio State University
email: takeshita.3@osu.edu

Daniel J. Costello, Jr.[1]
University of Notre Dame
email: costello.2@nd.edu

Abstract —

The purpose of this paper is to contradict a common myth about turbo codes. We are specifically addressing $R = 1/3$ parallel-concatenated codes using systematic, recursive constituent codes.

Myth: Turbo codes constisting of constituent codes with large memory order (i.e., a large number of trellis states) are not as effective as the original Berrou-Glavieux-Thitimajshima turbo code [1] in the waterfall region of small signal-to-noise ratios (SNR's).

This myth is contradicted by a turbo code whose recursive constituent codes have 256 states. Decoding this turbo code with the BCJR APP decoder gives bit-error-rate (BER) and frame-error-rate (FER) performance better than the original (Berrou) turbo-code at all SNR's.

I. Summary

The iterative BCJR APP decoding algorithm [1] [2] permits relatively quick decoding of turbo codes. Although the decoding algorithm is suboptimal, it does perform very close to the optimal maximum likelihood (ML) decoder except at very small SNR's in the waterfall region. The iterative algorithm has difficulty starting the convergence toward a solution. The first decoding iteration(s) of the constituent codes must produce *a posteriori* estimates that are good enough *a priori* estimates to push the subsequent iterations towards the ML solution instead of stalling the convergence in some region of the solution space. In general, at very small SNR's, a systematic, recursive constituent code with short cycle length will produce better extrinsic APP estimates for the information bits than a code with a long cycle length. For example, the 8-state code below has a cycle length of 3 (where the parentheses just indicate the periodic cycles within the recursive portion of the impulse response):

$$\frac{[1+D+D^2+D^3]}{[1+D^3]} \triangleq \frac{[1111]}{[1001]} \quad \Rightarrow \quad 1(110)(110)\ldots \ .$$

The single one bit, out in front, can be considered as the feedforward portion of the impulse response. A turbo code using this constituent code does give good extrinsic estimates at the start of the iterative decoding algorithm at very small SNR's (hence it starts to diverge away from the starting point), however it has difficulty finishing the convergence to the ML solution. We can "strengthen" the constituent code while retaining the short cycle length by increasing the complexity of the feedforward portion of the impulse response. Consider the code:

$$\frac{[110000011]}{[111]} \quad \Rightarrow \quad 1011011(110)(110)\ldots \ .$$

[1]This work was supported by NASA Grants NAG5-557 and NAG5-8355 and by NSF Grant NCR95-22939.

We call this a Big Numerator-Little Denominator (BN-LD) code. It is described by a trellis with 256 states. The turbo code using this 256-state constituent code has an improved ability to finish the convergence to the ML solution compared to the previous 8-state code with a single one in the feedforward portion. However, analogous to feedforward convolutional codes, the increased complexity of the feedforward portion of the impulse response does somewhat reduce the convergence start-up ability that is due to the short cycle length. See Fig.1 for BER and FER performance simulations of this 256-state BN-LD turbo code compared to the (Berrou) code.

The feedforward portion of the BN-LD code was not picked at random, but rather specifically designed to produce an additional "thinning" of the closest codewords due to weight-2 inputs. This is a new degree of freedom that can be exploited to give a new distance profile for the lowest weight codewords.

A useful application of BN-LD codes is as a replacement for the accumulator code, $[1, \frac{[1]}{[11]}] \Rightarrow (1)(1)(1)\ldots$, which is used in serial concatenation and other schemes [3]. The BN-LD accumulator code has the form $[1, \frac{[n(D)]}{[1+D]}]$ where the order of the numerator polynomial $n(D)$ is two or greater. For example, the code $[1, \frac{[10011]}{[11]}] \Rightarrow 1110(1)(1)(1)\ldots$ has a better ability to finish converging to the ML solution compared to the standard accumulator code.

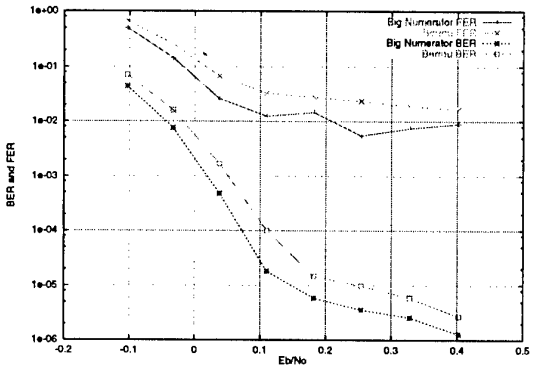


Figure 1: Simulation results for the rate-$\frac{1}{3}$, 256-state BN-LD turbo code (labeled "Big Numerator") and the Berrou turbo code. (The interleaver frame size is 16,384; and 18 iterations are used.)

References

[1] C. Berrou, A. Glavieux, and P. Thitimajshima,"Near Shannon limit error-correcting coding and decoding: turbo-codes," *Proc. IEEE Int. Conf. on Commun.*, pp. 1064-1070, May, 1993.

[2] L.R. Bahl, J. Cocke, F.Jelinek, and J. Raviv,"Optimal decoding of linear codes for minimizing symbol error rate," *IEEE Trans. Inform. Theory*, pp. 284-287, March, 1974.

[3] D. Divsalar, H. Jin, and R. McEliece,"Coding theorems for 'turbo-like' codes",*Proc. 1998 Allerton Conf.*,pp. 201-210.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Chaotic Turbo Codes

S. Adrian Barbulescu and Andrew Guidi
Institute for Telecommunications Research
University of South Australia
Mawson Lakes SA 5095
e–mail: adrian.barbulescu@unisa.edu.au
Steven S. Pietrobon
Small World Communications
e–mail: steven@sworld.com.au

Abstract – This paper describes a new class of codes, chaotic turbo codes. They were born from a symbiosis between a chaotical digital encoder and a turbo code. This paper investigates the most important properties of both chaotic digital encoders and turbo encoders in order to understand how the two complement each other. A Chaotic Turbo Encoder is then described and initial results will be presented.

I. Introduction

A chaotic digital encoder was defined for the first time in [1] as a non–linear digital filter with finite precision (8 bits) which behaves in a quasi–chaotic fashion, both with zero and nonzero input sequences. A simple chaotic encoder is shown in Figure 1 [1].

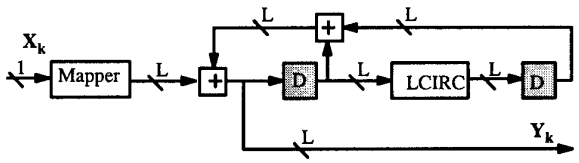


Figure 1: Chaotic Digital Encoder

The main features of chaotic digital encoders that are used in this paper are:

- The system is digital which makes possible its integration with a turbo code.
- The output of a chaotic digital encoder with arbitrary inputs has a broadband noiselike spectrum.
- The auto correlation function of the output is similar to an uncorrelated noise sequence.
- The outputs of a chaotic digital encoder with almost all arbitrary inputs are uncorrelated to the input for almost all choices of initial conditions.
- The outputs of a chaotic digital encoder with the same input sequences are uncorrelated to one another for almost all choices of different initial conditions.
- For almost all choices of input for two identical chaotic digital encoders having different but arbitrarily close initial states, the states of the two encoders will diverge.

Another important result in this area is that chaotic circuits taken from an appropriate class can be made to synchronise. It has been shown that a chaotic system, in the presence of a continuous perturbation, is able to asymptotically track a replica of itself if it can be decomposed into subsystems with stable Lyapunov exponents. Binary digits, X_k, are presented one at a time to the encoder and mapped onto either 0 or $2^{(L-1)}$. The additions are on L bits and the arithmetic is modulo 2^L. The non–linear map is the LCIRC bloc which performs a rotate left operation. There are only two delay elements (D) in the encoder, of L bits each. Each encoder output, Y_k, is L bits wide and can modulate one or more pulses.

II. Chaotic Turbo Encoder

The chaotic digital encoder shown in Figure 1 could replace the recursive systematic encoder used in a turbo code [2]. The key element in a turbo encoder is the interleaver. The role of the interleaver is to feed into the second encoder the same data but in a different random order, such that at the receiving end, each decoder to be able to make "independent" decisions for the same data bit. A similar effect to interleaving can be achieved with the chaotic digital encoder if the initial states are different. Both encoders use feedback registers, one using binary data, the other L–tuples. The advantage of using a chaotic encoder in a turbo encoder consists in the possible elimination of the interleaver, therefore reducing delay in the system. The only difference appears in the non–linearity inserted in the chaotic digital encoder.

II. Conclusions

The paper described a chaotic turbo encoder. Simulation of the new Chaotic Turbo Codes are expected to show an improvement on the results reported in [3], which are based on a decision directed state feedback decoder. Similar work in the area of secure communication using chaotic signals without coding was reported in [4] for both AWGN and mobile channels. The use of turbo codes might prove a key element in reducing the high signal–to–noise ratios required by chaotical systems.

References

1. D. R. Frey, "Chaotic digital encoding: an approach to secure communications," *IEEE Transactions on Circuits and Systems*, vol. 40, no. 10, pp. 660–666, Oct. 1993.
2. C. Berrou, A. Glavieux and P. Thitimajshima, "Near Shannon limit error–correcting coding and decoding: turbo–codes," *ICC 1993*, Geneva, Switzerland, pp. 1064–1070, May 1993.
3. T. Aislam and J. A. Edwards, "Secure communications using chaotic digital encoding," Electronics Letters, vol. 32, no. 3, pp. 190–191, Feb. 1996.
4. J. Lee, S. Choi and D. Hong, "Secure Communication using a Chaos System in a Mobile Channel," GLOBECOM'98, pp. 2520–2525, Sydney, Australia, Nov. 1998.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

The Index Entropy in Mismatched Lossy Source Coding

Ram Zamir[1]
Dpt. of EE-Systems,
Tel Aviv University,
Tel Aviv 69978 ISRAEL
e-mail: zamir@eng.tau.ac.il

Abstract — **If a random codebook for lossy source coding is generated by a non-optimum reproduction distribution Q, then the entropy of the index of the D-matching codeword is reduced by conditioning on the codebook: the number of bits saved is equal to the divergence between the "favorite type" in the codebook and the generating distribution Q.**

I. Statement of Main Result

Consider coding a source word $\mathbf{X} = X_1...X_l$, generated i.i.d. by a distribution P over a finite alphabet $\mathcal{X}$, into a code word $\mathbf{Y} = Y_1...Y_l$ ("reconstruction") from a finite alphabet $\mathcal{Y}$, under the distortion constraint $d(\mathbf{X},\mathbf{Y}) \triangleq 1/l \sum_i d(X_i,Y_i) \leq D$. As shown in [1], if a codebook $\mathbf{Y}_1, \mathbf{Y}_2, ...$ of words in $\mathcal{Y}^l$ is generated i.i.d. according to a distribution Q, and if we denote by N_ℓ the index of the first codeword that satisfies the distortion constraint, then

$$\frac{1}{l}\log(N_l) \to R(P,Q,D) \text{ in probability,} \qquad (1)$$

where the constant $R(P,Q,D)$ is given by, [2],

$$R(P,Q,D) = \min_{Q'}\Big\{ I_m(P\|Q',D) + D(Q'\|Q)\Big\}. \qquad (2)$$

Here $D(\cdot)$ denotes divergence (or relative entropy), and the function I_m denotes the "lower mutual information" $I_m(P\|Q,D) = \min_W I(P,W)$, where $I(P,W)$ denotes the mutual information associated with input distribution P and transition distribution W from $\mathcal{X}$ to $\mathcal{Y}$, and the minimization is taken over all W's such that the input P induces output distribution Q and average distortion less than or equal to D (if no such W exists then $I_m(P\|Q,D)$ is equal to infinity). The "mismatched" coding rate function $R(P,Q,D)$ is greater than or equal to the rate distortion function of the source, with equality if and only if Q is an optimum reproduction distribution which realizes the rate distortion function.

It was further shown in [2] that for large word length, the random type T_{N_l} of the D-matching codeword Y_{N_l} concentrates around a limiting distribution:

$$T_{N_l} \to Q^*_{P,Q,D} \text{ as } l \to \infty \text{ in probability,} \qquad (3)$$

where $Q^*_{P,Q,D}$ is the distribution Q' which achieves the minimum in (2). This distribution, called "the favorite type" (although $Q^*_{P,Q,D}$ is in general not an l-type), strikes the optimum balance between covering efficiency and frequency in the codebook. It follows from (3) that most of the first $2^{lR(P,Q,D)}$ codewords in the codebook are asymptotically useless; only those having a type close to $Q^*_{P,Q,D}$ - whose fraction in the codebook is only $\approx 2^{-lD(Q^*_{P,Q,D}\|Q)}$ - have a good chance to be the first to D-match the source word. In a sense, we are paying extra $D(Q^*_{P,Q,D}\|Q)$ bits in coding rate. Our main result shows that this redundancy can be removed by entropy coding conditioned on the codebook.

Theorem 1 *If Q is positive everywhere, then*

$$\lim_{l\to\infty}\frac{1}{l}H(N_l|\mathbf{Y}_1,\mathbf{Y}_2,...) \;=\; I_m(P\|Q^*_{P,Q,D},D). \qquad (4)$$

Note that without conditioning on the codebook, the index N_l is approximately uniformly distributed over the range $(1...2^{lR(P,Q,D)})$, so its entropy is equal to $R(P,Q,D)$.

II. Example

Assume $\mathcal{X} = \mathcal{Y} = \{0,\ldots,|\mathcal{X}|-1\}$. Consider a uniform codebook generating distribution $Q(y) = 1/|\mathcal{Y}|\ \forall y$, and a symmetric distortion measure of the form $d(x,y) = d(y-x)$, where the subtraction is modulo-$|\mathcal{X}|$. Then

$$R(P,Q,D) = \log|\mathcal{X}| - H_{max}$$

and

$$Q^*_{P,Q,D} = P * V^*\ ;$$

hence the conditional index entropy (4) is given by

$$I_m(P\|Q^*_{P,Q,D},D) = H(P*V^*) - H_{max},$$

where H_{max} and V^* denote the maximum-entropy under a D-constraint and the maximum-entropy achieving distribution, respectively:

$$H_{max} = H(V^*) = \max_{V:\ \sum_y V(y)d(y)\leq D} H(V)\ ,$$

and the $*$ sign denotes a circular convolution (i.e., $P*V^*$ is the distribution of the independent sum of a random variable $\sim P$ and a random variable $\sim V^*$).

A generalization of this work to the continuous case links the conditional entropy (4) with the entropy of dithered lattice quantizers.

Acknowledgments

I thank Y. Kontoyiannis for the discussion that motivated this result, and T. Linder, K. Rose and U. Erez for helpful comments.

References

[1] En-Hui Yang and John Kieffer. On the performance of data compression algorithms based upon string matching. *IEEE Trans. Information Theory*, IT-44:47–65, Jan. 1998.

[2] R. Zamir and K. Rose. A string-matching interpretation for the Arimoto-Blahut algorithm. In *Proc. of the Sixth Canadian Workshop on Information Theory, Kingston, Ontario*, page pp. 48, June 1999.

[1]This work was supported in part by the BSF grant no. 9800309.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

A Zero-Delay Sequential Quantizer for Individual Sequences

Tamás Linder
Dept. of Mathematics & Statistics
Queen's University
Kingston, Ontario
Canada K7L 3N6
email: linder@mast.queensu.ca

Gábor Lugosi
Department of Economics
Pompeu Fabra University
Ramon Trias Fargas 25-27 08005
Barcelona, Spain
email: lugosi@upf.es

Abstract — **We consider adaptive sequential lossy coding of bounded individual sequences. The encoder and the decoder are connected via a noiseless channel of capacity R and both are assumed to have zero delay. No probabilistic assumptions are made on how the sequence to be encoded is generated. For any bounded sequence of length n, the distortion redundancy is defined as the normalized cumulative squared distortion of the sequential scheme minus the normalized cumulative squared distortion of the best scalar quantizer of rate R which is matched to this particular sequence. We demonstrate the existence of a zero-delay sequential scheme which uses common randomization in the encoder and the decoder such that the normalized maximum distortion redundancy converges to zero at a rate $n^{-1/5}\log n$.**

I. Summary

A (randomized) zero-delay sequential source code of rate $R = \log M$ is described by an encoder-decoder pair which are connected via a noiseless channel of capacity R. It is assumed that both the encoder and the decoder have access to a common sequence of random variables $\{U_i\}_{i=1}^{\infty}$, where each U_i is uniformly distributed on the interval $[0,1]$. The input to the encoder is a sequence of real numbers $x_1, x_2, \ldots$ assumed to be bounded such that $x_i \in [0,1]$ for all $i \geq 1$. At each time instant $i = 1, 2, \ldots$, the encoder observes x_i and the random number U_i. Based on x_i, U_i, and the past input values $x^{i-1} = (x_1, \ldots, x_{i-1})$, the encoder produces a channel symbol $y_i \in \{1, 2, \ldots, M\}$ which is then transmitted to the decoder. After receiving y_i, the decoder outputs the reconstruction value $\widehat{x}_i$ based on U_i and the channel symbols $y^i = (y_1, \ldots, y_i)$ received so far.

More formally, the code is given by a sequence of encoder-decoder functions $\{f_i, g_i\}_{i=1}^{\infty}$, where

$$f_i : [0,1]^i \times [0,1] \to \{1, 2, \ldots, M\}$$

and

$$g_i : \{1, 2, \ldots, M\}^i \times [0,1] \to [0,1].$$

so that $y_i = f_i(x^i, U_i)$ and $\widehat{x}_i = g_i(y^i, U_i)$, $i = 1, 2, \ldots$. Note that there is no delay in the encoding and decoding process. Zero-delay schemes have an obvious advantage over other coding methods (such as block codes) in applications where decoding delay is a crucial factor.

The *normalized cumulative squared distortion* of the sequential scheme at time instant n is given by

$$D_n(x^n) = \frac{1}{n}\sum_{i=1}^{n}(x_i - \widehat{x}_i)^2$$

where the dependence of D_n on the randomizing sequence is suppressed in the notation. The expected cumulative distortion is $\overline{D}_n(x^n) = E\big[D_n(x^n)\big]$, where the expectation is taken with respect to the randomizing sequence $U^n = (U_1, \ldots, U_n)$.

Let $\mathcal{Q}$ denote the collection of all M-level scalar quantizers over $[0,1]$. For any sequence x^n, let $D_n^*(x^n)$ denote the minimum normalized cumulative distortion in quantizing x^n with an M-level scalar quantizer, that is, let

$$D_n^*(x^n) = \min_{Q \in \mathcal{Q}} \frac{1}{n}\sum_{i=1}^{n}(x_i - Q(x_i))^2.$$

Note that to find a $Q \in \mathcal{Q}$ achieving $D_n^*(x^n)$ one has to know the entire sequence x^n in advance. The next theorem asserts that there exists a zero-delay sequential source code of rate R which, for any bounded input sequence, performs asymptotically as well as the best scalar quantizer of rate R matched to the entire sequence.

Theorem 1 *For any $R = \log M$ there exists a randomized zero-delay sequential source code $\{f_i, g_i\}_{i=1}^{\infty}$ of rate R whose expected normalized cumulative distortion $\overline{D}_n(x^n)$ satisfies, for all $x^n \in [0,1]^n$,*

$$\overline{D}_n(x^n) - D_n^*(x^n) \leq Cn^{-1/5}\log n,$$

where C is a constant independent of n and x_1^n. In particular,

$$\limsup_{n\to\infty} \max_{x^n \in [0,1]^n} \left(\overline{D}_n(x^n) - D_n^*(x^n)\right) \leq 0.$$

The construction of the coding scheme in the theorem uses an appropriately modified version of the exponential weighting method of Vovk [1] in which the class of "experts" is a finite set of judiciously chosen reference quantizers. Ideally, the cumulative losses of these experts should be used to form the weights in the exponential weighting scheme. A substantial difficulty is that these losses are not available at the decoder since (unlike in sequential lossless coding) the decoder does not have access to the past source outputs. We overcome this problem by periodically transmitting approximate versions of the cumulative losses of the reference quantizers. We show that using only a small fraction of the overall available rate to transmit the approximate cumulative losses, the proposed scheme does asymptotically as well as a hypothetical scheme in which the decoder has full access to the cumulative losses of the reference quantizers (such a scheme requires a channel of infinite capacity).

References

[1] V. Vovk, "Aggregating strategies," in *Proceedings of the 3rd Annual Workshop on Computational Learning Theory*, pp. 372–383, 1990.

This research was supported in part by the Natural Sciences and Engineering Research Council (NSERC) of Canada and DGES grant PB96-0300.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

The Redundancy of Successive Refinement Codes and Codes with Side Information

German Voronov and Meir Feder[1]
Department of EE-Systems
Tel-Aviv University
Tel-Aviv, 69978, Israel
e-mail:[voron,meir]@eng.tau.ac.il

Abstract — **In this work we consider the problem of determining the redundancy of successive refinement codes and codes with side information, as a function of their blocklength. It is shown that successive refinement codes accumulate an $O(\log n/2n)$ redundancy term at each stage of the encoding process, which may result in a considerable degradation of the final description. Redundancy result for codes with side information is also presented.**

I. Introduction

The redundancy of a code is the difference between the average performance of the code and the theoretically expected performance. A smaller redundancy is achieved as the blocklength increases. However, the increase of the block length results in an exponential increase in coding complexity. Therefore, it is interesting to study the tradeoff between the redundancy and computational complexity.

In a lossy source coding the redundancy of a code at rate R is the difference between its average distortion and the distortion-rate function. Originally, the redundancy problem in the lossy source coding was considered by Pilc.However, only a few years ago, the problem was finally solved by Zhang *et al.*[2]. It has been shown that in the coding of a discrete memoryless source $\{X_i\}_{i=0}^{\infty}$, $X \sim p_X$, the distortion redundancy of a code with a fixed blocklength n, is $|\partial_R d(p_X, R)| \ln n/2n + o(\ln n/n)$, where $\partial_R d(p_X, R)$ is the partial derivative evaluated at R and assumed to exist.

II. Main Results

The Redundancy of Successive Refinement Codes

Successive refinement is a coding method that progressively improves previously obtained descriptions of the original data using additional information. The problem arises in a variety of applications, where coarse representation of data is always transmitted, and occasionally, finer reproduction is required. Furthermore, successive refinement scheme is also a technique for fast encoding since it possesses a tree structure. A Tree Structured Vector Quantizer (TSVQ) may be constructed following the successive refinement approach, which reduces exponentially the computational complexity. Moreover, it seems that for successively refinable source[1], there is no penalty due to the multi-stage encoding. Nevertheless, even for successively non-refinable sources this technique is still computationally efficient. Now it is clear that the investigation of the redundancy aspect is crucial for a performance estimation of the successive refinement codes as well as for analyzing fast encoding schemes such as TSVQ.

The i-th stage redundancy of an optimal K-stage successive refinement code[2] is given by the following theorem.

Theorem 1 *: Let $R_i > 0$ be the rate of stage i, $i = 1 \ldots K$. For any discrete memoryless source $X \sim p_X$ and K distortion levels $d_1 > \ldots > d_K > 0$, the distortion redundancy of a stage i, associated with an optimal code scheme, is*

$$\mathcal{D}_i(p_X, R_1, R_2, \ldots, R_K, n) = \sum_{j=1}^{i} \left| \frac{\partial}{\partial R_j} d_K(p_X, R_1, R_2, \ldots, R_K) \right| \frac{\ln n}{2n} + o\left(\frac{\ln n}{n}\right),$$

where blocklength n is sufficiently large.

The Redundancy of Codes with Side Information

Another closely related problem, is the redundancy problem of codes with side information. It arises when there exists a joint source (X, Y), where X is referred to as the source, while Y is referred to as the side information and available at the decoder. The decoder reproduces the source using the knowledge of the side information. The redundancy of an optimal code with side information is given by the following theorem.

Theorem 2 *: Let $R_y > 0$ be the rate of the code. For any joint discrete memoryless source $(X, Y) \sim p_{XY}$ and a distortion level $d_y > 0$, the distortion redundancy associated with an optimal side information code operating at rate R_y is*

$$\mathcal{D}_y(p_{XY}, R_y, n) = \left| \frac{\partial}{\partial R_y} d_y(p_{XY}, R_y) \right| \frac{\ln n}{2n} + o\left(\frac{\ln n}{n}\right),$$

where blocklength n is sufficiently large.

III. Conclusion

An interesting consequence of our result is that any multistage encoding scheme will accumulate the redundancy at each stage, which may lead to a significant increase in the overall distortion. An important example of this phenomenon is TSVQ. Practical implementations of TSVQ show that it can never achieve the performance of a block code, even for successively refinable sources. Until this work there was no theoretical understanding of this fact.

References

[1] W. H. R. Equitz and T. M. Cover, "Successiver refinement of information," *IEEE Trans. Inform. Theory*, vol. IT-37, pp. 269-274, 1973.

[2] Z. Zhang, E.-H. Yang and V. Wei, "The Redundancy of Source Coding with a Fidelity Criterion - Part One : Known Statistics," *IEEE Trans. Inform. Theory*, vol. IT-43, pp.71-91, 1997.

[1]This work was supported in part by a Grant from the Israel Science Foundation.

[2]The optimal K-stage code is a coding scheme that is optimal code with respect to all representations.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

All Sources Are Nearly Successively Refinable

Luis Lastras[1]
School of Electrical Engineering
Cornell University
Ithaca, NY, 14853
e-mail: lastras@ee.cornell.edu

Toby Berger[2]
School of Electrical Engineering
Cornell University
Ithaca, NY, 14853
e-mail: berger@ee.cornell.edu

Abstract — **Given an achievable quadruple (R_1, R_2, D_1, D_2) for successive refinement with $D_2 < D_1$, the rate loss at step i is defined as $L_i = R_i - R(D_i)$. It is shown that for a memoryless source and for MSE, an achievable quadruple can be found such that $L_i \leq 1/2$ bit. Moreover, an achievable quadruple can be found with L_2 arbitrarily small and $L_1 \leq 1/2$ bit if D_2 is small enough. If an information-efficient description at D_1 is required (i.e. $L_1 = 0$), then there exists an achievable quadruple with $L_2 \leq 1$ bit. The results are independent of both the source and the particular D_1, D_2 requirements and extend to any difference distortion measure. The techniques employed parallel Zamir's bounding of the rate loss in the Wyner-Ziv problem.**

I. Introduction

If one can design two-step compression systems that incur no rate loss relative to optimal one-step coding, (i.e. if there is an achievable quadruple $(R_1, R_1 + \Delta R, D_1, D_2)$ such that $R_1 = R(D_1)$ and $\Delta R = R(D_2) - R(D_1)$), the source is said to be *successively refinable* (SR) [1]. In [2] Koshelev introduced the notion of *divisibility*, and argued that successive refinement is possible if there exists a channel $Q_{U_2,U_1|X}$ such that i) the random variables U_1 and U_2 defined through this channel achieve the rate-distortion function of X at distortions D_1 and D_2, respectively, and ii) the Markov relation $X \longrightarrow U_2 \longrightarrow U_1$ is satisfied. Necessity was later proved by Equitz and Cover [1], who also used the Gerrish problem an example of a non-SR source with discrete alphabet.

Rimoldi [3] determined the achievable region for two-step compression of a discrete-alphabet memoryless source. In a subsequent paper, Effros [4] extended Rimoldi's results to handle stationary sources and Polish alphabets.

Given an achievable quadruple (R_1, R_2, D_1, D_2), we define the rate loss of at the ith stage as

$$L_i = R_i - R(D_i), \quad i \in \{1, 2\}$$

Let D_1 and D_2 be fixed (with $D_2 < D_1$). For a successively refinable source, there exists an achievable quadruple for which $L_1 = 0$ and $L_2 = 0$. For a non-successively refinable source, it is not possible to find achievable quadruples for which L_1 and L_2 are zero simultaneously. It is clear that it is important to investigate whether L_1 and L_2 can be made small simultaneously for any given source. Effros [4] computed for the Gerrish problem that the smallest possible rate loss L_2 when forcing $L_1 = 0$ is a relatively small fraction of a bit for a fixed D_1 as D_2 varies.

In this paper we provide source-independent bounds for the rate loss at both stages. The main result is that for squared error as the distortion measure, it is always possible to find an achievable quadruple for which the rate loss satisfies $L_1 \leq 1/2$ bit and $L_2 \leq 1/2$ bit, a result which is independent of the source and D_1, D_2 requirements.

II. Summary of results

We assume that D_1 and D_2 are some fixed distortion requirements satisfying $D_2 < D_1$. We will also assume an MSE distortion measure.

Theorem 1 *There exists an achievable rate pair (R_1, R_2) with $L_i = R_i - R(D_i) \leq 1/2$ bit, $i \in \{1, 2\}$.*

Theorem 2 *Let D_1 be fixed and let $D_2^k \longrightarrow 0$ as $k \longrightarrow \infty$. There exists a sequence of achievable quadruples $\{(R_1^k, R_2^k)\}_{k=1}^{\infty}$ with $L_1^k \leq 1/2$ bit and $\lim_k L_2^k = 0$.*

Theorem 3 *There exists an achievable rate pair (R_1, R_2) with $L_1 = 0$ and $L_2 \leq 1$ bit.*

Theorem 4 *Let the iid source $\{X_i\}_{i=1}^{\infty}$ have variance σ_X^2. There exists an achievable rate pair (R_1, R_2) for which*

$$L_i \leq \frac{1}{2}\log_2\left(2 - \frac{D_i}{\sigma_X^2}\right) \text{ bits}, \quad i \in \{1, 2\}.$$

Theorem 5 *Let the iid source $\{X\}_{i=1}^{\infty}$ have mean μ_X and variance σ_X^2 and let $X^* \sim \mathcal{N}(\mu_X, \sigma_X^2)$. There exists an achievable rate pair (R_1, R_2) with $L_i \leq D(X\|X^*)$, $i = 1, 2$.*

Acknowledgments

The authors wish to thank Ram Zamir who, after seeing our Theorem 1, suggested the ideas behind Theorems 2 and 5. We also thank Ying-On Yan for his careful reading of a draft of this manuscript.

References

[1] W.H. Equitz, T. Cover, "Successive Refinement of Information," *IEEE Trans. Inform. Theory*, 37(2), pp. 269–275, March 1991.

[2] V. Koshelev, "Hierarchical Coding of Discrete Sources," *Probl. Pered. Inform.*, 16(3), pp. 31–49, 1980.

[3] B. Rimoldi, "Successive Refinement of Information: Characterization of the achievable rates," *IEEE Trans. Inform. Theory*, 40(1), pp. 253–259, January 1994.

[4] M. Effros, "Distortion-rate bounds for fixed- and variable-rate multiresolution source codes", *IEEE Trans. Inform. Theory*, 45(6), pp. 1887–1910, September 1999.

[1]This work was partially supported by a CONACYT (MEXICO) doctoral grant (110412/110461)

[2]This work was partially supported by NSF Grant CCR-9632266.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

A Broadcast Approach for the Multiple-Access Slow Fading Channel

Shlomo Shamai (Shitz)
EE Dept., Technion
Haifa 32000, Israel, sshlomo@technion.ac.il

Abstract — **A 'single-user' based broadcast approach is adapted for the multiple access very slow fading channel. This strategy facilitates to adapt the reliably conveyed rate to the actual channel conditions experienced by each of the users without having any feedback links to the transmitters. This strategy implements simultaneously a continuum of capacity regions vs. outage pairs rather than a single value as is the case in the standard approach. We address specifically expected rates and outages, which are compared to ergodic capacities and also the capacity vs. outage. The main results presented and demonstrated for the two-user independent Rayleigh faded channel, are extended to the general multiple access slowly fading channel.**

I. Model, Assumptions and Preliminaries

We address here the standard Multiple Access Channel (MAC) model subjected to a static fading, which is not necessarily independent among the K-users. Complex notations are used throughout. Here y_i, the received signal at a discrete time instant-i, $i = 1, 2 \ldots N$, equals $y_i = \sum_{l=1}^{K} \rho_{il} x_{il} + n_i$. The i-th coded symbol of the l-th user is designated by x_{il} and n_i stands for the i-th iid additive Gaussian noise sample with variance $E|n|^2 = 1$. The fading power associated with user l is designated by $s_{il} = |\rho_{il}|^2$, $l = 1, 2, \ldots, K$, and is assumed to be static ($s_{il} = s_l$). The realizations of the fading coefficients $\{\rho_{il}\}$ are not available to the transmitters or the receiver, which are aware though of the underlying statistical law only. We adhere henceforth to the single block fading channel model where the block length, $N \gg K$, giving rise to equal achievable rates for channel state information available or not at the receiver.

In parallel to the single-user case [1], the capacity vs. outage for a K user system is associated with the event of $(s_1, s_2, \ldots, s_K)$ satisfying simultaneously the multiuser equation set for achievable rates where the signal to noise ratio reflects also the interference emerging from those users who do not belong to the decodable set [2]. The availability probability is associated with the simultaneous satisfaction of the equation set and outages are associated with the complimentary event. For equal rates these probabilities for a two user and many user case has been investigated in [2]. Clearly, expected rates are naturally associated to outage probabilities.

II. The Broadcast Approach Channel

Single-User: Assume now that the fading power random variable s is continuous and let $R(s)$ stand for the reliably conveyed information rate at fading level s which designates a certain realization of the fading (power) random variable. The transmitter views the fading channel as a degraded Gaussian broadcast channel with a continuum of receivers each experiencing a different signal-to-noise ratio specified by $s \cdot \mathrm{SNR}$. The receiver which experiences a realization s is able to decode its own data stream (indexed by s) and all those streams indexed by $u \leq s$ (intended to be decoded at receivers with lower signal-to-noise ratios $u\,\mathrm{SNR}$). Within this framework in [3] the achievable rates, expected rates and outages have been studied and the power assignment $\nu(s)$ has been optimized.

Two-Users: Let ω_k stand for the effective SNR of user $k = 1, 2$. It can be shown that $\{\omega_k\}$ is given by the solution of the equation pair $\omega_1 = \frac{s_1}{1+s_2\, y_2(\omega_2)}$, $\omega_2 = \frac{s_2}{1+s_1\, y_1(\omega_1)}$, where $y_k(s) = \int_s^\infty \nu_k(u)\, du$, $k = 1, 2$. We express $\omega_1 = \omega_1(s_1, s_2)$, $\omega_2 = \omega_2(s_1, s_2)$ as explicit functions of the actual fading realizations (s_1, s_2) for specified power assignments $\nu_1(s)$, $\nu_2(s)$. The simultaneously achievable rates of each of the users $R_1(s_1, s_2)$, $R_2(s_1, s_2)$ respectively depend now on both fading realizations s_1 and s_2, and are given by $R_k(s_1, s_2) = \int_0^{\omega_k(s_1, s_2)} \frac{-u dy_k(u)}{1+u y_k(u)}$, $k = 1, 2$. The expected rates are now $R_{kT} = \mathbb{E}(R_k(s_1, s_2)) = \int_0^\infty \Big(1 - F_{\omega_k}(u)\Big) \frac{-u dy_k(u)}{1+u y_k(u)}$, where $F_{\omega_k}(u)$ designates the probability distribution of the random variable $\omega_k(s_1, s_2)$. Also here the functions $y_1(u)$, $y_2(u)$ can be optimized as to maximize the expected rates, or the total expected throughput $R_{1T} + R_{2T}$. In parallel to the single user case, also here expected rates per outages can be considered by replacing the original probability distribution of the fading powers $F_{s_1, s_2}(\alpha, \beta)$ by $F^{\mathbf{s}_0}_{s_1, s_2}(\alpha, \beta)$ the conditional distribution function of s_1, s_2, conditioned on the event s_1, $s_2 \notin \mathbf{s}_0$, where the associated outage probability is Prob $(s_1, s_2 \in \mathbf{s}_0)$. A natural candidate for a suboptimal symmetric power distribution for the two-user case is a modification of the optimal single-user distribution found in [3].

K-Users: extends straightforwardly to the general K-user case. Let now $k = 1, 2, \ldots, K$, where $\nu_k(s)$ stands for the power distribution of the k-th user – all subjected to the same average power constraint, SNR. The strategy induces a set of K-nonlinear equations $\omega_k = s_k(1 + \sum_{l=1(1\neq k)}^{K} s_l y_l(\omega_l))^{-1}$.

The achievable rates associated with user k for a given realization of $\mathbf{s} = (s_1, s_2, \ldots, s_K)$ and the expected rates are still given by the former single-user based equations with $w_k = w_k(\mathbf{s})$. The results assume a compact form for large systems, $K \gg 1$. The general approach does not demand, in fact, independence among the fadings affecting all the users, making the current approach and analysis rather general and robust. Some interesting examples related to a variety of interference type channels are explored.

References

[1] E. Biglieri, J. Proakis and S. Shamai (Shitz), "Fading Channels: Information-Theoretic and Communications Aspects," *Trans. Inform. Theory*, Vol. 44, No. 6, pp. 2619–2692, October 1998.

[2] S. Shamai (Shitz) and I. Bettesh, "Outages, Expected Rates and Delays in Multiple-Users Fading Channels," *CISS'00*, Princeton, March 15–17, 2000, pp. WA4-7–WA4-15.

[3] S. Shamai (Shitz), "A Broadcast Strategy for the Gaussian Slowly Fading Channel," *IEEE Int. Symp. Inform. Theory (ISIT'97)*, p. 150, Ulm, Germany, June 29–July 1, 1997.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Multiuser Capacity in Block Fading with no Channel State Information

Shlomo Shamai (Shitz)[1]
Department of Electrical Engineering
Technion—Israel Inst. of Techn.
Haifa 32000, Israel
sshlomo@ee.technion.ac.il

Thomas L. Marzetta
Mathematical Sciences Research Center
Bell Labs, Lucent Technologies
Murray Hill, NJ 07974-0636, USA
tlm@research.bell-labs.com

Abstract — **Consider M independent users, each user having his own transmit antenna, that transmits simultaneously to one receiver antenna through a Rayleigh block-fading channel having a coherence interval of T symbols, with no channel state information available to either the transmitters or to the receiver. The total transmitted power is independent of the number of users. For a given coherence time T, we wish to identify the best multi-access strategy that maximizes the total throughput, where all users are subjected to the same average power constraint.**

If perfect channel state information were available to the receiver, it is known that the total capacity increases monotonically with the number of users. If the channel state information is available to both the receiver and all transmitters, the throughput maximizing strategy implies that only a single user that enjoys the best channel condition transmits. In the absence of any channel state information one is forced to a radically different conclusion. In particular we show that if the propagation coefficients take on new independent values for every symbol (e.g., $T = 1$) then the total capacity for any $M > 1$ users is equal to the capacity for $M = 1$ user, in which case TDMA is an optimal scheme for handling multiple users. This result follows directly from a recent treatment of the single-user multiple antenna block-fading channel.

Again, motivated by the single-user results, one is lead to the following conjecture for the multiple user case: for any $T > 1$ the maximum total capacity can be achieved by no more than $M = T$ users. The conjecture is supported by establishing the asymptotic result that, for a constant M/T for large T, the total capacity is maximized when $M/T \to 0$, which yields a total capacity per symbol of $\log(1+\rho)$, where ρ is the expected SNR at the receiver.

I. Signal Model

We use a block-fading model [1], with coherence interval T, where M independent users simultaneously transmit to a single receiver antenna in a flat-fading environment, where each user has sole access to one of M transmit antennas, and where nobody has any CSI. During each coherence interval, the M users collectively transmit a $T \times M$ complex matrix S, whose columns are statistically independent, and the receiver records a $T \times 1$ complex vector X,

$$X = \sqrt{\frac{\rho}{M}} SH + W, \tag{1}$$

where H is the $M \times 1$ complex-valued propagation vector, and W is a $T \times 1$ vector of additive receiver noise. All components of H and W are independent Gaussian CN(0, 1). The expected SNR is equal to ρ, subject to the power constraint,

$$\mathrm{tr}\,\mathrm{E}\left\{SS^\dagger\right\} = T\,M. \tag{2}$$

Our goal is to maximize mutual information $I(X;S)$, without any CSI, subject to 1) the power constraint (2), and 2) the statistical independence of the columns of S.

II. Capacity for $T = 1$; no CSI

An upper bound on capacity is obtained by permitting the columns of S to be statistically dependent. This leads directly [2] to the conclusion that, when $T = 1$, the capacity for $M > 1$ users is equal to the capacity for $M = 1$ user. In contrast, if perfect CSI were available to the receiver, the total M-user capacity would be equal to the single-user/M-antenna capacity [3], and in case CSI is available also to the transmitters the channel controled TDMA is optimal [4].

III. Conjecture for $T > 1$; no CSI

For the general case $T > 1$, a conjecture is that the total capacity for any $M > T$ is equal to the total capacity for $M \leq T$. At present we are unable to prove this conjecture, but we make some headway by studying the case where T and M grow big. In this case, with $M/T \to 0$, the asymptotic mutual information is $T\log(1+\rho)$, which is equal [3] to the capacity where a single user has access to an unlimited number of transmit antennas, with perfect CSI available to the receiver. This result strongly support our conjecture.

References

[1] L. H. Ozarow, S. Shamai (Shitz) and A. D. Wyner, "Information Theoretic Considerations for Cellular Mobile Radio" *IEEE Trans. Veh. Tech.*, vol. 43, pp. 359–378, 1994.

[2] T. L. Marzetta and B. M. Hochwald, "Capacity of a Mobile Multiple-Antenna Communication Link in Rayleigh Flat Fading", *IEEE Trans. Information Th.*, vol. 45, no. 1, pp. 139–157, 1999.

[3] I. E. Telatar, "Capacity of Multi-Antenna Gaussian Channels", *AT&T Bell Laboratories Technical Memo*, 1995.

[4] R. Knopp and P. A. Humblet, "Information Capacity and Power Control in Single-Cell Multiuser Communications", *Proc. Int. Conf. Communications, ICC'95* (Seattle, WA, June 18–22, 1995), pp. 331–335.

[1] This research was performed, in part, while the author was visiting the Mathematical Sciences Research Center, Bell Laboratories, Lucent Technologies

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Sum Capacity of DS-CDMA with Colored Noise

Pramod Viswanath[1]
Department of EECS,
University of California at Berkeley,
Berkeley, CA94720-1772.
e-mail:pvi@eecs.berkeley.edu

Venkat Anantharam
Department of EECS,
University of California Berkeley,
Berkeley, CA94720-1772.
e-mail:ananth@eecs.berkeley.edu

Abstract — **We consider a Direct Sequence Code Division Multiple Access (DS-CDMA) channel in colored additive Gaussian noise and focus on the sum capacity of this channel. Sum Capacity is the maximum sum of rates at which users can jointly reliably transmit, in an information theoretic sense. We completely characterize optimum sum capacity, which is obtained by choosing the signature sequences of the users appropriately. Our characterization is constructive in that we provide a combinatorial algorithm to generate the optimum signature sequences as a function of the covariance of the additive background noise and power constraints of the users. The characterization also allows us to identify a saddle property of the optimum sum capacity: convexity in the covariance matrix of the additive noise and concavity in the vector of user power constraints.**

I. Introduction and Problem Statement

A discrete time baseband no fading DS-CDMA channel (with short signature sequences) is the following:

$$\mathbf{y}(n) = \sum_{i=1}^{K} x_i(n)\mathbf{s}_i(n) + \mathbf{w}(n) \ .$$

Here K denotes the number of users and n the channel use instant. The user symbols are denoted by x_i and $\mathbf{y}(n)$ is the signal (thought of as a N dimensional vector, N being the processing gain or number of chips per symbol) at the receiver at time instant n. Here $\mathbf{w}(n)$ is an additive Gaussian noise with covariance matrix Σ. Each user i is subject to a time averaged power constraint of p_i. We denote D to be the diagonal matrix of the user power constraints.

Our focus will be on sum capacity: sum of rates at which users jointly reliably communicate. These rates are time averaged with the power constraint on the users also averaged in time. A generalization of the results in [2] to the colored noise case allows us to write the following expression for sum capacity of the DS-CDMA channel with signature sequences $S \stackrel{\text{def}}{=} [\mathbf{s}_1 \ldots \mathbf{s}_K]$.

$$C_{sum}(S, D, \Sigma) = \frac{1}{2}\log\det\left(I + \Sigma^{-1}SDS^t\right) \ .$$

Our main focus in this paper is to characterize the maximum sum capacity:

$$C_{opt}(D, \Sigma) \stackrel{\text{def}}{=} \max_{S \in \mathcal{S}} C_{sum}(S, D, \Sigma)$$

where $\mathcal{S}$ is the set of all $N \times K$ real matrices with all columns having l_2 norm equal to 1. Observe that C_sum is a continuous function defined on a compact set $\mathcal{S}$ and thus the use of max in above is justified.

[1]This work was supported by NSF under grant IRI 97-12131.

II. Main Results

Our main result is a complete characterization of C_{opt} as a function of D and Σ. This characterization is constructive in the sense that we develop a *combinatorial* algorithm to generate the optimum signature sequences (these achieve the maximum sum capacity). The details of this result are available in [3]. In this summary, we briefly describe a qualitative property of the optimum sum capacity that emerges out of our characterization. Our first result is a saddle property of the optimum sum capacity:

Theorem 1 *For every fixed Σ, $C_{opt}(D, \Sigma)$ is a concave function in D and a convex function in Σ for every fixed D.*

We can strengthen this result using the partial order of Schur majorization on vectors in $\mathbb{R}^N$. We say that a vector $\mathbf{a}$ majorizes another vector $\mathbf{b}$ if their components have the same sum and the components of $\mathbf{a}$ are "more spread out" than those of $\mathbf{b}$. For example, every vector in $\mathbb{R}^N$ with sum N *majorizes* the vector with all components unity. An exhaustive resource for results on this partial order is [1]. We show that the optimum sum capacity is a Schur-saddle function in the following sense. Below we have denoted the vector of eigenvalues of Σ by $\left(\sigma_1^2, \ldots, \sigma_N^2\right)$.

Theorem 2 *1. For every fixed D, $C_{opt}(D, \Sigma) > C_{opt}\left(D, \tilde{\Sigma}\right)$ for every $\Sigma \neq \tilde{\Sigma}$ such that $\left(\sigma_1^2, \ldots, \sigma_N^2\right)$ majorizes $\left(\tilde{\sigma}_1^2, \ldots, \tilde{\sigma}_N^2\right)$.*

2. For every fixed Σ and for every $D \neq \tilde{D}$ such that $(p_1, \ldots, p_K)$ majorizes $(\tilde{p}_1, \ldots, \tilde{p}_K)$ we have $C_{opt}\left(\tilde{D}, \Sigma\right) > C_{opt}(D, \Sigma)$.

References

[1] A. W. Marshall and I. Olkin, *Inequalities: Theory of Majorization and its applications*, Academic Press, 1979.

[2] P. Viswanath and V. Anantharam, "Optimal Sequences and Sum Capacity of Synchronous CDMA Systems", *IEEE Transactions on Information Theory*, vol. 45(6), Sept. 1999, pp. 1984-1991.

[3] P. Viswanath and V. Anantharam, "Total Capacity of Vector Multiple Access Channels", UCB/ERL Memorandum. M99/47.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On Capacity and Spreading in CDMA Systems

Mehul Motani[1]
Cornell University
Ithaca, NY 14850
e-mail: motani@ee.cornell.edu

Venugopal V. Veeravalli
Cornell University
Ithaca, NY 14850
e-mail: venu@ee.cornell.edu

Chris Heegard
Alantro Communications
Santa Rosa, CA 95401
e-mail: heegard@alantro.com

Abstract — **The problem of maximizing a weighted linear combination of the rates of users in a multiuser synchronous CDMA system is considered. We find that although spreading decreases capacity, nontrivial low rate coding can help to mitigate this loss.**

I. Introduction and Motivation

Massey [1] proposed a novel definition of a spread spectrum system as one in which the Fourier bandwidth W, defined as the "support" of the Fourier transform, is much greater than the Shannon bandwidth B, defined as one-half the number of dimensions of signal space used per second.

Following [1], which dealt with single user communication, we study multiuser CDMA communication systems from an information theoretic perspective. The sum capacity was studied and characterized in [2, 3]. In this paper, we consider the problem of maximizing an arbitrary linear combination of the users' rates over multiuser capacity regions.

II. Multiuser Capacity Regions

We assume a K-user, additive white Gaussian noise (AWGN) channel with usable bandwidth W, noise PSD $\frac{N_0}{2}$, and average power constraint P_i for the i^{th} user.

The capacity region, i.e., the set of rates at which reliable communication is possible, for unconstrained signaling (no spreading) is well known [4] and defined by the constraints:

$$0 \leq \sum_{i \in J} R_i \leq W \log_2 \left(1 + \sum_{i \in J} \frac{P_i}{N_0 W}\right) \quad \text{bits/sec}, \qquad (1)$$

where J is a nonempty subset of $\{1, \cdots, K\}$. We will denote this capacity region with no spreading as $\mathcal{C}_{\text{ns}}$.

The capacity region for symbol synchronous CDMA with spreading factor $N = \frac{W}{B}$ is defined by the constraints [5]:

$$0 \leq \sum_{i \in J} R_i \leq B \log \left(\det \left[\boldsymbol{I}_{|J|} + \frac{\boldsymbol{P}_J \boldsymbol{R}_J}{N_0 B}\right]\right) \quad \text{bits/sec}, \qquad (2)$$

where $|J|$ is the cardinality of J, I_k is a $k \times k$ identity matrix, and $\boldsymbol{R}_J$ and $\boldsymbol{P}_J$ are the matrix of normalized cross correlations and the diagonal matrix of received powers (P_i) respectively of the users in J. Since the capacity region for direct-sequence CDMA depends upon the cross-correlations between the users' spreading sequences, we will denote it as $\mathcal{C}_{\text{ds}}(\boldsymbol{R})$.

We also consider "naive" CDMA, in which all users are assigned identical spreading sequences. Defining $\mathbf{1}_K$ to be the $K \times K$ matrix of all ones, we note that $\mathcal{C}_{\text{naive}} = \mathcal{C}_{\text{ds}}(\boldsymbol{R} = \mathbf{1}_K)$.

A common performance metric is the sum capacity [2], which is the maximum value of the sum of all users' rates. The general problem of maximizing an arbitrary linear combination of the users' rates is considered by defining the capacity metric function: $M(\boldsymbol{\lambda} = [\lambda_1, \cdots, \lambda_K]) = \boldsymbol{\lambda}[R_1, \cdots, R_K]^\top$.

[1]This research is supported in part by NSF Grants CCR-9805885 and CCR-9733204 and in part by the Intel Foundation Fellowship.

III. Results and Discussion

1. The capacity regions are nested as follows:

$$\mathcal{C}_{\text{naive}} \subseteq \mathcal{C}_{\text{ds}}(\boldsymbol{R}) \subseteq \mathcal{C}_{\text{ns}} \qquad (3)$$

This immediately gives us, for any $\boldsymbol{\lambda}$,

$$\max_{\mathcal{C}_{\text{naive}}} M(\boldsymbol{\lambda}) \leq \max_{\mathcal{C}_{\text{ds}}(\boldsymbol{R})} M(\boldsymbol{\lambda}) \leq \max_{\mathcal{C}_{\text{ns}}} M(\boldsymbol{\lambda}) \qquad (4)$$

2. That spreading decreases capacity, suitably defined here as the maximum of a linear combination of the users' rates, is not surprising. The surprising result, also noticed in [1], is that spreading need not decrease capacity substantially. Consider the sum capacity, i.e., set $\boldsymbol{\lambda} = [1, \cdots, 1]$. Letting the Shannon bandwidth of the sum of the K users' modulated signals satisfy $B = \alpha \frac{\bar{P}}{N_0}$, where $\alpha > 0$ and $\bar{P}$ is the average power received from all users, a simple argument shows

$$\frac{C_{\text{ds}}(\boldsymbol{R})}{C_{\text{ns}}} = \frac{\max_{\mathcal{C}_{\text{ds}}(\boldsymbol{R})}\{M([1, \cdots, 1])\}}{\max_{\mathcal{C}_{\text{ns}}}\{M([1, \cdots, 1])\}} \geq \frac{\alpha}{\alpha + K}. \qquad (5)$$

3. A similar argument can be used to show that an arbitrary linear combination of the user's rates can be made close to the maximum achievable.

$$\frac{\max_{\mathcal{C}_{\text{ds}}(\boldsymbol{R})}\{M(\boldsymbol{\lambda})\}}{\max_{\mathcal{C}_{\text{ns}}}\{M(\boldsymbol{\lambda})\}} \geq \frac{\alpha}{\alpha + K}. \qquad (6)$$

We make no assumptions on the spreading sequences or the received powers of the users. Our results indicate that if the Shannon bandwidth is large enough, spreading does not entail a substantial loss in capacity. One way to increase the Shannon bandwidth is to use nontrivial low rate coding [1]. However, (5) and (6) indicate that coding provides diminishing returns, i.e, as the code rate decreases, the amount of improvement decreases. The implication to the coding-spreading tradeoff is that one should code to the point of diminishing returns (say 80-90% of capacity) and use the remaining bandwidth expansion for spreading.

References

[1] J. L. Massey, "Information theory aspects of spread-spectrum communications," in *Proc. ISSSTA'94*, volume 1, pages 16–21. ISSTA, July 1994.

[2] M. Rupf and J. Massey, "Optimum sequence multisets for synchronous code-division multiple-access channels," *IEEE Trans. Inform. Th.*, 40(4):1261–1266, July 1994.

[3] P. Viswanath and V. Anantharam, "Optimal sequences and sum capacity of synchronous CDMA systems," *IEEE Trans. Inform. Th.*, 45(6):1984–1991, September 1999.

[4] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, Wiley, New York, 1991.

[5] S. Verdu, "The capacity region of the symbol-asynchronous Gaussian multiple-access channel," *IEEE Trans. Inform. Th.*, 35(4):733–751, July 1989.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Suboptimal Schemes for Noncoherent Parallel Acquisition of Spreading Sequences in DS/SS Systems

Zhiyuan Yan and Dilip V. Sarwate
Coordinated Science Laboratory
Department of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign
Urbana, Illinois 61801-2307 USA
e-mail: yan,sarwate@uiuc.edu

Abstract — **Acquisition is a very important step in DS/SS communications systems. In this paper, we describe several suboptimal schemes for parallel noncoherent acquisition. Simulation results and performance analysis are also summarized.**

I. Introduction

In direct sequence spread-spectrum (DS/SS) communications systems, the transmitter's signature sequence and the receiver's replica of this sequence must be synchronized in order to provide enough signal energy for reliable data demodulation. The synchronization has two stages. In the first stage, often referred to as coarse acquisition, the receiver's sequence is synchronized to within some fraction of the chip duration with the transmitter's sequence. In the second stage, the receiver accomplishes and maintains fine alignment of the sequences by using a code tracking loop. In this paper, we consider only the coarse acquisition process. Our goal is to find effective acquisition schemes which are also easy to implement.

II. Estimation of Delay

In noncoherent parallel acquisition schemes, the receiver first computes, in parallel, the correlation of the received signal with the locally generated in-phase and quadrature RF carrier for each of the phases of the PN sequence. Next, the N complex observations $Z(i)$, where $i = 0, 1, \ldots, N-1$, are used to estimate the unknown delay between the local sequence and the sequence in the received signal.

Optimal Estimator The optimal estimation scheme [1] [2] minimizes P_e, the probability that the estimate of the true delay differs from the true delay by more than half a chip interval. $\mathcal{S}_{opt}$ as given in [2] is very intensive computationally and its performance is difficult to evaluate analytically.

Suboptimal Estimators Srinivasan and Sarwate [3] have considered suboptimal estimators in which the delay $\delta = k + \epsilon$ (where $k = \lfloor \delta \rfloor$) is estimated in two steps. First, k is estimated as $k_{est} = \arg\max_{l \in \{0,1,\ldots,N-1\}} |Z_l|$ and then ϵ is estimated in the same manner as in $\mathcal{S}_{opt}$ or the coherent version of $\mathcal{S}_{opt}$ [1]. These schemes perform nearly as well as the optimal estimator scheme but analytical evaluation of performances is difficult.

We have studied some two-stage suboptimal schemes that estimate k as

$$\arg \max_{l \in \{0,1,\ldots,N-1\}} (|Z_l|^2 + |Z_{l+1}|^2 + \mathrm{Re}(Z_l Z_{l+1}^*))$$

cf. [2], and ϵ from the ratio $|Z_{k_{est}}|/|Z_{k_{est}+1}|$. In particular, $\mathcal{S}_{rt3}$ uses

$$\frac{|Z_{k_{est}+1}|^2}{|Z_{k_{est}+1}|^2 + |Z_{k_{est}}|^2}$$

as the estimate of ϵ. The computational costs of these schemes are much smaller than the optimal scheme. Moreover, because of the simplicity of the decision statistics, analytical results can be obtained.

III. Performance Analysis

We have proved that P_e for all the suboptimal schemes is bounded above by a function that decreases exponentially with increasing SNR. This implies that $P_{e,opt}$, the error probability for $\mathcal{S}_{opt}$ is also an exponentially decreasing function of SNR.

We have studied the performances of the suboptimal schemes by simulation. The figure below compares the error probability performance of the optimal scheme and the four suboptimal schemes. For $\epsilon = 0.25$, two of the schemes have performance close to optimal. For other values of ϵ, other schemes are close to optimal. However, in all cases, $\mathcal{S}_{rt3}$ is always close to the optimal.

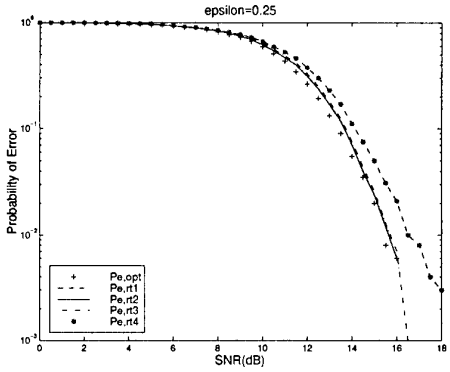


Figure 1: P_e for $\mathcal{S}_{opt}$ and four suboptimal schemes.

References

[1] K. K. Chawla and D. V. Sarwate, "Parallel acquisition of PN sequences in DS/SS systems", *IEEE Transactions on Communications*, vol. COM-42, pp. 2155-2164, May 1994.

[2] A. M. Slonneger and D. V. Sarwate, "Noncoherent Parallel Acquisition of PN Sequences in Direct-Sequence Spread-Spectrum Systems", *Proceedings of the Second IEEE International Symposium on Spread-Spectrum Techniques and Applications*, pp. 31-34, 1992.

[3] M. Srinivasan and D. V. Sarwate, "Noncoherent Parallel Acquisition of Spreading Sequences in DS/SS Systems", *Proceedings of the Conference on Information Sciences and Systems*, vol. II, pp. 858–863, 1996.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Analysis of Acquisition in WCDMA Systems

Sandip Sarkar, ssarkar@qualcomm.com
QUALCOMM Incorporated, 5775 Morehouse Drive, San Diego, CA 92121.

Abstract — **This paper analyzes the acquisition scheme of WCDMA, a standard for the next generation wireless systems, and characterizes its performance under various channel conditions.**

I. Introduction

WCDMA, a standard for 3G wireless systems, uses a three step search to acquire the asynchronous forward link. First, the Primary Synchronization Code (PSC) is used to detect the scramble code mask timing of the best cell site (slot timing) using the proper matched filter. Next, the Secondary Synchronization Code (SSC) is used to identify the scramble code group by cross-correlation of the received signal with all the Group Index (GI) code candidates used in the system. The frame timing is also given by the use of comma free codes. The final stage is the detection of the pilot by identifying the scramble code belonging to the group specified by the SSC.

II. Pilot Detection Technique

The PSC and SSC are multiplexed, and are orthogonal to each other, but not to the other forward link channels. The PSC consists of a length 256 sequence having good aperiodic correlation properties. The searcher coherently integrates the received waveform over a 256 chip duration, and non-coherently integrates a number of them. Then, it picks the maximum as the required estimate. Note that as the symbols transmitted with relatively low power, the signal needs to be accumulated over multiple frames to provide enough energy to successfully demodulate it. The SSC is essentially a two layer code. The outer code provides the frame synchronization information. The inner code provides information on the GI of the pilot.

The SSC consists of Hadamard sequences chosen appropriately and XOR-ed with the PSC. The frame timing is obtained by using a comma-free code on top of it, i.e. a sequence of short codes (SC's) is transmitted. These SC's are unmodulated, of length 16, and are Comma Free, i.e. all their cyclic shifts are unique. Thus the received cyclic shift of this sequence provides information about frame timing. The Comma Free code words are constructed from Reed-Solomon codes. A (16,3) Comma Free Code has more than 300 possible code words out of which only 32 are used, i.e., the process is scalable. Based on the GI, one of 32 possible masks need be identified for pilot acquisition. The pilot symbols are integrated for 1024 chips, and can be analyzed in a manner similar to that described in [1]. During initial acquisition, the MS first demodulates the PSC, then the SSC, including the inner and outer code. Finally, it demodulates the pilot to obtain synchronization. If it is unable to find any pilot in the given GI, it starts the process all over again till it succeeds.

III. Overall System Performance

Since all three stages are always carried out in this algorithm before going back to the first stage, the average total search time can be expressed as: $T_s = \frac{Tc}{1-P_e}$, where T_c is amount of time it takes to go through the three stages, and P_e is probability that one iteration of the three-step search misidentifies the spreading code number and timing. Adding the three stages, use $T_c = (30 + 20 + 10)$ ms $= 60$ ms. P_e, the misdetection probability for each search iteration is given by:

$$P_e = P_f^P + (P_d^P \times P_f^S) + (P_d^P \times P_d^S \times P_f^T),$$

where P_f^P denotes the false alarm probability in detecting the PSC, $P_d^P = 1 - P_f^P$ denotes the probability of correct detection of the PSC, P_f^S denotes the false alarm probability in detecting the SSC, $P_d^S = 1 - P_f^S$ denotes the probability of correct detection of the SSC, and P_f^T denotes the probability of false alarm in detection of the pilot. Fig. 1 shows the search performance for Rayleigh fading channels:

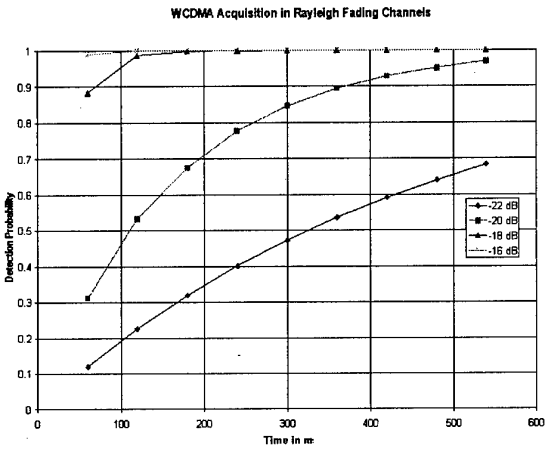


Figure 1: **Acquisition Time in WCDMA**

IV. Conclusion

In practice, the signal may be received at -21dB at the cell boundary for a Rayleigh fading channel. Then, it can be seen that for a 90% reliability, the acquisition time in a practical situation is close to 500 ms. This is in accordance with the simulations shown in [2]. The practical deployment scenario governs the requisite power needed for good system performance. Details of the analysis are omitted here.

References

[1] A. J. Viterbi, *CDMA Principles of Spread Spectrum Communications*, Addison-Wesley, MA, 1995.

[2] K. Higuchi, M. Sawahasi, and F. Adachi, "Fast cell search algorithm in inter-cell asynchronous ds-cdma mobile radio", *IEICE Trans. Commun.*, vol. E-81B, pp. 1527–1534, July 1986.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Maximum Likelihood Symbol Synchronization in Channels with Data Dependent Noise

A. Gameiro
Dept. of Electronics and Telec ./ Inst. Telec., Univ. of Aveiro, 3810 Aveiro Portugal
Tel: (351)34-377926; Fax: (351)34-383128; E-mail: amg@ua.pt

Abstract

In this communication we deal with symbol synchronization in channels with data dependent noise. Examples of such channels arise in optical communications using APD receivers, or direct detection of optically amplified signals [1] where the noise power is higher when a logical one is received. Another situation of data dependent noise arises in the detection of signals in the presence of clutter [2,3]. In these systems the disturbance exhibits cyclostationary statistics that are ignored by the conventional synchronizers designed for the additive Gaussian noise (AGN) channel, although this cyclostationarity contains timing information that can be explored to improve the tracking performance of the symbol synchronizer.

We consider a channel model where the additive disturbance corrupting the received signal consists in the sum of an AWGN process and a cyclostationary component modeled by a Gaussian process with power proportional to the data symbol transmitted. In spite of its simplicity this model represents a good approximation for many direct detection optical systems with APD's or in line optical amplifiers. The maximum-likelihood (ML) data aided (DA) symbol synchronizer for this class of channels is derived and its performance assessed. Comparing the new synchronizer against the well known MLDA synchronizer designed for the AWGN channel, shows that basically the new structure includes in addition to the operations performed by the AWGN-MLDA synchronizer, processing that explores the cyclostationary characteristics of the additive disturbance to enhance the accuracy of the time-delay estimation.

The tracking performance is derived assuming that the synchronizer is designed to operate with a small output jitter, and consequently its behavior can be linearized. It is shown that the timing estimates produced by the maximum likelihood synchronizer are unbiased provided the elementary data pulses exhibit time symmetry around their center, and consequently in such cases the linearized performance achieves the Cramer-Rao bound. The performance of the new synchronizer is compared against the one that would be achieved with the AWGN-MLDA structure when used in channels with data-dependent noise. The results show that non-negligible (up to 6dB) improvements are achieved with the new structure in situations where there is a considerable asymmetry between the noise powers corresponding to a one or zero. The structure is thus of interest for APD based optical communications.

References

[1] R. M. Gagliardi, and S. Karp, *Optical Communications*, 2nd Ed. Wiley, 1995.

[2] C. S. Tsang and W. C. Lindsey, "Bit synchronization in the presence of asymmetric channel noise", *IEEE Trans. Commun.*, June 1986, pp. 528-537.

[3] A. M. Maras and E. A. Kokkinos, "Locally optimum Bayes detection (LOBD) in signal-dependent noise" *IEEE Trans. Commun.*, May. 1997, pp. 523-526.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On the Capacity of a Pulse Position Hopped CDMA System

Ola Wintzell[1]
Dept. of Information Technology
Lund University
Box 118, SE-221 00 Lund, Sweden
ola.wintzell@it.lth.se

Dmitri K. Zigangirov[2]
Institute for Problems of
Information Transmission
Russian Academy of Science
Bolshoy Karteny per. 19
Moscow, 101 447, Russia
zig@iitp.ru

Kamil Sh. Zigangirov
Dept. of Information Technology
Lund University
Box 118, SE-221 00 Lund, Sweden
kamil.zigangirov@it.lth.se

Abstract — **Pulse Position Hopping (PPH) is a new promising multiple access technique which has several benefits, such as coherent reception, low transmit power and it can be constructed to be near-far robust. Analysis [1, 2] shows that, it can reach an order of several thousands of active users per cell. In this paper we have estimated the effective capacity for the uplink and the downlink communication in a PPH spread spectrum system.**

I. Introduction

We consider a PPH-CDMA system with K users. Let $\boldsymbol{u}^{(k)} = (u_0^{(k)}, u_1^{(k)}, \dots u_{L-1}^{(k)})$, $u_l^{(k)} \in \{0,1\}$ and $k = 1, 2, \dots, K$, be the information sequence of the kth user and $\boldsymbol{v}^{(k)} = (v_0^{(k)}, v_1^{(k)}, \dots v_{N-1}^{(k)})$, $v_n^{(k)} \in \{0,1\}$ be the corresponding code sequence. The code rate is then $r = L/N$. The transmission of the code symbols is divided into frames of length T_f. Each active user transmits one code symbol in each frame. The kth user's information rate is then $R^{(k)} = r/T_f$ (bit/s), $k = 1, 2, \dots, K$, independent of the user. The frame time is divided in Q slots of length Δ, $T_f = Q\Delta$, and a pseudo-random "hopping"-sequence $a_n^{(k)} \in \{0, 1, \dots, Q-1\}, n = 0, \dots, N-1$, provides a time shift within the nth frame.

II. PPH-CDMA

We have analyzed the transmission by rectangular pulses of duration T_c with unit energy and Gaussian shaped pulses, such that

$$h(t) = \frac{1}{\sqrt[4]{2\pi\gamma T_c^2}} e^{-\frac{t^2}{4\gamma T_c^2}},$$

where T_c determines the width of the pulse. The parameter γ is chosen such that about 99% of the Gaussian pulse energy is located in the interval $\left(-\frac{T_c}{2}, \frac{T_c}{2}\right)$. The kth transmitters' output signal is

$$s^{(k)}(t) = \sum_{n=0}^{N-1} v_n^{(k)} h(t - nT_f - a_n^{(k)}\Delta),$$

and the received signal is

$$r(t) = \sum_{k=1}^{K} \sqrt{E^{(k)}} s^{(k)} h(t - \delta^{(k)}) + n(t),$$

where $E^{(k)}$ is the energy of the received signal from the kth user, $\delta^{(k)}$ is the time offset, $n(t)$ is the additive white Gaussian noise. Assuming that the system has perfect power control, i.e., $E^{(k)} = E$, $k = 1, \dots, K$, and perfect synchronization, the nth output of the correlation receiver and input to the decoder, for the kth user, is

$$\begin{aligned} z_n^{(k)} &= \int_{-\infty}^{\infty} r(t) h(t - nT_f - a_n^{(k)}\Delta) dt \\ &= v_n^{(k)} \sqrt{E^{(k)}} + \sum_{k' \neq k} I_n^{(k,k')} + n_n \end{aligned}$$

where $I_n^{(k,k')}$ is the interference from the transmission of the k'th user and n_n is the background noise. As $Q \gg 1$ we neglect the interferences from pulses transmitted in other frames and by the assumption that the system is interference limited we neglect the background noise. We estimate the interference between the users and model it as white Gaussian noise, which is reasonable as there is several thousands of users in each cell.

Given the parameters $\mu_0 = E[z_n^{(k)} | v_n^{(k)} = 0]$, $\mu_1 = E[z_n^{(k)} | v_n^{(k)} = 1]$, and $\sigma^2 = \mathrm{var}[z_n^{(k)}]$ the effective signal-to-interference ratio (SIR) per time unit, η, is defined as

$$\eta \stackrel{def}{=} \frac{1}{T_f} \frac{\left(\frac{\mu_1 - \mu_0}{2}\right)^2}{2\sigma^2}.$$

In [2] we have shown that the overall effective system capacity (in bits/s), C, can be lower bounded by $C > \frac{\eta K}{\ln 2}$. For Gaussian and rectangular pulses we get

$$C > \frac{1}{8\sqrt{\pi\gamma} T_c \ln 2} \quad \text{(Gaussian)}$$

$$C > \frac{3}{8 T_c \ln 2} \quad \text{(rectangular.)}$$

III. Numerical evaluation

We have investigated the performance of a PPH-CDMA system transmitting Gaussian pulses and employing a concatenated code with an inner first order Reed-Muller code and an outer rate convolutional code. Simulation of this system indicates that it can host more than 30 000 active users transmitting at a bit rate of 10 kbit/s if you choose T_c to be 1 ns.

References

[1] M. Z. Win, R. A. Scholtz, *Impulse Radio: How it works*, IEEE Communications Letters, vol 2, No 1, 1998

[2] O. Wintzell, D. K. Zigangirov, K. Sh. Zigangirov, *On the Capacity of a Pulse Position Hopped CDMA System*, submitted for publication in IEEE Transactions of Information Theory

[1]This work was supported in part by the Foundation for Strategic Research - Personal Computing and Communication(PCC) and Ericsson Mobile Communications.

[2]This work was supported in part by the Royal Swedish Academy of Science in cooperation with the Russian Academy of Science.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Differential Phase Shift Keying with Constellation Expansion Diversity

Lutz H.-J. Lampe, Robert F.H. Fischer, Johannes B. Huber
Lehrstuhl für Nachrichtentechnik II, Universität Erlangen–Nürnberg, Cauerstr. 7/NT, D–91058 Erlangen, Germany

Abstract — **A new differential encoding strategy is introduced, which is shown to be advantageous for bandwidth efficient transmission over flat Rician fading channels when using multiple symbol differential detection.**

I. System Model and Differential Encoding

Consider a stationary, slowly time–varying, frequency non–selective (flat) Rician fading channel. Channel state and carrier phase offset are expected to be constant over a block of at least N consecutive symbols, but not known at the receiver. For such situations, differential phase encoding at the transmitter and noncoherent demodulation at the receiver are appropriate. To achieve higher spectral efficiencies APSK constellations are attractive, which points are arranged in α distinct concentric rings with radii r_i and β uniformly spaced phases.

Because the received signal amplitude still provides information on the transmitted amplitude, information should be carried in the *actual amplitude*. But then, due to fading, part of the information carried in the amplitude will be lost. One possible approach to overcome this drawback and to exploit the potential of amplitude modulation is to completely map the information onto phase changes, and additionally, to (partly) map the same information onto the amplitude of the transmit symbols. This redundant mapping introduces *diversity*.

The most promising arrangement for the signal points is

$$\mathcal{A} \triangleq \left\{ c = r_{m \bmod \alpha} e^{j\frac{2\pi}{\alpha\beta}m} \mid m = 0, \ldots, \alpha\beta - 1 \right\}, \qquad (1)$$

because points whose phases differ by the minimum value $\frac{2\pi}{\alpha\beta}$ have different amplitudes.

Given the data–carrying *differential symbol* $a = r_j e^{j\frac{2\pi}{\alpha\beta}m} \in \mathcal{A}$ and the state $s = r_i e^{j\phi_n}$ of the differential encoder, the current transmit symbol $x \in \mathcal{X}$ is calculated according to

$$x = r_j e^{j\phi_{(n+m) \bmod \alpha\beta}} . \qquad (2)$$

The transmit signal constellation $\mathcal{X}$ now consists of again α amplitudes but $\alpha\beta$ phases. Due to the redundant mapping, $\mathcal{X}$ is *expanded* and the set $\mathcal{A}$ is a proper subset of $\mathcal{X}$. For $\alpha = 4$, $\beta = 4$ the constellations $\mathcal{A}$ and $\mathcal{X}$ are shown in Figure 1.

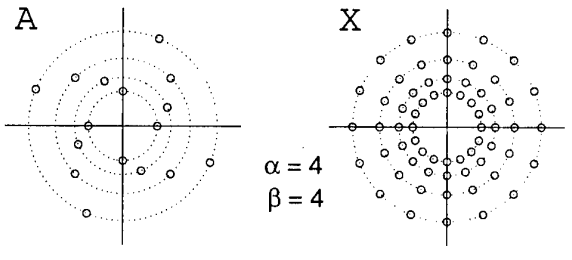


Fig. 1: Signal constellations $\mathcal{A}$ (left) according to (1) and $\mathcal{X}$ (right) for $\alpha = 4$, $\beta = 4$ (geometric ring spacing).

For slow fading channels we apply multiple symbol differential detection [1], where the receiver processes blocks of N consecutive receive symbols. Due to (ideal) interleaving at the transmitter and deinterleaving at the receiver of vector symbols a (virtually) memoryless block fading channel is obtained.

II. Numerical Results

For the AWGN channel and the Rayleigh fading channel the achievable capacity is numerically evaluated as a function of the (average) signal–to–noise ratio $\bar{E}_s/N_0$ ($\bar{E}_s$: average energy per received symbol, N_0: one–sided noise power spectral density). As shown in [2], it is sufficient to fix the differential symbols to be uniformly, independently and identically distributed, and to solely optimize the ring ratio.

Figure 2 shows the capacities of 16–ary modulation schemes using two signaling amplitudes and multiple symbol differential detection of $N = 3$. Clearly, for the AWGN channel, where the amplitude transmit factor is constant, differential encoding of the amplitude is not rewarding. In case of fading channels, absolute amplitude modulation without diversity leads to a flattening of the capacity curve at high SNR. This drawback is overcome by the proposed mapping, which performs best over the whole region of SNR. Hence, the novel scheme incorporates the advantages of the competitors.

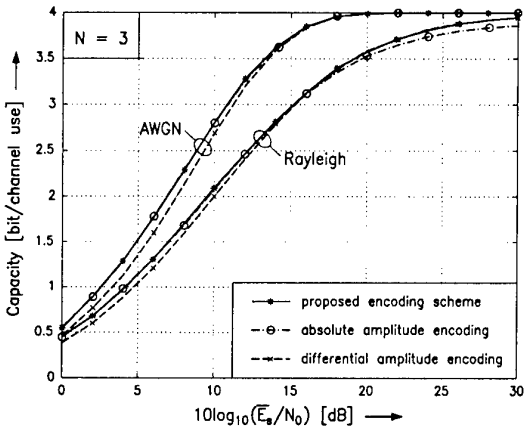


Fig. 2: Capacities for AWGN and Rayleigh fading channel. $N = 3$. Ring ratio $r_1/r_0 = 2$.

Noteworthy, the attainable gain is for free, since it does not require any increment in the coding/decoding complexity when used together with channel coding. The theoretical statements have been verified by simulations, which show a great accordance. For details see [2].

References

[1] D. Divsalar, M.K. Simon. Maximum-Likelihood Differential Detection of Uncoded and Trellis Coded Amplitude Phase Modulation over AWGN and Fading Channels — Metrics and Performance. *IEEE Trans. Commun.*, pp. 76–89, Jan. 1994.

[2] R.F.H. Fischer, L.H.-J. Lampe, S. Calabrò. Differential Encoding Strategies for Transmission over Fading Channels. *International Journal on Elect. and Comm.*, pp. 59–67, Jan. 2000.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

CODED M-FSK for POWER LINE COMMUNICATIONS

A.J. Han Vinck, Juergen Haering and Tadashi Wadayama
University of Essen
vinck@exp-math.uni-essen.de

Abstract - We discuss the application of coded modulation for power-line communications. We combine M-FSK with permutation codes to include frequency and time diversity. This makes the transmissions robust against permanent frequency disturbances and impulse noise. The scheme is applicable to any frequency range.
keywords: modulation; power-line communications; coding.

I. INTRODUCTION

Power Line Communication (PLC) can be seen as one of the possible solutions to the "last dirty mile" problem for communication providers. However, there are several obstacles. According to the European standards (CENELEC), the transmitters are output voltage limited and bandwidth limited. In addition, there are different types of noise involved in PLC. *Narrow band noise*, generated by television sets or computer terminals. This type of noise is permanent over a long period of time. *Impulse noise* has been reported in [1]. From this it can be concluded that impulses are .1 – 1. second apart and have a duration of typically less than 100 μsec. More details regarding the channel properties can be found in [2].
The key idea in this contribution is the combination of the following: 1) We use M-FSK for a constant envelope modulator output; 2) We use a modified non-coherent demodulation with multi valued outputs; 3) We use a permutation code of length M where every code word has M different symbols. 4) The decoding is minimum distance decoding.

II. COMBINED MODULATION and CODING

Encoding: The information is encoded with a permutation code. A permutation code C consists of |C| words of length M, where every code word has M different symbols. The code has minimum Hamming distance d_{min}.
Modulator: The symbols of a code word are transmitted in time as the corresponding frequencies of an M-ary FSK orthogonal signal set. Note that we obtain a constant signal envelope and frequency-/ time diversity simultaneously.
Modified demodulator: We use a simple modified non-coherent demodulator with M envelope detectors. Every envelope detector has a threshold T_i, $1 \le i \le M$. The value of T_i can be optimized with respect to symbol detection error rate and depends on the received signal energy and noise power spectral density per sub-channel. The demodulator outputs in parallel all envelopes that are larger than their respective threshold T_i. Thus, the inputs to the decoder for the permutation code are then multi-valued.
Decoder: We use minimum distance decoding, i.e. we output the message corresponding to the code word that has the minimum number of differences with the M subsequent detector outputs. The following errors may occur in the detector output: 1) insertions or deletions due to background noise; 2) single insertions due to permanent narrow-band noise; 3) multiple parallel insertions due to broad-band (impulse) noise.
Performance: A permanent frequency disturbance only affects one symbol in a code word of the permutation code. Impulse noise may signal the presence of all frequencies in the demodulator output. If restricted to one symbol time interval, this type of error reduces the distance to an incorrect code word with one. It does not decrease the distance to the correct word. Background noise: A deletion error only reduces the distance to the correct code word with one. An insertion error only reduces the distance to an incorrect code word with one. The minimum distance decoder is capable of correcting the combination of d_{min}-1 of these types of errors.

III. CODE PROPERTIES

An interesting mathematical problem is the design of codes. The next theorem gives an upper bound on the number of code words in a permutation code.
Theorem 1. For a permutation code of length M with M different code symbols in every code word and minimum Hamming distance d_{min}, the cardinality

$$|C| \le \frac{M!}{(d_{min}-1)!}. \qquad (1)$$

It can be shown that for $M < 6$, codes exist that meet the upperbound with equality for any $d_{min} \le M$. The smallest value of M for which the upperbound (1) cannot be met with equality is $M = 6$ and $d_{min} = 5$. It has been shown that for these parameters $|C| = 18$, [3]. Blake, [4], uses the concept of sharply k-transitive groups to define permutation codes with minimum distance M-k+1.
The following Theorem gives the parameters of an example of a class of permutation codes based on a multi-level code construction with Reed Muller component codes.
Theorem 2. There exists an $(M, |C|, d_{min})$-permutation code with the following parameters:

$$M = 2^m, \qquad (2a)$$
$$|C| = (2^{m+1}-2)\,x\,(2^m-2)\,x \cdots x\,(2^2-2), \qquad (2b)$$
$$d_{min} = 2^{m-1}, \qquad (2c)$$

where m is an arbitrary positive integer.

IV. SIMULATION RESULTS and CONCLUSIONS

We show how a PLC system with reasonable transmission speed can use this modulation/coding scheme. It appears that for such a system, background noise is of no importance up to a distance of 750 meters. Extensive simulation reports are available from [5].

REFERENCES

[1] M.Chan and R. Donaldson, "Amplitude, Width, and Interarrival Distributions for Noise Impulses on Intrabuilding PLC Networks," *IEEE Tr.on EMC*, Vol. 31, August 1989, pp. 320-323.
[2] O. Hooijen, "A Channel Model for the Residential Power Circuit used as a Digital Communication Medium," *IEEE Tr. on EMC*, Vol. 40, pp. 331-336, 1998.
[3] Torleiv Klove, private communication, to be presented at *ISITA2000*, Hawaii.
[4] Ian F. Blake, "Permutation Codes for Discrete Channels," *IEEE Tr. on Information Theory*, pp. 138-140, Jan 1974.
[5] A.J. Han Vinck and Jürgen Häring, Coding and Modulation for Power Line Communication," *4th Symposium on Power Line Communications*, April 4-6, Limerick, Ireland.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Error Performance of Multilevel Modulation Codes over Phase Noisy Fading Channels

Robert H. Morelos-Zaragoza
Advanced Telecommun. Lab.
SONY Computer Sci. Lab., Inc.
3-14-13 Higashi-Gotanda
Shinagawa, 1410022 Tokyo, Japan
morelos@csl.sony.co.jp

Motohiko Isaka[1]
Institute of Industrial Science
University of Tokyo
7-22-1 Minato-ku, Roppongi
1068558 Tokyo, Japan
isaka@imailab.iis.u-tokyo.ac.jp

Hideki Imai[1]
Institute of Industrial Science
University of Tokyo
7-22-1 Minato-ku, Roppongi
1068558 Tokyo, Japan
imai@iis.u-tokyo.ac.jp

Abstract — **The performance of multilevel coded modulation with multistage and iterative decodings over phase noisy fading channels is evaluated. Semi-analytical upper bounds on the bit error probability are derived and verified to be tight.**

I. Summary

Ever since coding for bandwidth limited channels with expanded signal sets was introduced, the subtleties of trellis codes against phase noise especially over fading channels have been of interest in the literature. However, similar analysis for multilevel coded modulation [1] can be scarcely found although the situation is rather different, due to the multiply represented signal points in multistage decoding. The advantages of this coding scheme are: (1) optimality in information theoretic sense is guaranteed over Gaussian channels with staged decoding; (2) flexibility to coordinate the parameters; and (3) applicability to *unequal error protection* (UEP) coding as shown and analyzed in [2, 3]. In this paper, we extend the results in [4], and evaluate the error performance of multilevel codes with coherent detection over phase noisy flat fading channels, based upon union bound arguments for the conditional probability of a bit error and Monte Carlo integration.

Multilevel codes with multistage decoding can be constructed based on unconventional partitioning, i.e., other than Ungerboeck's set partitioning, effectively for both UEP and *equal error protection*. Hence, various combinations of signal partitioning, component codes and (asymmetric) constellations can be considered, each usually showing a different bit error rate characteristic [2, 3]. One of the goals of this paper is to discuss the sensitivity of each coded level to phase noise in the receiver for a number of code constructions, assuming maximum likelihood decoding in each staged decoder.

With multistage decoding, at a given level of a multilevel coded modulation system, let $P_e(w)$ denote the pairwise error probability (PEP) that the decoder chooses a wrong codeword different in w positions from the transmitted codeword. Conditioned on a vector of fading amplitudes $\bar{\rho} = (\rho_1, \cdots, \rho_n)$ and phase jitter components $\bar{\theta} = (\theta_1, \theta_2, \cdots, \theta_n)$, the PEP becomes the same as that of an AWGN channel. In deriving this conditional PEP, denoted $P_e(w|\bar{\rho}, \bar{\theta})$, careful treatment is necessary since in general different pairs of code sequences considered in the union bound share the same decision regions. The line joining the code sequences of each pair considered in the multidimensional Euclidean space is no longer always orthogonal to the decision region considered by the decoder, as shown in [3]. The PEP can then be obtained by integrating $P_e(w|\bar{\rho}, \bar{\theta})$ over the probability density functions of the random vectors $\bar{\rho}$ and $\bar{\theta}$. In general, the expression for $P_e(w)$ is difficult, if not impossible, to evaluate in a closed form. Following the approach of [5], the conditional PEP is first expressed with an alternate form of the Gaussian Q-function. The resulting expression, although still needs to be evaluated numerically, contains a single integral over a finite range and an integrand that can be evaluated using a Gauss-Hermite quadrature integration formula. Although semi-analytical in nature, the results obtained constitute useful tools in the design of multilevel codes for phase noisy fading channels, particularly when the Hamming weight of the error events is relatively small. This includes short block component codes as well as the error floor region of turbo component codes. Moreover, the same set of bounds can be used to evaluate the effect of co-channel interference on the error performance of multilevel codes.

On the other hand, the sensitivity in the waterfall region with respect to phase noise, when turbo decoding is performed in each stage, can be reduced in essence to that of decoding over mismatched channels. A similar argument holds for iterative decoding of multilevel codes, as discussed in [6], in which the design rules of code construction are different from that for multistage decoding. In both cases, certain performance degradation due to phase noise has been observed by simulation.

[1]This work was supported in part by Association of Radio Industries and Businesses under the Public Participation Program for Frequency Resources Development.

References

[1] H. Imai and S. Hirakawa, "A new multilevel coding method using error-correcting codes," *IEEE Trans. Inform. Theory*, vol. IT-23, no.3, pp.371-377, May 1977.

[2] R.H. Morelos-Zaragoza, M.P.C. Fossorier, S. Lin and H. Imai "Multilevel coded modulation for unequal error protection and multistage decoding: part I–symmetric constellations," *IEEE Trans. Commun.*, vol. 48, no.2, pp. 204-213, Feb. 2000.

[3] M. Isaka, R.H. Morelos-Zaragoza, M.P.C. Fossorier, S. Lin and H. Imai "Multilevel coded modulation for unequal error protection and multistage decoding: part II–asymmetric constellations," to appear in *IEEE Trans. Commun.*

[4] R.H. Morelos-Zaragoza, M.P.C. Fossorier, S. Lin and H. Imai, "On the error performance of multilevel block coded 8-PSK modulation for unequal error protection over Rayleigh fading channels," presented at *CISS'97*, Baltimore, MA, Mar. 1997.

[5] M.K. Simon and M.-S. Alouini, "A unified approach to the performance analysis of digital communication over generalized fading channels," *Proc. IEEE*, vol. 86, no. 9, pp. 1860-1877, Sept. 1998.

[6] M. Isaka and H. Imai,"Design and iterative decoding of multilevel modulation codes," *Technical Report of IEICE*, IT99-78, Mar. 2000.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

How Large is the Coding Gain for Multilevel Modulation Systems?

Gerd Beyer, Karin Engdahl and Kamil Sh. Zigangirov
Dept. of Information Technology, Lund University
Box 118, SE-221 00 Lund, Sweden
E-mail: gerd,karin,kamil@it.lth.se

Abstract — **It is well known that Ungerbœck's and Imai/Hirokawa's multilevel coded modulation systems give essential gain in comparison to a conventional coded modulation system, but as we know a rigorous analysis of this gain has not yet been done. In this work we present the results of an asymptotical analysis and a comparison of two coded modulation systems, conventional modulation and multilevel modulation, using q-PSK signaling and transmission over the AWGN channel.**

I. Introduction and Problem Formulation

We study asymptotical performances of trellis coded transmission over AWGN channel with q-PSK signaling, when $q = 2^L$, L is integer, and the memory of the code goes to infinity. We consider two trellis coded modulation systems, conventional trellis coded modulation and multilevel modulation.

In the case of conventional modulation the binary information sequence $\underline{\mathbf{u}}$ enters a memory m, rate $R = b/c$ (bits/q-ary symbol) convolutional encoder, whose output is over the integer ring $\mathbf{Z}_q$ modulo q. The encoder output symbol $\mathbf{v}$, maped q-PSK signal waveform $s_i(t)$. The sequence of signal waveforms $s_i(t)$ is transmitted over the AWGN channel. The receiver is maximum likelihood (Viterbi) receiver.

In the case of multilevel modulation the binary information sequence $\mathbf{u}$ is first partitioned into L binary subsequences $\mathbf{u}^{(1)}, \mathbf{u}^{(2)}, \ldots, \mathbf{u}^{(L)}$. The subsequences $\underline{\mathbf{u}}^{(l)}$ are encoded by L independent binary component convolutional codes of rates $R^{(l)} = b^{(l)}/c^{(l)}$ (bits/code symbol) and memories $m^{(l)}$. The set of L bits (one output bit from each encoder) is synchronously mapped onto the signal point waveform. The sequence of signal waveforms $\mathbf{s}$ is transmitted over the channel. The transmission rate is equal to $R = \sum_{l=1}^{L} R^{(l)}$ (bits/channel use). The multistage decoder consists of a set of L Viterbi-type decoders matched to the codes, used at the corresponding levels of encoding.

Let κ and $\tilde{\kappa}$ be the decoders complexity (number of encoder states) for conventional and multilevel system respectively, P_e and $\tilde{P}_e$ be the decoding error probability for two systems. We proved [1] that for all $R < C$, where C is the capacity of the AWGN channel with q-PSK signaling, there exist, for both modulation systems, positive limits

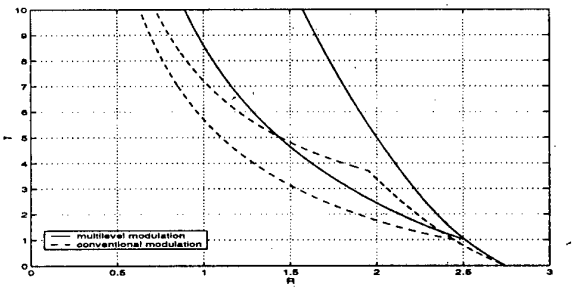


Figure 1: Comparison of upper $\overline{\gamma}(R)$, $\overline{\tilde{\gamma}}(R)$ and lower $\underline{\gamma}(R)$, $\underline{\tilde{\gamma}}(R)$ bounds of the overall state-complexity error exponents for conventional and multilevel modulation systems; $q = 32$, $E_s/N_0 = 10$ dB.

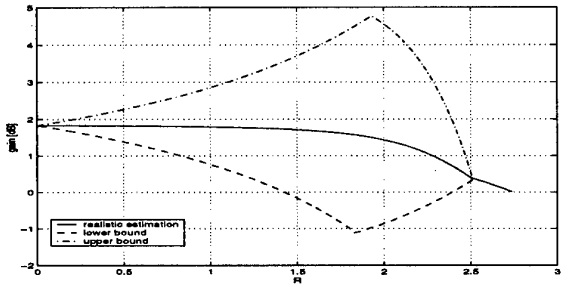


Figure 2: The optimistic (upper), pessimistic (lower) and realistic estimation of the coding gain of multilevel modulation system compared to the conventional modulation system.

E_s/N_0 [dB]	gain$\|_{R=0}$ [dB]	$\tilde{R}_0$	gain$\|_{R=\tilde{R}_0}$ [dB]
0	0.85	0.70	0.5
1	0.95	0.85	0.51
3	1.16	1.20	0.5
5	1.37	1.59	0.47
8	1.66	2, 16	0.41
10	1.83	2.51	0.35
15	1.7	3.37	0.3

Table 1: The asymptotical gain of multilevel 32-PSK signaling in comparison to conventional 32-PSK signaling for $R = 0$ and $R = \tilde{R}_0$ as a function of the signal-to-noise ratio E_s/N_0 for the multilevel system.

$$\gamma \stackrel{def}{=} -\lim_{\kappa\to\infty} \frac{\log P_e}{\log \kappa} > 0, \qquad \tilde{\gamma} \stackrel{def}{=} -\lim_{\tilde{\kappa}\to\infty} \frac{\log \tilde{P}_e}{\log \tilde{\kappa}} > 0. \quad (1)$$

We call γ and $\tilde{\gamma}$ the (asymptotical) state-complexity error exponent for the modulation systems considered. Let $\underline{\gamma}$ and $\underline{\tilde{\gamma}}$ denote lower bounds for γ and $\tilde{\gamma}$ respectively, $\overline{\gamma}$ and $\overline{\tilde{\gamma}}$ denote upper bounds.

II. Comparison of Two Modulation Systems and Numerical Results

In Figure 1 the curves $\underline{\gamma}(R)$, $\underline{\tilde{\gamma}}(R)$, $\overline{\gamma}(R)$ and $\overline{\tilde{\gamma}}(R)$ are given. In Figure 2 three bounds for coding gain of multilevel system in comparison with conventional system are presented.

The realistic bound corresponds to the coding gain of the multilevel system over the conventional system, given that the upper (existens) bounds for the decoding error probabilities are the same.

In Table 1 the gains are presented for different signal-to-noise ratios E_s/N_0 at rate $R = 0$ and at the computational cutoff rate $R = R_0 = \tilde{R}_0$.

References

[1] G. Beyer, K. Engdahl and K. Sh. Zigangirov, "Asymptotical analysis and comparison of two coded modulation schemes using PSK signaling – Part I and II," submitted to *IEEE Transactions on Information Theory*, June 1999. (See http://www.it.lth.se/~karin/)

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Type II Codes over F_4

Philippe Gaborit
Université de Limoges
123, Av. A. Thomas
87000 Limoges, France
e-mail: gaborit@unilim.fr

Vera Pless
University of Illinois–Chicago
851 S. Morgan
Chicago, IL, 60607, USA
e-mail: pless@math.uic.edu

Patrick Solé
CNRS, I3S, ESSI, BP 145
Route des Colles
06 903 Sophia Antipolis, France
e-mail:ps@essi.fr

Oliver Atkin
University of Illinois–Chicago
851 S. Morgan
Chicago, IL 60607, USA
e-mail: aolatkin@math.uic.edu

Abstract — **The natural analogues of Lee weight and Gray map over F_4 are introduced. Self-dual codes for the euclidean scalar product with Lee weights multiple of 4 are called Type II. They produce Type II binary codes by Gray map. All extended Q–codes [3] of length multiple of 4 are Type II, this includes Generalized Quadratic Residue Codes attached to a prime power $q \equiv 7 \pmod 8$. Certain double circulant codes are also considered. The first binary extremal singly-even $[92, 46, 16]$ self-dual code is constructed. A general mass formula is derived.**

I. Definitions and first properties

Let $F_4 := \{0, 1, \omega, \bar{\omega} = \omega^2\}$ be the finite field of order 4, A code C of length n over F_4 is an F_4-subspace of F_4^n. Duality for codes is understood with respect to the Euclidean form $\sum_i x_i y_i$. C is said to be self-dual if $C = C^\perp$. The **Lee composition** of a vector $x = (x_1, \ldots, x_n) \in F_4^n$ is defined as $(n_0(x), n_1(x), n_2(x))$ where $n_0(x)$ is the number of $x_i = 0$, $n_2(x)$ the number of $x_i = 1$ and $n_1(x) = n - n_0(x) - n_2(x)$ where n is the length. The **Lee weight** $w_L(x)$ of x is then defined as $n_1(x) + 2n_2(x)$. There is a natural (*not* F_4-linear!) Gray map ϕ which is a F_2-linear isometry from (F_4^n, Lee distance) onto (F_2^{2n}, Hamming distance) where the Lee distance of two codewords x and y is the Lee weight of $x - y$. We let, for all $x, y \in F_2^n$

$$\phi(\omega x + \bar{\omega} y) = (x, y).$$

This leads us to introduce an **Euclidean weight** $w_E(.)$ on F_4 by the rule $w_E(0) = 0, w_E(\omega) = w_E(1) = 1, w_E(\bar{\omega}) = 2$. Observe that $x \mapsto \omega x$ is an isometry from (F_4, w_E) to (F_4, w_L).

Since multiplying a column by ω does not preserve the Euclidean or Lee weight of a codeword, we need a restricted definition of equivalence and we say that two codes are **equivalent** if one can be obtained from the other by permuting the coordinates (this is not the usual monomial equivalence).

A self-dual code over F_4 is said to be **Type II** if the Lee weight of every codeword is a multiple of 4 and **Type I** otherwise. The following lemma follows:

Proposition I.1 *If C is self-orthogonal so is $\phi(C)$. In this case $\phi(C)$ is a Type I (resp. Type II) code iff C is a Type I (resp. Type II) code.*

II. Constructions

(a) Quadratic residue codes

Let q be a power of a prime with q congruent to 3 (mod 8). Let $C(q)$ denote the extended generalized quadratic residue code of length $q + 1$ over F_4 [2].

Proposition II.1 *The code $C(q)$ is a Type II code over F_4.*

(b) Quadratic double circulant codes

Recently a class of codes which generalizes binary double circulant codes and the Pless symmetry codes to codes over F_4 was introduced in [1]. These codes are also Type II. The following table gives the parameters of these codes along with those of their binary images:

n	k	d	→	n_b	k_b	d_b	Type
14	7	6		28	14	6	I
16	8	6		32	16	8	II
46	23	14		92	46	16	I
48	24	14		96	48	16	II
62	31	16		124	62	16	I
64	32	16		128	64	16	II

Table 1: Quadratic double circulant codes over F_4 and their Type II binary images

(c) Q-codes

The case of quadratic residue codes is a special case of Q-codes of prime length. An extended Q-code of composite length is Euclidean self-dual if and only if its length is a multiple of primes which are congruent to 3 modulo 4 ([3]). We already saw that Euclidean self-dual quadratic residue codes were Type II. We now generalize this result to Q-codes:

Theorem II.2 *Let C be an odd-like duadic code (or Q-code) over F_4 of length $n \equiv 3$ modulo 4, with splitting given by μ_{-1}. Let $\overline{C}$ be the extended code of C. Then the Gray image of $\overline{C}$ is of Type II.*

III. Classification

To elaborate a mass formula, useful for a complete classification, we need to know the number of distinct Type II codes, which is given by:

Theorem III.1 *Let n be an integer multiple of 4 and let $N_{d_{II}}(n)$ be the number of distinct Type II codes over F_4 then:*

$$N_{d_{II}}(n) = \prod_{i=1}^{\frac{n}{2}-1} \frac{4^{n-2k-1} + 3.2^{n-2-2k} - 1}{4^k - 1}.$$

References

[1] P. Gaborit, Quadratic double circulant codes over GF(q), *preprint*.

[2] J. H. van Lint and F. J. MacWilliams, Generalized quadratic residue codes, *IEEE Trans. Inform. Theory* **24**, (1978), 730-737.

[3] V. Pless, Q-Codes, *J. Combin. Theory Ser. A* **43** (1986), 258-276.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On Type II Codes over $\mathbb{F}_4$

Koichi Betsumiya
Graduate School of Mathematics
Nagoya University
Nagoya 464–8602, Japan

T. Aaron Gulliver
Dept. of Electrical & Computer Eng.
University of Victoria
Victoria, BC, Canada V8W 3P6

Masaaki Harada
Dept. of Mathematical Sciences
Yamagata University
Yamagata 990–8560, Japan

Akihiro Munemasa
Graduate School of Mathematics
Kyushu University
Fukuoka 812–8581, Japan

Abstract — **Recently Type II codes over $\mathbb{F}_4$ have been introduced as Euclidean self-dual codes with the property that all Lee weights are divisible by four. We construct new extremal Type I and Type II codes, and show that there are seven Type II codes of length 12, up to permutation-equivalence.**

I. Introduction

Recently Gaborit, Pless, Solé and Atkin [1] introduced Type II codes over $\mathbb{F}_4 = \{0, 1, \omega, \bar{\omega} = \omega^2\}$. These codes are closely related to binary Type II codes via the Gray map defined in [2].

A linear code C of length n and dimension k over $\mathbb{F}_4$ is a k-dimensional vector subspace of $\mathbb{F}_4^n$. A code C is said to be *Euclidean self-dual* (resp. self-orthogonal) if $C = C^\perp$ (resp. $C \subset C^\perp$) where $C^\perp$ is the dual code of C under the Euclidean inner product.

Let $n_0(x), n_\omega(x), n_{\bar{\omega}}(x)$ and $n_1(x)$ be the numbers of 0's, ω's, $\bar{\omega}$'s and 1's in a vector $x \in \mathbb{F}_4^n$, respectively. The *Lee weight* $wt_L(x)$ of x is defined as $2n_1(x)+n_\omega(x)+n_{\bar{\omega}}(x)$. *Type II codes* are self-dual codes under the Euclidean inner-product with the property that all Lee weights are divisible by four. Euclidean self-dual codes which are not Type II are called Type I. Type II codes are divided into two classes, namely, odd Type II codes and even Type II codes.

The Hamming weight of x is the number of non-zero components of x. The minimum Lee weight d_L (resp. Hamming weight d_H) of C is the smallest Lee (resp. Hamming) weight among all non-zero codewords of C.

We have found several properties of even Type II codes as well as odd Type II codes from properties of binary Type II codes. For example, there is a Type II code of length n if and only if n is divisible by four. The minimum Lee weight d_L of a Type II code of length n is upper bounded by $d_L \leq 4\left[\frac{n}{12}\right] + 4$. A Type II code of length n with $d_L = 4\left[\frac{n}{12}\right] + 4$ is *extremal*. We have found that an even Type II code is not extremal for lengths $n \geq 16$.

II. Classification of Lengths up to 12

There is a unique Type II code C_4 of length 4 [1]. Let C_8 be the code with generator matrix $(\ I_4\ ,\ J_4 - I_4\ )$, where I_4 and J_4 are the identity matrix and the all-ones matrix of order 4, respectively. C_8 is the only extremal even Type II code, up to permutation-equivalence. C_8 and C_4^2 are the only Type II codes of length 8, up to permutation-equivalence [1].

The classification of Type II codes of length 12 is given in Table 1. The mass formula in [1] shows that our classification is complete.

Theorem 1 *There are seven Type II codes of length 12, up to permutation-equivalence.*

Table 1: The Type II codes of length 12

Codes	d_L	$\lvert PAut(C_{12,i})\rvert$	$\phi(C_{12,i})$
$C_{12,1}$	4	10368	e_8^3
$C_{12,2}$	4	16128	e_8^3
$C_{12,3}$	4	972	D_{24}
$C_{12,4}$	4	432	D_{24}
$C_{12,5}$	4	23040	A_{24}
$C_{12,6}$	4	1152	F_{24}
$C_{12,7}$	8	660	G_{24}

The generator matrices $(\ I\ ,\ A_i\ )$ of $C_{12,i}$ using the form $a_1, a_2, \ldots, a_6$ where a_j is the j-th row of A_i.

A_1 : $0000\omega\bar{\omega}, 0000\bar{\omega}\omega, 00\omega\bar{\omega}00, 00\bar{\omega}\omega00, \omega\bar{\omega}0000, \bar{\omega}\omega0000,$

A_2 : $0000\omega\bar{\omega}, 0000\bar{\omega}\omega, 011100, 101100, 110100, 111000,$

A_3 : $0000\omega\bar{\omega}, 00\omega\bar{\omega}00, 0\omega\bar{\omega}1\bar{\omega}, 0\bar{\omega}\omega1\bar{\omega}\omega, \omega01\bar{\omega}\bar{\omega}\omega, \bar{\omega}0\bar{\omega}\omega\omega1,$

A_4 : $0000\omega\bar{\omega}, 0\omega\omega\bar{\omega}1\bar{\omega}, 0\omega\bar{\omega}\omega1\bar{\omega}, 0\bar{\omega}\omega\omega1\bar{\omega}, \omega1111\bar{\omega}, \bar{\omega}\bar{\omega}\bar{\omega}\bar{\omega}\omega,$

A_5 : $000111, 001011, 010011, 100011, 1111\omega\bar{\omega}, 1111\bar{\omega}\omega,$

A_6 : $000111, 0\omega\bar{\omega}\omega\bar{\omega}1, 0\bar{\omega}\omega\omega\bar{\omega}1, 1\omega\omega\bar{\omega}0\bar{\omega}, 1\bar{\omega}\bar{\omega}0\omega\omega, 111\bar{\omega}\omega1,$

A_7 : $0\omega\omega\bar{\omega}\bar{\omega}1, \omega0\bar{\omega}\omega1\bar{\omega}, \omega\bar{\omega}\bar{\omega}0\omega1, \bar{\omega}\omega0\bar{\omega}1\omega, \bar{\omega}1\omega111, 1\bar{\omega}1\omega11.$

III. New Extremal Type II Codes

A *pure double circulant* code of length $2n$ has a generator matrix of the form $(\ I\ ,\ R\ )$ where I is the identity matrix of order n and R is an $n \times n$ circulant matrix. Extremal double circulant Type II codes are given in Table 2

Table 2: Type II pure double circulant codes

Codes	The first row r	d_L
$D_{II,20}$	$11\bar{\omega}\omega110000$	8 (extremal)
$D_{II,24}$	110111101000	8
$D_{II,28}$	$\bar{\omega}\bar{\omega}\omega\bar{\omega}0\omega\omega0110000$	12 (extremal)
$D_{II,32}$	$\bar{\omega}\bar{\omega}0\omega01\bar{\omega}1\omega0\omega00000$	12 (extremal)
$D_{II,36}$	$\omega01\bar{\omega}\omega1\omega\omega100100000$	12

Extremal Type II codes of lengths 16, 20 and 28 were constructed in [1]. $D_{II,32}$ is the first example of an extremal Type II code of length 32.

References

[1] P. Gaborit, V. Pless, P. Solé and O. Atkin, Type II codes over $\mathbb{F}_4$, (preprint).

[2] F.J. MacWilliams and N.J.A. Sloane, "The Theory of Error-Correcting Codes," North-Holland, Amsterdam 1977.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Error-Correcting Codes over an Alphabet of Four Elements[1]

Galina T. Bogdanova
Institute of Math. and Inf.
Bulgarian Academy of Sci.
P.O. Box 323, 5000 V.
Tarnovo, Bulgaria
lpmivt@vt.bia-bg.com

Andries E. Brouwer
Department of Mathematics
Eindhoven Univ. of Technology
P.O. Box 513, 5600 MB
Eindhoven, The Netherlands
andries.brouwer@cwi.nl

Stoian N. Kapralov
Department of Mathematics
Technical University
5300 Gabrovo, Bulgaria
kapralov@tugab.bg

Patric R. J. Östergård
Dept. of Comp. Sci. and Eng.
Helsinki Univ. of Technology
P.O. Box 5400, 02015 HUT,
Finland
patric.ostergard@hut.fi

Abstract — **The problem of finding the values of $A_q(n,d)$—the maximum size of a code of length n and minimum distance d over an alphabet of q elements—is considered. When $q \leq M < 2q$, all parameters for which $A_q(n,d) = M$ are determined. Methods for obtaining upper and lower bounds on $A_4(n,d)$ are discussed.**

I. Introduction

Let Z_q denote the set $\{0,1,\ldots,q-1\}$ and let Z_q^n be the set of all n-tuples (vectors) over Z_q. An $(n,M,d)_q$ code is a code over Z_q that has length n, size M, and minimum distance d. One of the main problems in combinatorial coding theory is to find the largest possible value of M when the other parameters have been fixed; this value is denoted by $A_q(n,d)$ and corresponding codes are called *optimal*.

Linear quaternary codes have earlier been considered, for example, in [3]. Except for some preliminary results of this work, which were presented in [2], only sporadic results have been published earlier in the general quaternary case.

II. On Small Optimal Codes

To obtain our main result, we combine the Plotkin bound, the juxtaposition construction, a result by Baranyai [1], and the following theorem, which generalizes a result from [4].

Theorem 1 *Suppose we have a resolvable PBD($v = M, K; \lambda$) with n parallel classes, where each parallel class has at most q blocks. Then there exists an equidistant $(n, M, n-\lambda)_q$ code.*

The main theorem is as follows.

Theorem 2 *Let $q < M \leq 2q$. Then an $(n, M, n-\lambda)_q$ code exists if and only if $n/\lambda \leq M(M-1)/2(M-q)$. For $M \neq 2q-1$ equality implies that such a code is optimal.*

Corollary 1 *For $q \leq M < 2q$, $A_q(n,d) = M$ exactly when*

$$\frac{(M+1)^2 - 3(M+1) + 2q}{(M+1)^2 - (M+1)} n < d \leq \frac{M^2 - 3M + 2q}{M^2 - M} n.$$

[1]This work was partially supported by the Bulgarian National Science Fund and by the Academy of Finland.

III. Finding Bounds on $A_q(n,d)$

Upper bounds on $A_q(n,d)$ can be obtained, for example, from the Plotkin bound, the Hamming bound, and the linear programming bound.

Lower bounds on $A_q(n,d)$ are obtained by constructing corresponding codes. An exhaustive computer search is for all but the smallest parameters out of question. To search for codes, we therefore have to use stochastic methods and/or prescribe a structure of the codes to restrict the search.

As for the structure of the codes, four different methods have been used for $q = 4$. These give additive codes over $Z_2 \times Z_2$, lexicographically minimal codes, codes that consist of orbits of words under the action of a permutation group, and codes that consist of cosets of a linear code, respectively.

To give an example, the 13 vectors below generate a $(12, 2^{13}, 5)$ additive code over $Z_2 \times Z_2$, a current record. (The four symbols 00,01,10,11 of $Z_2 \times Z_2$ are written 0,1,2,3.)

111110000000	130102100001
110001110000	110020201000
101001001100	011121021001
010100101010	101100102200
211001000001	000121002020
022001101000	131121002002
021200001001	

We have collected the best known bounds on $A_4(n,d)$ for $n \leq 12$.

References

[1] Zs. Baranyai, "On the factorization of the complete uniform hypergraph," in *Infinite and Finite Sets, I, Colloq. Honour Paul Erdős, Keszthely 1973, Colloq. Math. Soc. János Bolyai*, vol. 10, pp. 91–108, 1975.

[2] G. Bogdanova, "Optimal codes over an alphabet of 4 elements," *Proc. Fifth International Workshop on Algebraic and Combinatorial Coding Theory, Sozopol, June 1–6, 1996*, Shumen: Unicorn, 1996, pp. 46–53.

[3] F. R. Kschischang and S. Pasupathy, "Some ternary and quaternary codes and associated sphere packings," *IEEE Trans. Inform. Theory*, vol. 38, pp. 227–246, 1992.

[4] N. V. Semakov and V. A. Zinov'ev, "Equidistant q-ary codes with maximal distance and resolvable balanced incomplete block designs," (in Russian), *Probl. Peredach. Inform.*, vol. 4, no. 2, pp. 3–10, 1968.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

A Construction of Ternary Constant-Composition Codes with Weight Three and Minimum Distance Four

Mattias Svanström[1]
Dept. of Electrical Engineering
Linköpings universitet
SE-581 83 Linköping, Sweden
e-mail: mattias@isy.liu.se

Abstract — **We consider the problem of finding the maximal size $A_3(d, w_0, w_1, w_2)$ of a ternary constant-composition code. We describe a construction of ternary constant-composition codes that proves $A_3(4, 4m+1, 2, 1) = (m+1)(4m+2)$ and $A_3(4, 4m-1, 2, 1) = m(4m+2)$.**

I. Introduction

We study the problem of determining the maximal size of a ternary block code with constant composition. The metric we are interested in is the Hamming metric. Let each codeword have w_0 0's, w_1 1's and w_2 2's. Denote the minimum Hamming distance of a code by d and let $A_3(d, w_0, w_1, w_2)$ denote the maximal size of a code. We let n denote the length of a code. The corresponding functions $A_2(n, d)$ for binary codes without restrictions, $A_2(n, d, w)$ for binary constant-weight codes and $A_3(n, d)$ for ternary codes without restrictions have been thoroughly investigated. The papers [1] and [2] contain extensive lists of references on these problems. The problem of determining $A_3(d, w_0, w_1, w_2)$ on the other hand has received very little attention. Two references for results on this problem are [3] and [4].

We focus on ternary constant-composition codes with Hamming weight three. Without loss of generality we assume $w_1 = 2$ and $w_2 = 1$. In [5] we presented a construction of codes with this composition and minimum distance three, whereas we here give a construction of codes with minimum distance four.

II. Construction

Let m be a positive integer. Take D^* to be the $m \times (2m+1)$ matrix with

$$D^*_{ij} = \begin{cases} 2, & \text{if } j = 1; \\ 1, & \text{if } j = i+1 \text{ or } j = 2m-i+2; \\ 0, & \text{otherwise.} \end{cases}$$

Let D be the $m(2m+1) \times (2m+1)$ matrix with rows equal to all different cyclic shifts of the rows of D^*, in arbitrary order. Let D_1 and D_2 be two $m(2m+1) \times (2m+1)$ matrices. Take D_1 to be 1 in exactly those positions where D is 1, and take it to be 0 elsewhere. Similarly, take D_2 to be 2 in exactly those positions where D is 2, and take it to be 0 elsewhere. We note that all rows of D_1 are different and that for any selection of two columns of D_1 there is exactly one row that has its 1's in these two columns.

We use the notation I_{2m+1} for the $(2m+1) \times (2m+1)$ identity matrix and $2I_{2m+1}$ for the $(2m+1) \times (2m+1)$ matrix with 2's on the main diagonal and 0's elsewhere. We construct matrices B_1, B_2, B_3 and B_4 as follows:

$$B_1 = \left[\begin{array}{c|c|c} 10 & I_{2m+1} & 2I_{2m+1} \\ \vdots & & \\ 10 & & \end{array}\right],$$

$$B_2 = \left[\begin{array}{c|c|c} 01 & 2I_{2m+1} & I_{2m+1} \\ \vdots & & \\ 01 & & \end{array}\right],$$

$$B_3 = \left[\begin{array}{c|c|c} 00 & D_1 & D_2 \\ \vdots & & \\ 00 & & \end{array}\right], \qquad B_4 = \left[\begin{array}{c|c|c} 00 & D_2 & D_1 \\ \vdots & & \\ 00 & & \end{array}\right].$$

Let C_{4m+1} be the code consisting of the union of all the rows of B_1, B_2, B_3 and B_4. We define C_{4m-i} for $i = 0, 1, 2$ to be C_{4m+1} shortened with respect to 0's in the first $i+1$ positions.

III. Bounds on $A_3(4, w_0, 2, 1)$

Our main result is the following theorem:

Theorem 1 *For any integer $m \geq 1$, the equalities*

$$\begin{aligned} A_3(4, 4m+1, 2, 1) &= (m+1)(4m+2), \\ A_3(4, 4m-1, 2, 1) &= m(4m+2), \end{aligned}$$

hold.

We are currently not aware of any codes having a larger number of codewords than C_{4m} as constructed above. However, larger codes than C_{4m-2} are known for small m, see also [3] and [4].

References

[1] A. E. Brouwer, J. B. Shearer, N. J. A. Sloane, and W. D. Smith, "A new table of constant weight codes," *IEEE Transactions on Information Theory*, vol. IT-36, no. 6, pp. 1334–1380, Nov 1990.

[2] A. E. Brouwer, H. O. Hämäläinen, P. R. J. Östergård, and N. J. A. Sloane, "Bounds on mixed binary/ternary codes," *IEEE Transactions on Information Theory*, vol. 44, no. 1, pp. 140–161, Jan 1998.

[3] G. T. Bogdanova and D. S. Ocetarova, "Some ternary constant-composition codes," in *Proceedings of the Sixth International Workshop on Algebraic and Combinatorial Coding Theory*. Pskov, Russia, Sep 1998, pp. 41–45.

[4] M. Svanström, *Ternary Codes with Weight Constraints*, Ph.D.. thesis, Linköpings universitet, Sweden, 1999, Dissertation No. 572.

[5] M. Svanström, "Optimal ternary constant-composition codes with Hamming weight three," in *Proceedings of the Seventh Nordic Combinatorial Conference*. Turku, Finland, Aug 1999, pp. 81–84.

[1] This work was supported by the Swedish Research Council for the Engineering Sciences under grant 271–97–532.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Capacity of weakly (d,k)-constrained sequences

Kees A. Schouhamer Immink
Institute for Experimental
Mathematics, Ellernstrasse 29,
45326 Essen, Germany.
immink@exp-math.uni-essen.de

Augustus J.E.M. Janssen
Philips Research Laboratories,
WY 81, Prof. Holstlaan 4, 5656
AA Eindhoven, The Netherlands.
a.j.e.m.janssen@philips.com

Abstract — *In the presentation we find an analytic expression for the maximum of the normalized entropy* $-\sum_{i\in T} p_i \ln p_i / \sum_{i\in T} ip_i$ *where the set* T *is the disjoint union of sets* S_n *of positive integers that are assigned probabilities* P_n, $\sum_n P_n = 1$. *This result is applied to the computation of the capacity of weakly* (d,k)*-constrained sequences that are allowed to violate the* (d,k)*-constraint with small probability.*

I. Problem description and results

Let T be a set of positive integers, and assume that T is the disjoint union of a (finite or infinite) number of non-empty sets $S_n, n \in M$. Also assume that there are given numbers $P_n \geq 0$, $n \in M$, with $\sum_n P_n = 1$. We show the following result.

Theorem: *The maximum of*

$$H := \frac{-\sum_{i\in T} p_i \ln p_i}{\sum_{i\in T} ip_i} \tag{1}$$

(ln : natural logarithm) under the constraints that $p_i \geq 0$, $\sum_{i\in S_n} p_i = P_n$, $n \in M$, *equals* z_0, *where* $z_0 > 0$ *is the unique solution* z *of the equation*

$$-\sum_{n\in M} P_n \ln Q_n(z) = -\sum_{n\in M} P_n \ln P_n \tag{2}$$

with for $z > 0$

$$Q_n(z) := \sum_{i\in S_n} e^{-iz}, \quad n \in M. \tag{3}$$

Moreover, the optimal p_i *are given by*

$$p_i = \frac{P_n}{Q_n(z_0)} e^{-iz_0}, \quad i \in S_n, n \in M, \tag{4}$$

and for these p_i *we have that*

$$\sum_{i\in T} ip_i = \frac{d}{dz}\left[-\sum_{n\in M} P_n \ln Q_n(z)\right](z_0). \tag{5}$$

As an application of this result we consider *weakly constrained (d,k)* sequences [1]. A binary (d,k)-constrained sequence has by definition at least d and at most k 'zeros' between consecutive 'ones'. Weakly constrained codes produce sequences that violate the specified constraints with a small probability. It is argued that if the channel is not free of errors, it is pointless to feed the channel with perfectly constrained sequences. A (d,k)-constrained sequence can be thought to be composed of 'phrases' 10^i, $d \leq i \leq k$, where 0^i means a series of i 'zeros'. In order to compute the channel capacity, i.e. the maximum $z_0/ln2$ of the entropy $H/\ln 2$, we define

$$\begin{aligned} T &= \{1,\ldots,d\} \cup \{d+1,\ldots,k+1\} \\ &\cup \{k+2,k+3,\ldots\} =: S_1 \cup S_2 \cup S_3, \end{aligned} \tag{6}$$

where $d = 0, 1, \ldots$, and $k = d+1, d+2, \ldots$ are given, and we compute the capacity for the case that the probabilities P_1, P_3 assigned to the sets S_1, S_3 are both small. Clearly, the quantities P_1 and P_3 denote the probabilities that phrases are transmitted that are either too short or too long, respectively. We find that the familiar capacities of (d,k)-constrained sequences [2] are approached from above as P_1, $P_3 \to 0$ with an error $A(P_1 \ln P_1 + P_3 \ln P_3)$, where we can evaluate the A explicitly. We obtain a similar result for the case that T is as in (6) with S_1, S_3 merged into a single set $S_1 \cup S_3$. Further results are published in [3].

Conclusions

We have presented an analytic expression for the maximum of the normalized entropy $-\sum_{i\in T} p_i \ln p_i / \sum_{i\in T} ip_i$ under the condition that T is the disjoint union of sets S_n of positive integers that are assigned probabilities P_n, $\sum_n P_n = 1$. We computed the capacity of weakly (d,k)-constrained sequences that are allowed to violate the (d,k)-constraint with given probability.

References

[1] K.A.S. Immink, 'Weakly Constrained Codes', *Electronics Letters,* vol. 33, no. 23, pp. 1943-1944, Nov. 1997.

[2] K.A.S. Immink, *Codes for Mass Data Storage Systems,* Shannon Foundation Publishers, Eindhoven, The Netherlands, 1999.

[3] A.J.E.M. Janssen and K.A.S. Immink, 'An entropy theorem for computing the capacity of weakly (d,k)-constrained sequences', *IEEE Trans. Inform. Theory*, vol. IT-46, no. 5, pp., May 2000.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On Codes that Avoid Specified Differences

Bruce E. Moision
Bell Laboratories
600 Mountain Avenue
Murray Hill, NJ 07974
bmoision@research.bell-labs.com

Alon Orlitsky
Dept. of Electrical Engineering
University of California, San Diego
La Jolla, CA 92093-0407
alon@ucsd.edu

Paul Siegel
Dept. of Electrical Engineering
University of California, San Diego
La Jolla, CA 92093-0407
psiegel@cwc.ucsd.edu

Abstract — **We study the number of binary sequences whose differences do not include certain disallowed patterns. We show that the number of such sequences increases exponentially with their length and that the exponent, or capacity, is the logarithm of the joint spectral radius of an appropriately defined set of matrices. We derive a new algorithm for determining the joint spectral radius of sets of nonnegative matrices and combine it with existing algorithms to determine the capacity of several sets of disallowed differences that arise in practice.**

I. Codes that avoid difference patterns

The bit-error-rate of a recording channel is often dominated by a small set of error, or difference, patterns. Binary codes have been proposed which exploit this fact, e.g.,[1]. The codes are designed to avoid the most problematic difference patterns by constraining the set of allowed recorded sequences and have been shown to improve system performance. In order to maximize the achievable linear density for a recording channel, it is important to identify constraints that permit the highest possible code rate. To that end, we study the largest number of sequences whose differences exclude a given set of disallowed patterns.

More specifically, let D be a finite set of finite-length disallowed difference patterns, and let $\mathcal{C}_n$ be a collection of n-bit sequences whose differences do not contain any patterns in D. The largest number of sequences whose pairwise differences do not include any pattern in D is

$$\delta_n(D) \stackrel{\text{def}}{=} \max\{|\mathcal{C}_n| : \mathcal{C}_n \text{ avoids } D\}.$$

We define the *capacity* of D as the limit

$$\mathsf{cap}(D) \stackrel{\text{def}}{=} \log\left[\lim_{n\to\infty} (\delta_n(D))^{1/n}\right].$$

We show that, for every finite D,

$$\mathsf{cap}(D) = \log\ \rho(\Sigma(D))$$

where $\Sigma(D)$ is an appropriately defined set of adjacency matrices and ρ is the *joint spectral radius* of the set [2]. This equality may be viewed as a generalization of the well-known result that the growth rate of the number of sequences, or Shannon capacity, of a constrained system is the logarithm of the spectral radius of an appropriately defined adjacency matrix.

II. Computing the joint spectral radius

Computing the joint spectral radius of a set of matrices is, in general, a hard problem [3]. Algorithms for computing it have been described in [4, 5]. We derive a new algorithm to compute $\rho(\Sigma(D))$ and determine or closely approximate $\mathsf{cap}(D)$ for a number of difference sets D of practical interest.

Table 1: Capacity of various difference sets D

m	D	$\mathsf{cap}(D)$	$\mathcal{O}$
$m \geq 1$	$0^{m-1}+$	0	-
2	+-	α	$10^{(0)}, 01^{(1)}$
	++	α	11
3	0+0	.5	$00^{(1)}, 11^{(1)}$
	+0+	α	101, 111
	+++	δ	111
	+-+	δ	$101^{(0)}, 010^{(1)}$

$$\alpha = \log_2((1+\sqrt{5})/2) = .6942...$$

$$\delta = \log_2((1 + (19+3\sqrt{33})^{1/3} + (19-3\sqrt{33})^{1/3})/3) = .8791...$$

Table 1 summarizes known values of $\mathsf{cap}(D)$ for a number of difference sets D consisting of a single pattern of length m. Next to the capacity, we list a constraint describing a sequence of codes, $\{\mathcal{C}_n\}$, such that each $\mathcal{C}_n$ avoids D and

$$\lim_{n\to\infty} \log|\mathcal{C}_n|^{1/n}$$

achieves $\mathsf{cap}(D)$. The constraint is defined by a list of forbidden patterns $\mathcal{O}$. If no superscript is listed with a pattern, the pattern is forbidden from appearing in all positions of the code. If superscripts appear, then the patterns are periodic and the period is one more than the largest superscript. The superscript then represents the positions (modulo the period) in which the pattern is disallowed from starting.

References

[1] R. Karabed, P. Siegel, and E. Soljanin, "Constrained coding for binary channels with high intersymbol interference," *IEEE Transactions on Information Theory*, vol. 45, pp. 1777–1797, Sept. 1999.

[2] G. C. Rota and G. Strang, "A note on the joint spectral radius," *Indagationes Mathematicae*, vol. 22, pp. 379–381, 1960.

[3] J. N. Tsitsiklis and V. D. Blondel, "The Lyapunov exponent and joint spectral radius of pairs of matrices are hard–when not impossible–to compute and to approximate," *Mathematics of Control, Signals, and Systems*, vol. 10, pp. 31–40, 1997.

[4] I. Daubechies and J. C. Lagarias, "Two-scale difference equations II. Local regularity, infinite products of matrices and fractals," *SIAM Journal Math. Anal.*, vol. 23, pp. 1031–1079, 1992.

[5] G. Gripenberg, "Computing the joint spectral radius," *Linear Algebra and its Applications*, vol. 234, pp. 43–60, 1996.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Optimal Block Codes for *M*-ary Runlength-Limited Channels

Steven W. McLaughlin and Suparna Datta[1]
School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332
email: swm@ece.gatech.edu, sd12@cornell.edu

Abstract — **In this paper we consider the analysis and design of optimal block-decodable *M*-ary runlength-limited (RLL) codes. We present two general construction methods: one based on permutation codes due to Datta and McLaughlin, and the other a nonbinary generalization of the binary enumeration methods of Patrovics and Immink, and Gu and Fuja. The construction based on permutation codes is simple and asymptotically (in blocklength) optimal, while the other construction is optimal in the sense that the resulting codes have the highest rate among all block-decodable codes for any blocklength. In the process, we shall also prove a new result on the capacity of *(M,d,k)* constraints. Finally, we present examples of remarkably low-complexity *(M,d,k)* block codes which achieve the optimal rate without the use of enumeration.**

I. Introduction

Traditional optical recording employs saturation recording, where the channel input is constrained to be a binary sequence satisfying runlength-limiting (RLL) or (d,k) constraints. A binary (d,k)-constrained sequence is one in which the number of zeroes between consecutive ones is at least d and at most k. The idea of optical recording with M $(M>2)$ levels has been proposed [1], and previous work in coding for such nonbinary channels includes [1]-[3]. Assuming an M-ary symbol alphabet, $\{0,1, ..., M-1\}$, $M<\infty$, an M-ary runlength-limited or (M,d,k) sequence [3]-[4] is one where at least d and at most k zeroes occur between nonzero symbols. Binary (d,k) codes are (M,d,k) codes with $M=2$.

In this paper we present two broad code construction techniques for block-decodable (M,d,k) codes. First, we give a new result on the capacity of (M,d,k) constraints; this leads to a simple code construction which produces codes that asymptotically (in blocklength) achieve capacity. Second, we extend the enumerative construction of Patrovics and Immink [5] to the nonbinary case. We show how this algorithm can be used to design optimal deterministic block codes; these codes are optimal in the sense that they have the highest possible rate among all block-decodable codes. Finally, we present examples of M-ary block codes that achieve the optimal rate through a novel use of lookup tables rather than the more complex enumeration scheme.

II. On the Capacity of (M,d,k) Codes

The allowable sequences in an (M,d,k)-constrained code are made up of phrases, where each phrase begins with at least d and at most k zeroes and ends with a single nonzero symbol. For example, an allowable $(M,d,k)=(5,1,7)$ sequence is

0002 00001 0000004 003 01 00000004

where individual phrases have been underlined for emphasis.

Next, we state a result on capacity. This is the M-ary generalization of Theorem 1 of Zehavi and Wolf [6]. Let X_i be a random variable describing the number of symbols in the ith phrase of the parsed sequence, and let A_i be a random variable denoting the nonzero value (amplitude) of the terminating symbol of the phrase.

Theorem 1. The code achieving maximum information rate has the following properties:

(1) The random variables $A_1,A_2,...$ are statistically independent and uniformly distributed

(2) The random variables $X_1,X_2,...$ are statistically independent and identically distributed

(3) The probability distribution of X is

$$P(X=i)=(M-1)2^{-iC},\ i=d+1, ..., k+1$$

where C is the capacity of the (M,d,k) constraint. Any (M,d,k) code that achieves capacity satisfies (1)-(3), and conversely, any code satisfying (1)-(3) achieves capacity. ❑

Using this theorem, we present an asymptotically efficient, fixed-rate, parallel encoder that is scalable with respect to M and maintains backward compatibility with a binary RLL system [9].

III. Block Codes Based on (M,d,k,l,r) Sequences

In our talk, we present a nonbinary generalization of the enumeration algorithm given by Patrovics and Immink [5]. Using this enumeration algorithm for (M,d,k,l,r) sequences, we are now able to extend two important (d,k) code constructions ([7],[8]) to the nonbinary case [9]-[10]. Based on this, we can show that the optimal rate of the (M,d,k) code with blocklength n is

$$R_{opt} = \log_2\left(\sum_{i=d}^{k} N^0_{k-1}(n-i)\right)\Big/ n.$$

IV. Examples of Optimal (M,d,k) Block Codes

Next, we present examples of block-encodable/block-decodable codes which achieve the optimal code rate, but do not require the aforementioned enumeration algorithm. Rather, these codes use a series of look-up tables consisting of 'templates' in order to encode and decode with very low complexity. As a result, the storage space required for these codes is remarkably small.

Specifically, for an $(M,1,7)$-constrained code with blocklength $n=8$, it can be shown that the optimal rate $R_{opt}=10/8$, $13/8$ for $M=5$, 9 respectively. In our talk, we show how one look-up table consisting of 37 templates of 8-bit codewords can be used to generate *both* of these optimal codes.

Finally, we present an optimal, 92.4% efficient, (5,2,10)-code with blocklength $n=26$ and $R_{opt}=24/26$. This code requires the use of 6 look-up tables containing a total of only 203 13-bit templates [9].

References

[1] A. Earman, "Optical data storage with electron trapping materials using *M*-ary data channel coding," *Proceedings of the SPIE 1663, Optical Data Storage*, pp. 92-103, San Jose, CA, 1992.

[2] S.W. McLaughlin, "Five runlength-limited codes for *M*-ary recording channels," *IEEE Trans. Magn.*, vol. 33, no. 3, pp. 2442-2450, May 1997.

[3] C.A. French, G.S. Dixon, and J. Wolf, "Results involving (d,k)-constrained *M*-ary codes," *IEEE Trans. Magn.*, vol. 23, no. 5, pp. 3678-3680, Sept. 1987.

[4] D.T. Tang and L.R. Bahl, "Block Codes for a Class of Constrained Noiseless Channels", *Information and Control*, vol. 17, pp. 436-461, 1970.

[5] L. Patrovics and K.A.S. Immink, "Encoding of *dklr*-sequences using one weight set," *IEEE Trans. Inform. Theory*, vol. 42, no. 5, pp. 1553-1554, Sept. 1996.

[6] E. Zehavi and J.K. Wolf, "On runlength codes," *IEEE Trans. Inform. Theory*, vol. 34, no. 1, pp. 45-55, Jan. 1988.

[7] G.F.M. Beenker and K.A.S. Immink, "A generalized method for encoding and decoding runlength-limited binary sequences," *IEEE Trans. Inform. Theory*, vol. 29, no. 5, pp. 751-754, Sept. 1983.

[8] J. Gu and T. Fuja, "A new approach to constructing optimal block codes for runlength-limited channels," *IEEE Trans. Inform. Theory*, vol. 40, no. 3, pp. 774-785, May 1994.

[9] S. Datta and S.W. McLaughlin, "Optimal block codes for *M*-ary runlength-constrained channels," submitted, *IEEE Trans. Inform. Theory*, Aug. 1999.

[10] S. Datta, "New results on coding for nonbinary runlength-limited channels," Ph.D. thesis, Georgia Institute of Technology, 2000.

[1] This work was supported by the National Science Foundation under award no. NCR-9702024

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Art of Constructing Low-complexity Encoders/Decoders for Constrained Block Codes

Dharmendra S. Modha
Brian H. Marcus
IBM Almaden Research Center
650 Harry Road
San Jose, CA 95120
{dmodha,marcus}@almaden.ibm.com

Abstract — **Suppose we are given a *block code*, that is, a list of at least 2^p q-bit self-concatenable codewords. A rate p : q block encoder is a dataword-to-codeword assignment from 2^p p-bit datawords to 2^p q-bit codewords, and the corresponding block decoder is the inverse of the encoder. We propose efficient heuristic computer algorithms (i) to eliminate the excess codewords; and (ii) to construct low hardware complexity block encoders/decoders. Constructing low-complexity encoder/decoders for very high rate codes is of immense economical value–as these codes may be implemented in mass-market magnetic recording systems. For several practical constraints, block encoders/decoders generated using the proposed algorithms are comparable in complexity to human-generated encoders/decoders, but are significantly simpler than lexicographical encoders/decoders.**

I. Extended Abstract

Constrained coding is used in magnetic recording systems to encode unconstrained user sequences into channel output sequences that satisfy certain hard constraints such as various limits on the run lengths of zeroes. A block code is a collection of codewords satisfying a certain constrint such that these codewords can be freely concatenated with each other without violating the underlying constraint. Block codes have been widely used for converting unconstrained user sequences into desired constraint sequences. The basic idea in a rate p : q block code is to identify a codebook containing 2^p q-bit codewords that satisfy the desired constraint, and to design an encoder that assigns each 2^p p-bit dataword in a one-to-one and onto fashion to a q-bit codeword in the codebook. In other words, a block encoder is a dataword-to-codeword assignment. The corresponding block decoder is the inverse mapping or the codeword-to-dataword assignment.

We motivate the problem of interest using a concrete example of $(d, k) = (0, 2)$ run-length limited (RLL) constraint which demands that runs of consecutive symbols "0" must not be more than 2. We are interested in a rate 4 : 5 block code for this constraint. A set of valid 5-bit codewords for this constraint can be obtained by starting from all 5-bit words and eliminating all words that have more than two consecutive symbols "0" anywhere in the words and by eliminating all words that have more than one symbol "0" at the beginning or at the end of the word. This process leaves a set of 17 codewords which can be freely concatenated without violating the constraint.

Since $17 > 16 = 2^4$, these set of codewords can support a rate 4 : 5 block code. Thus, the problem is (i) to select an excess codeword and (ii) to determine a mapping from the remaining 16 codewords to the set of all 4-bit datawords. There are 17 choices for the excess codeword, and for each such choice there are 16! choices for the encoder. In all there are $17! \approx 3.5568 \times 10^{14}$ ways to select a codebook and an encoder! In other words, there is a great amount of freedom in selecting the encoder/decoder pair to implement a given block code. In this paper, we are interested in exploiting this freedom to select an encoder/decoder pair that has a low-complexity of hardware implementation. Typically, given the large number of possibilities, a brute-force search is out of the question for even relatively low rate block codes. Currently such a task is performed in a laborious, ad-hoc, and human-centric fashion, and becomes nearly impossible for very high-rate codes.

Datawords	Codewords
excess	10101
0000	10010
0001	10110
0010	10011
0011	10111
0100	01001
0101	01101
0110	11001
0111	11101
1000	01010
1001	01110
1010	01011
1011	01111
1100	11010
1101	11110
1110	11011
1111	11111

Table 1: A block encoder for the $(0, 2)$ RLL constraint.

As our main contribution, we propose efficient heuristic computer algorithms to select a codebook and to construct low-complexity encoder/decoder; for example, the encoder in Table 1 was found using the new algorithm. Furthermore, we demonstrate the algorithm using rate 8 : 9 block codes for $(0, 4/4)$ and $(0, 3/6)$ PRML constraints.

References

[1] D. S. Modha and B. H. Marcus, "Art of constructing low-complexity encoders/decoders for constrained block codes," submitted for publication, 2000. http://www.almaden.ibm.com/cs/people/dmodha

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Cycle Length Distributions in Graphical Models for Iterative Decoding

Xianping Ge, David Eppstein,
and Padhraic Smyth[1]
Information & Computer Science
University of California, Irvine
Irvine, CA 92697-3425, U.S.A.
e-mail:
{xge,eppstein,smyth}@ics.uci.edu

I. Introduction

This paper analyzes the distribution of cycle lengths in turbo decoding graphs. It is known that the widely-used iterative decoding algorithm for turbo codes is in fact a special case of a quite general local message-passing algorithm [1] for efficiently computing posterior probabilities in acyclic directed graphical (ADG) models (also known as "belief networks") [2, 3]. However, this local message-passing algorithm in theory only works for graphs with no cycles. Why it works in practice (i.e., performs near-optimally in terms of bit decisions) on ADGs for turbo codes is not well understood since turbo decoding graphs can have many cycles.

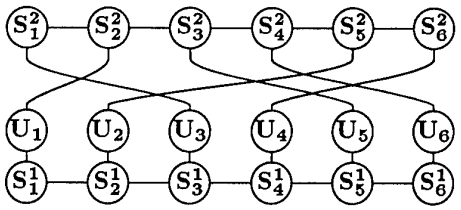


Fig. 1: An example of a turbo decoding graph for a $K = 6$, $n = 12$, rate 1/2 turbocode.

II. Method

The ADG model for a turbo-decoder can be reduced to what we call a *turbo decoding graph* (Figure 1), which is an undirected graph capturing the inherent loop structure of a turbo decoder. There are two parallel chains, each having n nodes (for real turbo codes, n can be very large, e.g., $n = 64,000$). Each node is connected (via a **U** node) to exactly one node on the other chain and these one-to-one connections are chosen randomly, e.g., by a random permutation of the sequence $\{1, 2, \ldots, n\}$.

To help count the cycles in the graph, we drop the **U** nodes, and label the edges in any simple cycle as

1. $\rightarrow$: "Left-to-right on a chain" (e.g., $\mathbf{S}_1^2 \rightarrow \mathbf{S}_2^2$ in Figure 1),
2. $\leftarrow$: "Right-to-left on a chain" (e.g., $\mathbf{S}_3^1 \leftarrow \mathbf{S}_4^1$), or
3. $=$: "Across the chains" (e.g., $\mathbf{S}_3^1 - \mathbf{S}_1^2$).

For example, the cycle $\mathbf{S}_1^2 - \mathbf{S}_2^2 - \mathbf{S}_3^2 - \mathbf{S}_5^1 - \mathbf{S}_4^1 - \mathbf{S}_3^1 - \mathbf{S}_1^2$ will be labeled $\rightarrow\rightarrow=\leftarrow\leftarrow=$. Starting from a node on a chain, and a label sequence $L \in \{\rightarrow, \leftarrow, =\}^+$, there is at most one cycle being labeled L. We count the number of cycles of length k at a node by computing

1. The total number of possible label sequences L,
2. The probability of finding a cycle with the label sequence L.

More complete details can be found in [4].

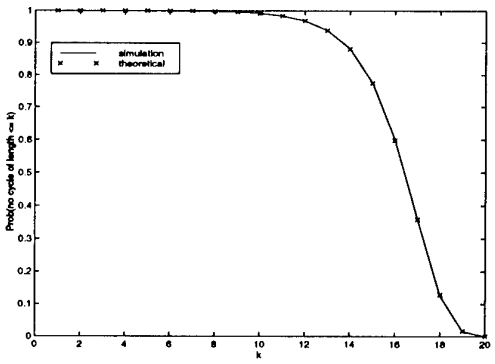


Fig. 2: Theoretical vs. simulation estimates of the probability of no cycles of length k or less, as a function of k, in a turbo decoding graph (chain length $n = 64,000$).

III. Conclusions

Using this general approach, we estimate the probability that there exist no simple cycles of length $\leq k$ at a randomly chosen node in a turbo decoding graph. In Figure 2, we compare both analytical and simulation results. For turbo codes with a block length of 64000, a randomly chosen node has a less than 1% chance of being on a cycle of length less than or equal to 10, but has a greater than 99.9% chance of being on a cycle of length less than or equal to 20.

[1]This work was supported in part by NSF CAREER award IRI-9703120 and by AFOSR grant F49620-97-1-0313.

References

[1] R.J. McEliece, D.J.C. MacKay, and J.-F. Cheng (1998). Turbo Decoding as an Instance of Pearl's 'Belief Propagation' Algorithm. *IEEE Journal on Selected Areas in Communications*, SAC-16(2):140-152.

[2] B. J. Frey (1998). *Graphical Models for Machine Learning and Digital Communication*. MIT Press: Cambridge, MA.

[3] J. Pearl (1988), *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*. Morgan Kaufmann Publishers, Inc., San Mateo, CA.

[4] X. Ge, D. Eppstein, and P. Smyth (1999). The distribution of cycle lengths in graphical models for iterative decoding. Technical Report UCI-ICS 99-10, March 1999. Available at http://www.ics.uci.edu/~datalab/papers.html.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Efficient Decoding of Interleaved Linear Block Codes

C. Haslach, A. J. Han Vinck
Institute for Experimental
Mathematics
University of Essen
Ellernstr. 29
45326 Essen, Germany
haslach@exp-math.uni-essen.de

Abstract — **The error correction capability of interleaved linear block codes is discussed. We assume that the channel behaves such that each row of a received array is either error free or corrupted by many symbol errors. Provided that the error vectors are linearly independent, we show that some interleaved block codes can correct asymptotically one erroneous row per redundant row, even without having reliability information from the channel output. An efficient decoding algorithm that achieves the error correction capability is presented. Using this algorithm we derive a random access scheme that has many similarities with the Aloha system. This paper represents a generalization of our work [2]. As it finally turned out, many ideas from [2] were already discussed in 1990 by Metzner and Kapturowski [3].**

I. Introduction

Block interleaving of linear block codes is a well known method for the correction of long error bursts. Therefore we arrange n_2 codewords of an (n_1, k_1, d_1)-code as the columns of an $n_1 \times n_2$ interleaver matrix. Then the matrix is transmitted over the channel row by row. Using column-wise BMD-decoding we do not exploit the knowledge that errors occur in bursts and that only a limited number of rows is corrupted. In this paper we present a decoding algorithm that makes use of these facts.

II. Transmission scheme

Each column of the $n_1 \times n_2$ block interleaver matrix $\mathbf{C}$ represents a codeword of a given linear block code $\mathcal{C}_1(n_1, k_1, d_1)$ with parity check matrix $\mathbf{H}$. The symbol alphabet corresponds to a finite field denoted by $\mathcal{A}$. We will consider $\mathbf{C}$ to be *one* code matrix of an $n_1 \times n_2$ array code $\mathcal{C}$. The errors inserted by the channel can be described by an additive error matrix $\mathbf{F} \in \mathcal{A}^{n_1 \times n_2}$ where $\mathbf{R} = \mathbf{C} + \mathbf{F}$. According to the parity check matrix $\mathbf{H}$ we can calculate a syndrome vector for each column of the received matrix. Arranging theses syndromes as columns of a $(n_1 - k_1) \times n_2$ matrix we get the so-called syndrome matrix $\mathbf{S}$, where $\mathbf{S} = \mathbf{H} \cdot \mathbf{R}$ holds. It follows that $\mathrm{rank}(\mathbf{S}) = \mathrm{rank}(\mathbf{F})$, as long as $t \leq d_1 - 1$ is fulfilled.

III. Error correction capability

The number of erroneous rows is the metric that we use for decoding. Hence an optimal decoder tries to find that code matrix, that has as many identical rows with $\mathbf{R}$ as possible. It can be shown that $\mathbf{R}$ can be correctly decoded if the following condition is fulfilled:

$$t < d_1 - 1 - (t - \mathrm{rank}\,(\mathbf{F})) \ . \qquad (1)$$

Hence, for linearly independent error vectors we can correct $d_1 - 2$ erroneous rows without using any soft information for symbols or rows. It can be shown for many applications that the matrix dimensions can be designed such that the probability of linearly dependent error vectors becomes arbitrarily small [2]. Using an MDS-code as column code, this means that the corresponding interleaved code can correct $n_1 - k_1 - 1$ erroneous rows without using any reliability information from the channel output, provided that the error vectors are linearly independent.

IV. Decoding

A decoding algorithm can be derived that actually achieves the error correction capability for linearly independent error vectors [2] [3]. The complexity of this algorithm has order $O(n_1^2 \cdot n_2)$. The algorithm can be generalized for the case of linearly dependent error vectors, such that the error correcting capability corresponding eqn. 1 is achieved. The generalized algorithm has low complexity for small values of $t - \mathrm{rank}(\mathbf{F})$. It can be shown that the problem of correcting a linearly dependent error pattern is equivalent to finding a minimum weight codeword of the code that is defined by a submatrix of an equivalent parity check matrix $\mathbf{H}'$.

V. Aloha-Like Random Access Scheme without Feedback

The Aloha system is a simple and well known random access scheme. Nevertheless it requires collision detection and feedback from the receiver or channel to the transmitters. The idea is to consider one row of the interleaver matrix as one received data slot of a random access scheme and to use a long RS code as column code. It turns out that the proposed scheme has the same throughput as slotted Aloha $(1/e)$ without requiring a feedback channel or additional redundancy for error detection.

Acknowledgments

The authors wish to thank Ludo Tolhuizen from Philips Research, Eindhoven, who gave the idea for the formal derivation of the error correction capability.

References

[1] N. Abramson, "The Throughput of Packet Broadcasting Channels," *IEEE Trans. Commun.*, vol. COM-25, no. 1, pp. 117-128, Jan. 1977.

[2] C. Haslach, H. Vinck, "A Decoding Algorithm with Restrictions for Array Codes", *IEEE Trans. Inform. Theory,* vol. 45, no. 7, pp. 2339-2345, Nov. 1999.

[3] J. J. Metzner, E. J. Kapturowski, "A General Decoding Technique Applicable to Replicated File Disagreement Location and Concatenated Code Decoding," *IEEE Trans. Inform. Theory,* vol. 36, no. 4, pp. 911-917, July 1990.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Performance Limits of Concatenated Codes with Iterative Decoding

Sandrine Vialle
Centre de Recherche Motorola
Espace Technologique, Saint Aubin
91193 Gif sur Yvette, France
e-mail: vialle@crm.mot.com

Joseph Boutros
ENST Paris
46 Rue Barrault
75013 Paris, France
e-mail: boutros@com.enst.fr

Abstract — **We present the performance limits of concatenated codes with interleaver of infinite size and under iterative decoding. We study the propagation of the probabilities at the output of the SISO decoder, and give a general formula for the density propagation through iterations.**

I. Introduction

Compound codes have been extensively studied in the literature [1]-[6]. All these codes are decoded iteratively since no maximum-likelihood decoding algorithm of reasonable complexity is available. Recently, [7] and [8] presented a method for determining the performance limits of LDPC codes under iterative decoding. Their approach is based on the estimation of the probability density function of the decoder output from its input density. In this paper, we establish a general density propagation formula available for all isotropic codes, i.e., when the probability distribution of the a posteriori probability (APP) is independent of the bit position, and we give numerical results for different compound codes.

II. Isotropy of constituent codes

All concatenated codes can be modeled as a graph having two types of nodes representing bits and subcodes respectively. In the sequel, this graph is assumed to be cycle-free, i.e., the length of the interleaver is infinite. Let $C(n,k)$ be the linear binary constituent block code. The APP associated to a coded bit c_j, $j = 1 \dots n$, can be written as a function of the conditional weight enumerator $(A_{ji}^{c_j=0}, A_{ji}^{c_j=1})_{i,j=1,\dots,n}$:

$$APP(c_j) \propto \sum_{i=0}^{n} A_{ji}^{c_j} \otimes [p(r/c)p(c)]^{\otimes i} [p(r/\bar{c})p(\bar{c})]^{\otimes n-i}$$

where r is the received symbol, c being transmitted, and $p(r_\ell/c_\ell)p(c_\ell), \ell = 1, ..., n$ are identically distributed. $X + Y$ and XY are respectively denoted $2 \otimes X$ and $X^{\otimes 2}$ when X and Y are identically distributed. If the probability distribution of the APP information is independent of the bit position, the constituent code is said to be isotropic. All bits in the graph are then equally protected by the information propagation. For example, cyclic codes and extended BCH primitive codes are isotropic codes.

III. Log-likelihood ratio density propagation

Let us describe the information propagation in the graphical model of the concatenated code. d (resp. n, the code length or a restricted window containing the local constraints for a convolutional code) is the degree of the bit node (resp. the subcode node). The constituent code is assumed to be isotropic. A subcode node computes an extrinsic information $extLLR_m$ from its $n-1$ inputs. A bit node evaluates its a posteriori probability LLR_m, combining the channel observation, the extrinsic information, and the a priori probability resulting from the product of $d-1$ independent extrinsic informations supplied by the other $d-1$ subcode neighbors. The total APP is the product of d extrinsic informations and the initial observation. Let $\mathcal{B}_m$ be the partial a posteriori log-likelihood ratio (LLR) at iteration m (bit position j omitted):

$$\mathcal{B}_m = log \frac{p(r/c=1)p(c=1)}{p(r/c=0)p(c=0)}$$

The density propagation through the graph can be summarized by the following general formula

$$\mathcal{B}_m = \mathcal{B}_0 + (d-1) \otimes \left[log \frac{\sum_{i=0}^{n} A_i^1 \otimes [\exp(\mathcal{B}_{m-1})]^{\otimes i-1}}{\sum_{i=0}^{n} A_i^0 \otimes [\exp(\mathcal{B}_{m-1})]^{\otimes i}} \right]$$

The total APP distribution is equal to the convolution of the $\mathcal{B}_m$ density and the $extLLR_m$ density. If $p_m(x)$ is the probability density function of LLR_m and if the all zero codeword has been transmitted, the bit error probability at iteration m is $Pe_m = \int_0^{+\infty} p_m(x)dx$. The performance limit of the iterative SISO decoder is given by the minimal value of the signal-to-noise ratio E_b/N_0 for which Pe_m tends to 0 when m goes to $+\infty$.

IV. Numerical results

The following table summarizes the thresholds of different compound codes, obtained by a Monte Carlo method.

PCCC [3] $R = 0.5$ $C = (13, 15)$	0.58dB
SCCC [4] $R = 0.5$ $C_1 = (17, 6, 15), C_2 = (31, 25, 33, 37)$	0.87dB
Block GLD [6] $R = 0.5$ $C = (15, 11)$	0.83dB
Convolutional GLD [5] $R = 0.5$ $C = (13, 15, 2, 14)$	0.85dB

Acknowledgments

The authors wish to thank Olivier Pothier for his precious help and Emanuele Viterbo for his constructive comments.

References

[1] R.G. Gallager, "Low-density parity-check codes," MIT Press, 1963.

[2] R.M. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. on Information Theory*, vol. 27, Sept. 1981.

[3] C. Berrou, A. Glavieux, P. Thitimajshima,"Near Shannon Limit Error-Correcting Coding and Decoding: Turbo-Codes," *ICC'93*, Genève, May 1993.

[4] S. Benedetto, G. Montorsi, D. Divsalar, F. Pollara, "Serial concatenation of interleaved codes: Performance analysis, design and iterative decoding," *TDA Progress Report 42-126*, 1995.

[5] S. Vialle, J. Boutros, "A Gallager-Tanner construction based on convolutional codes," *WCC'99*, Paris, Jan. 1999.

[6] J. Boutros, O. Pothier, G. Zémor, "Generalized Low Density (Tanner) Codes," *ICC'99*, Vancouver, June 1999.

[7] A.J. Felström and K.Sh. Zigangirov, "Time varying periodic convolutional codes with Low-Density-Parity-Check matrix," *IEEE Trans. on Information Theory*, vol. 45, Sept. 1999.

[8] T. Richardson, R. Urbanke, "The capacity of low-density parity check codes under message-passing decoding," *Bell Labs report*, Nov. 1998.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On the Training Distortion of Vector Quantizers

Tamás Linder
Dept. of Mathematics & Statistics
Queen's University
Kingston, Ontario, Canada K7L 3N6
email: linder@mast.queensu.ca

Abstract — **The in-training-set performance of a vector quantizer as a function of its training set size is investigated. For squared error distortion and independent training data, worst-case type upper bounds are derived on the minimum training distortion achieved by an empirically optimal quantizer. These bounds show that the training distortion can underestimate the minimum distortion of a truly optimal quantizer by as much as a constant times $n^{-1/2}$, where n is the size of the training data. Earlier results provide lower bounds of the same order.**

I. Introduction

A d-dimensional k-point vector quantizer Q is a (measurable) mapping of $\mathbb{R}^d$ into a finite set of points $\{y_1, \ldots, y_k\}$, called the codebook. Let $\mathcal{Q}_k$ denote the family of all d-dimensional k-point vector quantizers. Given a d-dimensional random vector X with distribution μ_X, a quantizer $Q^* \in \mathcal{Q}_k$ is called an *optimal* k-point quantizer for μ_X if it has minimum mean squared distortion in $\mathcal{Q}_k$:

$$D(Q^*) = E\big[\|X - Q^*(X)\|^2\big] = \min_{Q \in \mathcal{Q}_k} E\big[\|X - Q(X)\|^2\big].$$

Assume that a quantizer is to be designed on the basis of the *training data* $X_1, X_2, \ldots, X_n$ consisting of n vectors independently drawn according to μ_X. In general, the objective of a quantizer design algorithm (such as the generalized Lloyd algorithm) is to find an empirically optimal quantizer $Q_n^* \in \mathcal{Q}_k$ whose distortion in quantizing the training data is minimum:

$$D_n(Q_n^*) = \min_{Q \in \mathcal{Q}_k} \frac{1}{n} \sum_{i=1}^{n} \|X_i - Q(X_i)\|^2.$$

The random quantity $D_n(Q_n^*)$ is called the *training distortion* of Q_n^*. Since the training distortion is obtained as a by-product of the design procedure without requiring additional test data, it can be considered an inexpensive estimate of $D(Q^*)$. It is easy to see that $D(Q_n^*)$ is optimistically biased in the sense that $E[D_n(Q_n^*)] \le D(Q^*)$ (the inequality is strict whenever $D(Q^*) > 0$). The size of the bias was first investigated in a work by Kim and Bell [1] who showed that $E[D_n(Q_n^*)] \le D(Q^*)(1 - 1/n)$ for any source distribution with a finite second moment. Our main result shows that this bound can be considerably improved in a worst case sense: the difference $D(Q^*) - E[D_n(Q_n^*)]$ of the minimum distortion of an optimal quantizer and the expected training distortion of the empirically optimal quantizer can be as large as constant times $n^{-1/2}$.

II. Minimax bounds on the training distortion

Let $\mathcal{P}(B)$ denote the class of all source distributions which satisfy the peak power constraint $P\{(1/d)\|X\|^2 \le B\} = 1$. In other words, for any $B > 0$, the class $\mathcal{P}(B)$ consists of all source distributions whose support is contained in the ball $\{x : \|x\| \le \sqrt{dB}\}$.

Theorem 1 *For any quantizer dimension $d \ge 1$ and codebook size $k \ge 3$ there exists a source distribution $\mu_X \in \mathcal{P}(B)$ such that for all training set size $n \ge \frac{2}{3}k$,*

$$E\big[D_n(Q_n^*)\big] \le D(Q^*) - \frac{c(B,d,k)}{\sqrt{n}}$$

where $c(B,d,k) = \frac{Bd\sqrt{k^{1-\frac{4}{d}}}}{2^8 3}$.

If the relative difference is considered, the following simple bound can be obtained in terms of the training ratio $\beta = n/k$.

Theorem 2 *For any quantizer dimension $d \ge 1$ and codebook size $k \ge 3$ there exists a source distribution $\mu_X \in \mathcal{P}(B)$ such that for all training set size $n \ge \frac{2}{3}k$,*

$$E\big[D_n(Q_n^*)\big] \le D(Q^*)\left(1 - \frac{c_0}{\sqrt{\beta}}\right)$$

where $c_0 = \frac{1}{4}\sqrt{\frac{7}{6}} \approx 0.27$.

Note that in the above bounds the "bad" source distribution giving a large bias does not depend on the training data size n. Thus Theorem 1 guarantees the existence of at least one *fixed* source distribution in $\mathcal{P}(B)$ such that

$$\liminf_{n\to\infty} \sqrt{n}\Big(D(Q^*) - E\big[D_n(Q_n^*)\big]\Big) > 0.$$

In contrast, the worst case bound developed in [2] on the test distortion of an empirically optimal quantizer is obtained by constructing a different "bad" source distribution for each training data size n.

Using an earlier result [3], it can be shown that Theorem 1 is essentially tight. We can conclude that for all $k \ge 3$ and all n large enough,

$$\frac{c}{\sqrt{n}} \le \sup_{\mu_X \in \mathcal{P}(B)} \Big(D(Q^*) - E\big[D_n(Q_n^*)\big]\Big) \le \frac{\hat{c}}{\sqrt{n}}$$

for some constants $c, \hat{c} > 0$ depending on d, k, and B.

This research was supported in part by the Natural Sciences and Engineering Research Council (NSERC) of Canada.

References

[1] D. S. Kim and M. R. Bell, "Bounds on the trained vector quantizer distortion measured using training data." Tech. Rep. TR-ECE 98-6, Purdue University, April 1998.

[2] P. Bartlett, T. Linder, and G. Lugosi, "The minimax distortion redundancy in empirical quantizer design," *IEEE Trans. Inform. Theory*, vol. IT-44, pp. 1802–1813, Sep. 1998.

[3] T. Linder, G. Lugosi, and K. Zeger, "Rates of convergence in the source coding theorem, in empirical quantizer design, and in universal lossy source coding," *IEEE Trans. Inform. Theory*, vol. 40, pp. 1728–1740, Nov. 1994.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Asymptotic Two-Stage Two-Dimensional Quantizer

Tsutomu Kawabata
Dept. of Information and Communication Engineering
University of Electro-Communications,
1-5-1,Chofugaoka,Chofu,Tokyo,182-8585,Japan
e-mail: kawabata@ice.uec.ac.jp

Abstract — **We present a new asymptotic quantization theory on a plane for a known smooth non-uniform data density. Based upon a two-stage model, we design a mapping for harmonic cluster. We argue angular phase field. We give a relative distortion mismatch for a case of asymptotic clusters, and optimize over the cluster centers.**

I. Introduction

When $\| \quad \|^s$ represents the s-th power ($s > 0$) of the Euclidean distance, the integral

$$\int_{R^2} \min_{1 \le i \le N} \|x - y_i\|^s p(x) dx. \tag{1}$$

measures a performance of an N-quantizer, $y_1, \ldots, y_N$, of a random point from a smooth probability density $p(x)$ on a plane. We study an asymptotic geometry of a near optimal quantizer when N is large enough. Let $\beta = s/k$ and $\rho = 2/(s+2)$, and let $\| p \|_\rho$ denote $\{\int p(x)^\rho\}^{1/\rho}$, then it is well known that

$$\min_{\{y_1,\ldots,y_N\}} (1) \sim N^{-\beta} R_{2,s} \| p \|_\rho, \tag{2}$$

where $R_{2,s}$ is the normalized s-th moment of the regular hexagon. This result holds under a mild regularity condition on p, including the moment condition $\int \|x\|^{s+\varepsilon} p(x) dx < \infty$ for any $\varepsilon > 0$. On the one hand the result means that the optimal quantizer have a density proportional to $p^\rho(x)$, and on the other hand each point in the quantizer, call which a generator, have a Voronoi region being almost similar to the regular hexagon. Only a few [1][2][3][4] study this seemingly contradictory facts. We continue them and propose a new asymptotic approach in the design of two-stage quantizer.

II. Results

Define $\tilde{g}(x) := p^\rho / \int p^\rho dx$, thus $N\tilde{g}$ is the optimal number density of generators. We identify $\mathcal{R}^2$ as a complex plane $\mathcal{C}$. Let $\mathcal{C}$ be decomposed into domains $\mathcal{C} = \bigcup_\xi U_\xi$, where U_ξ is indexed by some central point ξ. We design a compressor,*i.e.* a mapping, $\varphi(z;\xi)$ from the distribution space U_ξ (parameterized by $z = z_1 + iz_2$) to the quantization space $\mathcal{C}$(parameterized by w), such that $\varphi(\xi;\xi) = 0$.

At first let $l(z) := \ln \tilde{g}(z)$, and define a holomorphic function

$$L(z;\xi) := l(\xi) + (z-\xi)\partial l(\xi) + \frac{1}{4}(z-\xi)^2 \partial^2 l(\xi), \tag{3}$$

where $\partial = \frac{\partial}{\partial z_1} - i\frac{\partial}{\partial z_2}$. Using this function we define

$$g(z) := c_\xi |e^{L(z;\xi)}| \text{ for } z \in U_\xi, \tag{4}$$

where the normalizing constant c_ξ is determined such that $g(U_\xi) = \tilde{g}(U_\xi)$.

For a phase $\theta(\xi) \in [0, 2\pi]$ given at ξ, we design the compressor by the complex integral

$$\varphi(z;\xi) = \int_\xi^z \sqrt{c_\xi} \exp\{\frac{1}{2} L(z;\xi) - \theta(\xi) i\} dz. \tag{5}$$

The inverse image of this function of a hexagonal lattice spanned by λ and $\lambda e^{\frac{\pi}{3} i}$, with the lattice constant $\lambda = \frac{\sqrt{2}}{\sqrt[4]{3}\sqrt{N}}$, approximate the optimal quantizer. We can also argue that the angular phase $\theta(\xi)$ satisfies the partial differential equation:

$$\frac{\partial}{\partial \xi_i} \theta(\xi) = \sum_{j=1}^{2} \frac{1}{2} \epsilon_{ij} \frac{\partial}{\partial \xi_j} l(\xi), \tag{6}$$

through our two-stage model, where ϵ_{ij} being of Eddington. We can also verify this by experiments[4].

Define the optimal distortion as $D_\infty := N^{-\beta} R_{2,s} \int \tilde{g}(x)^{-\beta} p(x) dx$. Let $Ng(x)$ be the actual quantizer number density defined as above and let it yield a distortion D_g. Then the relative distortion mismatch can be formulated as follows. We assume that N is large enough while the number of partitioned domain is finite.

Fact

$$\frac{D_g - D_\infty}{D_\infty} \sim \frac{\beta(\beta+1)}{2} \sum_\xi \tilde{g}(U_\xi) \{A \textit{ variance of } \frac{1}{4}\|x-\xi\|^2 \triangle l(\xi) \textit{ with } \tilde{g}(\cdot|U_\xi).\} \tag{7}$$

where $\tilde{g}(\cdot|U_\xi)$ is a conditional distribution of $\tilde{g}$ in U_ξ, and the asymptotics hold when the diameters of U_ξs are sufficiently small, and $\triangle$ represents the Laplacian operator.

Both 'domain effect' and 'boundary effect' can contribute to the actual relative distortion mismatch. When the cluster centers have a number density $N_q k(z)$, where $\int k(z) = 1$, and if $1 << N_q << N^{1/5}$, and also under a working assumption that the cluster centers form a Voronoi diagram with each Voronoi cell being almost regular hexagon, then the formula (7) takes the following minimum:

$$\frac{\beta(\beta+1)}{32 {N_q}^2} (R_{2,4} - R_{2,2}^2) \frac{\rho^2}{\int p^\rho} \{\int p(x)^{\rho/3} (\triangle \ln p(x))^{2/3}\}^3, \tag{8}$$

when $k(x) = const.p(x)^{\rho/3} (\triangle \ln p(x))^{2/3}$.

[1] A part of the work was done while the author stayed in 1996 at Information Systems Laboratory, Dept. of EE, Stanford Univ.

References

[1] A.Heppes and P.Szüsz,El.Math.,vol.15,pp.134-136,1960.
[2] J. A. Bucklew, *IEEE-IT*, vol. 29, p. 279, Feb. 1983.
[3] T. Kawabata and H. Nakanishi, Proceedings of the IEICE Spring Conference,vol.6,p.4,1985.
[4] T. Kawabata and K. Uchiyama, The 9th symposium on Science on Form,pp.26-27,1987.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On the Whiteness of High Resolution Quantization Errors

Harish Viswanathan
Lucent Technologies Bell Labs
Holmdel
NJ 07733, U.S.A
e-mail: harishv@lucent.com

Ram Zamir
Department of Electrical
Engineering - Systems
Tel Aviv University, Israel
e-mail: zamir@eng.tau.ac.il

Abstract — **A common belief in quantization theory says that the quantization noise process resulting from uniform scalar quantization of a correlated discrete time process tends to be *white* in the limit of small distortion ("high resolution"). We show that the quantization errors resulting from independent non-uniform, vector quantizations of dependent real random vectors become asymptotically uncorrelated if the joint Fisher information under translation of the two vectors is finite and the quantization cells shrink uniformly as the distortion tends to zero.**

I. Introduction

The Asymptotic Whiteness Property (AWP) of the quantization error process [2, sec. 5.6] says that the quantization noise process resulting from uniform scalar quantization of a correlated discrete time process tends to be *white* in the limit of small distortion ("high resolution"). The AWP also gives interesting insight into the behavior of multiterminal coding of correlated continuous sources [3], where the correlation between the errors at separate terminals may affect the estimation error at the centralized decoder. Our main result in this paper generalizes the AWP to *non-uniform* quantization. Unlike lattice quantization, in this case the quantization cells are not necessarily convex, and may be even unions of disconnected regions, as happens in the case of multiterminal source coding [3]. However, while a sufficient condition for AWP for vector *lattice* quantization is that the pair X_n and X_{n+k} have a joint probability density function and finite power, the more general formulation of the AWP requires stronger conditions on the joint distribution of (X_n, X_{n+k}).

The intuition behind the AWP comes from the combination of two ideas:

1. **Local uniformity:** If the joint distribution of the source samples is "smooth", then it is approximately uniform inside small cells (corresponding to high resolution quantization).
2. **Rectangular partition:** Independent quantization of random variables $X \in \mathcal{X}$ and $Y \in \mathcal{Y}$ induces a rectangular ("Cartesian") partitioning of the $(\mathcal{X}, \mathcal{Y})$-plane.

The property of rectangular partition above seems simple and clear. The main purpose of this paper is to make a precise statement of the idea of local uniformity, to propose a sufficient condition for it to hold and to prove a general form of the AWP using the local uniformity condition. For lattice quantization existence of the joint probability density of the source turns out to be sufficient. For general non-uniform quantization our condition is based on the finiteness of the *Fisher Information under translation* [1], a quantity which is a function of the joint distribution of the source samples and a *moment condition* defined below (2).

II. Summary of Results

Let $\mathbf{X} \in \mathcal{X}, \mathbf{Y} \in \mathcal{Y}$, where $\mathcal{X} = \mathcal{Y} = \mathcal{R}^k$, be random vectors with joint density $p(\mathbf{x}, \mathbf{y})$. Let

$$i(\mathbf{x}) : \mathcal{X} \to \{1, 2, \ldots, N_x\}, \quad j(\mathbf{y}) : \mathcal{Y} \to \{1, 2, \ldots, N_y\}$$

induce two partitions of $\mathcal{R}^k$ corresponding to *independent* quantization of $\mathbf{X}$ and $\mathbf{Y}$, respectively. Let $(\hat{\mathbf{x}}, \hat{\mathbf{y}}) = Q\Big(i(\mathbf{x}), j(\mathbf{y})\Big)$ denote the quantizer reconstruction. We define $Q(i, j)$ to be the joint centroid of the cell relative to the source distribution.

Consider a sequence of pairs of partition functions $i_N(\mathbf{x}), j_N(\mathbf{y})$ of $\mathcal{X}, \mathcal{Y}$, $N = 1, 2, \ldots$, and a corresponding sequence of reconstruction functions $(\hat{\mathbf{x}}_N, \hat{\mathbf{y}}_N)$, such that

$$D_{x,N} \triangleq E\|\mathbf{X} - \hat{\mathbf{X}}_N\|^2 \to 0, \quad D_{y,N} \triangleq E\|\mathbf{Y} - \hat{\mathbf{Y}}_N\|^2 \to 0. \quad (1)$$

at the same rate. Assume that there exists some $\delta > 0$ such that

$$\limsup_{N\to\infty} \; E\left(\frac{\|\mathbf{X} - \hat{\mathbf{X}}_N\|^2}{D_{x,N}}\right)^{1+\delta}, E\left(\frac{\|\mathbf{Y} - \hat{\mathbf{Y}}_N\|^2}{D_{y,N}}\right)^{1+\delta} < \infty. \quad (2)$$

Define the joint Fisher Information (FI) under translation of $(\mathbf{X}, \mathbf{Y})$ [1] as

$$J(\mathbf{X}, \mathbf{Y}) \triangleq \int \frac{1}{p(\mathbf{x}, \mathbf{y})} \cdot \left\| \frac{\partial p(\mathbf{x}, \mathbf{y})}{\partial (\mathbf{x}, \mathbf{y})} \right\|^2 d\mathbf{x}d\mathbf{y} \, .$$

Theorem 1 *Let $(\mathbf{X}, \mathbf{Y}) \in (\mathcal{X}, \mathcal{Y})$, where $\mathcal{X} = \mathcal{Y} = \mathcal{R}^k$, be correlated random vectors with continuous source density $p(\mathbf{x}, \mathbf{y})$, a.s. continuously differentiable $\ln p(\mathbf{x}, \mathbf{y})$ and joint FI $J(\mathbf{X}, \mathbf{Y}) < \infty$. Let $i_N(\mathbf{x})$ and $j_N(\mathbf{y})$ be a sequence of independent partition functions of $\mathcal{X}$ and $\mathcal{Y}$, let $\hat{\mathbf{x}}_N$ and $\hat{\mathbf{y}}_N$ be the corresponding reconstructions, and let*

$$\rho_N \triangleq \frac{E\{(\mathbf{X} - \hat{\mathbf{X}}_N)^t (\mathbf{Y} - \hat{\mathbf{Y}}_N)\}}{\sqrt{D_{x,N} D_{y,N}}} \quad (3)$$

be the correlation coefficient between the quantization errors. If the sequence $(\hat{\mathbf{x}}_N, \hat{\mathbf{y}}_N)$ satisfies (1) and (2), then

$$\rho_N \to 0 \quad as \quad N \to \infty. \quad (4)$$

Acknowledgments

We thank Toby Berger and Tamas Linder for several discussions that helped improve the paper.

References

[1] T. M. Cover and J. A. Thomas. *Elements of Information Theory.* Wiley, New York, 1991.

[2] A. Gersho and R. M. Gray. *Vector Quantization and Signal Compression.* Kluwer Academic Pub., Boston, 1992.

[3] R. Zamir and T. Berger. Multiterminal source coding with high resolution. *IEEE Trans. Information Theory,*IT-45:106–117, January 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Worst-case rate of scalar vs. vector quantization

Alon Orlitsky[1]
ECE Department, UCSD, La Jolla, CA 92093, alon@ucsd.edu

Abstract — **We show that there can be an arbitrary discrepancy between the worst-case rate required for scalar and vector quantization. Specifically, that for every δ, however large, and every $\epsilon > 0$, however small, there is a random variable and a distortion measure where quantization of a single instance within a given distortion requires more than δ bits in the worst case, but quantization of multiple *independent* instances within the same distortion requires at most ϵ bits per instance in the worst case. Furthermore, these discrepancies can be achieved by simple distortion measures that attain just two values: 0 and ∞.**

I. Summary

The results follow from a judicious application of the following examples.

Example 1 (Mail order, see Slepian, Wolf, and Wyner [1] for average-case analysis.) A mail-order firm sells n different shirts. Experience has shown that each customer likes m of the n shirts and wants to get just one of them. For example, a customer may like all m blue shirts and have no preference for one blue shirt over another, while another customer may want to buy any one of the m shirts designed by Giorgio Armani.

The firm designs a new order form. It would like to know the shortest length of the reply field which the customer fills out to request one of his m favorite shirts. In other words, the firm is interested in $\hat{L}(n,m)$, the smallest number of bits the customer must specify for the "worst" set of m shirts. Note that n and m are known in advance and the only uncertainty is which set of m shirts the customer likes.

For example, if $m = 1$ every customer likes exactly one shirt and wants to get it. Clearly the shirt must be completely specified, so $\hat{L}(n,1) = \lceil \log n \rceil$. On the other extreme, if $m = n$ each customer likes all n shirts and the firm can mail him any of them. Hence no bits need to be transmitted, so $\hat{L}(n,n) = 0$.

One can show (proof in full version) that in general,

$$\hat{L}(n,m) = \lceil \log(n-m+1) \rceil. \quad (1)$$ □

Next we consider independent repetitions of the previous scenario and compare the number of bits required by treating each case individually to their combined treatment.

Example 2 (Multiple mail orders.) The mail-order firm expands into k product lines. In addition to shirts it now sells, say, pants, shoes and $(k-3)$ other product lines. Again, all customers exhibit the same buying pattern: Every customer considers all k product lines. In each line the customer likes m items and wants to receive one. There is no relation between the items liked in different product lines.

For example, a customer may like all m striped shirts, all m pants whose catalog number is a prime, and so on for the other lines. He then wants to get one striped shirt, one prime-numbered pair of pants, etc.

We are interested in $\hat{L}_k(n,m)$, the number of bits the customer must transmit in the worst case. No errors are tolerated, so the customer always receives k products, one from each line, and likes all of them. By definition, $\hat{L}_1(n,m) = \hat{L}(n,m)$. We would like to know how $\hat{L}_k(n,m)$ grows with k.

By treating each product line separately and describing the smallest-numbered desirable item in each line, we see that

$$\hat{L}_k(n,m) \le \lceil \log(n-m+1)^k \rceil \approx k\lceil \log(n-m+1) \rceil = k\hat{L}(n,m).$$

Since the sets of desirable items in different product lines (say shirts and pants) are completely independent of each other, knowing one set conveys no information about the other. One could therefore be tempted to believe that this upper bound is tight, and only roundoff bits ($\lceil k \log(n-m+1) \rceil$ vs. $k\lceil \log(n-m+1) \rceil$) can be saved. This is not the case. We show that for every integers $m \le n$ and k,

$$\hat{L}_k(n,m) \le k \log \frac{n}{m} + \log n + \log k. \quad (2)$$

The proof is similar to one used in Alon and Orlitsky [2] and will be provided in the full version of this paper.

To gain intuition about this result, suppose first that n is even and $m = n/2$. Namely, each customer likes half the items in each line. Specifying one item takes

$$\hat{L}(n, \frac{n}{2}) = \lceil \log(n - \frac{n}{2} + 1) \rceil = \lceil \log(\frac{n}{2} + 1) \rceil$$

bits. For multiple lines, the customer can describe each line separately using $\lceil k \cdot \log(n/2+1) \rceil \ge k \cdot (\log n - 1)$ bits. However, Inequality (2) shows that the number of bits needed is

$$\hat{L}_k(n, n/2) \le k \cdot \log \frac{n}{n/2} + \log n + \log k = \log n + k + \log k.$$

It follows that while the first product line takes $\log n - 1$ bits to describe, the second product line requires at most two additional bits, and subsequent lines add even fewer bits. In the limit, the number of bits per line is only $\lim_{k\to\infty} (\log n + k + \log k)/k = 1$. Significantly less than the $\log n - 1$ bits per line needed to describe each line separately.

Returning to the general case of Inequality (2), we see that after the initial $\log(n-m+1)$ bits, additional product lines require about $\log \frac{n}{m}$ bits per line. Consequently, for every δ, however large, and every $\epsilon > 0$, however small, one can choose m and n so that a single line would require $> \delta$ bits while multiple lines would need $< \epsilon$ bits per instance. □

The average-case analysis of Example 2 will be carried out in the full version of this paper.

References

[1] D. Slepian, A.D. Wyner, and J.K. Wolf. A note on specifying one of k items from a list of n items. Technical report, Bell Laboratories, 1973.

[2] N. Alon and A. Orlitsky. Repeated communication and Ramsey graphs. *IEEE Transactions on Information Theory*, 41(5):1276–1289, September 1995.

[1]Supported by NSF Grant #CCR-9815018.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Achievable rates of random number generators for an arbitrary prescribed distribution from an arbitrary given distribution

Takahiro Yoshida*
School of Science and Engneering
Waseda University
Shinjuku-ku, Tokyo, Japan.
takahiro@matsu.mgmt.waseda.ac.jp

Toshiyasu Matsushima
School of Science and Engneering
Waseda University
Shinjuku-ku, Tokyo, Japan.

Shigeichi Hirasawa
School of Science and Engneering
Waseda University
Shinjuku-ku, Tokyo, Japan.

Abstract — **In this paper, we show maximal rates in the case that random number generators generate a random sequence with an arbitrary prescribed distribution from a random sequence with an arbitrary given distribution.**

I. Introduction

One of generalizing the random number generation problem is to relax the requirement that the target random numbers should be generated exactly according to the prescribed distribution. We are especially concerned with the case of the fixed length random number generation. Let $\mathcal{X}$ and $\mathcal{Y}$ be countable infinite set. Let us define a general source as an infinite sequence $\mathbf{X} = \{X^n\}_{n=1}^{\infty}$ of n-dimensional random variable X^n taking value in $\mathcal{X}^n$ and $\mathbf{Y} = \{Y^m\}_{m=1}^{\infty}$ of m-dimensional random variable Y^m taking value in $\mathcal{Y}^m$.

In this paper, we shall investigate into maximal rate in the case that random number generators generate a random sequence with an arbitrary prescribed distribution from a random sequence with an arbitrary given distribution in the sense of vanishing variational distance. The variational distance between two distributions P_z and $P_{\hat{z}}$ on $\mathcal{Z}$ is defined as follows

$$d\left(Z,\hat{Z}\right) = \sum_{z\in\mathcal{Z}} |P_Z(z) - P_{\hat{Z}}(z)|. \quad (1)$$

In this setting, there are two types of the case for the fixed length random number generation. One is that every source n_m symbol realization is deterministically transformed into a sequence with length m where n_m depends only on m. The other is that every source n symbol realization is deterministically transformed into a sequence with length m_n.

II. Formulation of the problem

Definition II. 1 *R is called a type A achievable rate for the source $\mathbf{X}$ and $\mathbf{Y}$ if there exists a sequence of mappings $\varphi_n : \mathcal{X}^n \to \mathcal{Y}^{m_n}$ such that*

$$\liminf_{n\to\infty} \frac{m_n}{n} \geq R \quad (2)$$

and

$$\lim_{n\to\infty} d(Y^{m_n}, \varphi_n(X^n)) = 0. \quad (3)$$

Moreover the supremum of R that are type A achievable rate for the source $\mathbf{X}$ and $\mathbf{Y}$ is denoted by $S_A(\mathbf{X},\mathbf{Y})$ which we call maximal type A achievable rate.

Definition II. 2 *R is called a type B achievable rate for the source $\mathbf{X}$ and $\mathbf{Y}$ if there exists a sequence of mappings $\varphi_m : \mathcal{X}^{n_m} \to \mathcal{Y}^m$ satisfying the condition that n_m and m replace n and m_n respectively in Formula (2) and (3). Moreover the supremum of R that are type B achievable rate for the source $\mathbf{X}$ and $\mathbf{Y}$ is denoted by $S_B(\mathbf{X},\mathbf{Y})$ which we call maximal type B achievable rate.*

*This research was supported in part of Waseda University under Grant 99A-551 for Special Research Projects.

III. Main Results

We denote the *limsup in probability* of $\left\{\frac{1}{n}\log\frac{1}{P_{Z^n}(Z^n)}\right\}_{n=1}^{\infty}$ and the *liminf in probability* of that by $\overline{H}(\mathbf{Z})$ and $\underline{H}(\mathbf{Z})$, respectively[1][2][3]. Then we have

Theorem III. 1

$$\frac{\underline{H}(\mathbf{X})}{\overline{H}(\mathbf{Y})} \leq S_A(\mathbf{X},\mathbf{Y}) \leq \min\left(\frac{\underline{H}(\mathbf{X})}{\underline{H}(\mathbf{Y})}, \frac{\overline{H}(\mathbf{X})}{\overline{H}(\mathbf{Y})}\right), \quad (4)$$

$$\frac{\underline{H}(\mathbf{X})}{\overline{H}(\mathbf{Y})} \leq S_B(\mathbf{X},\mathbf{Y}) \leq \min\left(\frac{\underline{H}(\mathbf{X})}{\underline{H}(\mathbf{Y})}, \frac{\overline{H}(\mathbf{X})}{\overline{H}(\mathbf{Y})}\right). \quad (5)$$

We notice that if either source $\mathbf{X}$ or source $\mathbf{Y}$ satisfies the *strong converse property*[3], then

$$S_A(\mathbf{X},\mathbf{Y}) = S_B(\mathbf{X},\mathbf{Y}) = \frac{\underline{H}(\mathbf{X})}{\overline{H}(\mathbf{Y})}. \quad (6)$$

In the case that source $\mathbf{Y}$ is uniform distribution, i.e., $P_Y(Y) = 1/M$ $(M < \infty)$, by replacing m_n with $\log M_n$ in Formula (2) of definition II. 1 , it is equivalent to the intrinsic randomness problem defined by Vembu and Verdú[1]. Then,

$$S_A(\mathbf{X},\mathbf{Y}) = \underline{H}(\mathbf{X}), \quad (7)$$

where $M_n = M^{m_n}$. On the other hand, in the case that source $\mathbf{X}$ is uniform distribution, i.e., $P_X(X) = 1/M$, by replacing n_m with $\log M_m$ in definition II. 2 , the minimum of reciprocal number of type B achievable rate is equivalent to the minimal achievable resolvability rate defined by Han and Verdú[2], i.e.,

$$\frac{1}{S_B(\mathbf{X},\mathbf{Y})} = \overline{H}(\mathbf{Y}), \quad (8)$$

where $M_m = M^{n_m}$.

For the reasons stated above, essence of which maximal achievable rate is uniquely decidable is that either source $\mathbf{X}$ or source $\mathbf{Y}$ satisfies the strong converse property. Since uniform distribution satisfy the strong converse property, Both maximal achievable intrinsic randomness rate[1] and minimal achievable resolvability rate[2] are the special case of theorem III. 1 .

IV. Conclusion

We have defined two types of random number generation problem and obtained two maximal achievable rates. Both intrinsic randomness problem[1] and resolvability problem[2] are the special case of our result.

References

[1] S. Vembu and S. Verdú, "Generating Random Bits from an Arbitrary Source: Fundamental Limits," *IEEE Trans. Inf. Theory*, vol. 41, no.5, pp.1322-1332, Sept. 1995

[2] T. S. Han and S. Verdú, "Approximation theory of output statistics," *IEEE Trans. Inf. Theory*, vol.39, no.3, pp.752-772, May 1993

[3] T. S. Han, "Information-Spectrum methods in information theory," Baifukan, Tokyo, 1998 (In Japanese)

0-7803-5857-0/00/$10.00 ©2000 IEEE.

An Information–Spectrum Approach to Rate–Distortion Function with Side Information

Ken-ichi IWATA
Department of Communication and Culture, Matsuyama Shinonome College,
3-2-1 Kuwabara Matsuyama Ehime, 790-8531 Japan. e-mail: iwata@shinonome.ac.jp

Abstract — **We describe an information-spectrum approach to rate-distortion function with side information at the decoder for the general class of non-stationary and/or nonergodic sources, where the distortion measure is arbitrary and may be nonadditive. We establish a general formula for the rate-distortion function of the Wyner-Ziv problem[1] for the general sources with the maximum distortion criterion under fixed-rate coding.**

Let us define a general source $\mathbf{X}$ as an infinite sequence $\mathbf{X} = \left\{X^n = \left(X_1^{(n)}, X_2^{(n)}, \cdots, X_n^{(n)}\right)\right\}_{n=1}^{\infty}$ of n-dimensional random variables X^n, where each component random variable $X_i^{(n)}, (1 \le i \le n)$ takes values in countably infinite sets $\mathcal{X}$ that we call the source alphabets. We use the convention defined in Han[2]. We consider the class of correlated sources $\mathbf{X} = \{X^n\}_{n=1}^{\infty}, \mathbf{Y} = \{Y^n\}_{n=1}^{\infty}$ that are quit general. We use $\mathbf{X}$ as the source for encoder and use $\mathbf{Y}$ as the side information for decoder as shown in Fig.1.

In order to define a distortion measure, we need to specify another countably infinite set $\hat{\mathcal{X}}$, which is called the reproduction alphabet. Then, $d_n(\mathbf{x}, \hat{\mathbf{x}})$ is called the distortion between $\mathbf{x} \in \mathcal{X}^n$ and $\hat{\mathbf{x}} \in \hat{\mathcal{X}}^n$, $d_n : \mathcal{X}^n \times \hat{\mathcal{X}}^n \to [0, \infty)$, and the normalized distortion is bounded by $d_{\max}$ such that $\frac{1}{n} d_n(\mathbf{x}, \hat{\mathbf{x}}) \le d_{\max}$ for all $\mathbf{x} \in \mathcal{X}^n, \hat{\mathbf{x}} \in \hat{\mathcal{X}}^n$. Furthermore, let us consider any reproduction process $\hat{\mathbf{X}}$ of n-dimensional random variables $\hat{X}^n$. Moreover, we need the concept of "lim sup in probability". For any sequence $\{A_n\}_{n=1}^{\infty}$ of random variables, the infimum of α such that $\lim_{n\to\infty} \Pr\{A_n > \alpha\} = 0$ is called the lim sup in probability of $\{A_n\}_{n=1}^{\infty}$ and is indicated by p-lim sup$_{n\to\infty} A_n$. Then we consider the sequence of the normalized distortions $\left\{\frac{1}{n} d_n(X^n, \hat{X}^n)\right\}_{n=1}^{\infty}$, and the lim sup in probability of which is denoted by $\overline{D}(\mathbf{X}, \hat{\mathbf{X}})$, i.e., $\overline{D}(\mathbf{X}, \hat{\mathbf{X}}) = \text{p-lim sup}_{n\to\infty} \frac{1}{n} d_n(X^n, \hat{X}^n)$.

A code is defined by two mappings: Encoder $\varphi_n : \mathcal{X}^n \to \mathcal{I}_{k_n}$ and Decoder $\psi_n : \mathcal{I}_{k_n} \times \mathcal{Y}^n \to \hat{\mathcal{X}}^n$, where $\mathcal{I}_{k_n} = \{1, 2, \cdots, k_n\}$. The limit superior of the code length per source letter $\limsup_{n\to\infty} \frac{1}{n} \log |\varphi_n|$ is called the rate of the encoder φ_n, where $|\varphi_n|$ denotes the cardinality of range of φ_n.

For given general source $\mathbf{X}$ and distortion D, a pair R is called achievable with side information $\mathbf{Y}$ if there exists a code (φ_n, ψ_n) such that p-lim sup$_{n\to\infty} \frac{1}{n} d_n(X^n, \psi_n(Y^n, \varphi_n(X^n)))$ $\le D$ and $\limsup_{n\to\infty} \frac{1}{n} \log |\varphi_n| \le R$. Moreover, $R(D) = \inf\{R | R$ is achievable with side information for given $D\}$.

In order to give the characterization of the general rate-distortion functions, we define the mutual information spectrum-sup. Given any three correlated processes, $\mathbf{X} = \{X^n\}_{n=1}^{\infty}$, $\mathbf{Y} = \{Y^n\}_{n=1}^{\infty}$ and $\mathbf{Z} = \{Z^n\}_{n=1}^{\infty}$, we define the sequence of the normalized information densities

$$\left\{\frac{1}{n} \log \frac{P_{Z^n|X^nY^n}(Z^n|X^nY^n)}{P_{Z^n|Y^n}(Z^n|Y^n)}\right\}_{n=1}^{\infty}, \tag{1}$$

where we use the convention that $P_{Y|X}$ denotes the conditional probability distribution of Y given X. Then the lim sup in probability of (1) is denoted by $\overline{I}(\mathbf{X}; \mathbf{Z}|\mathbf{Y})$, i.e., $\overline{I}(\mathbf{X}; \mathbf{Z}|\mathbf{Y}) = \text{p-lim sup}_{n\to\infty} \frac{1}{n} \log \frac{P_{Z^n|X^nY^n}(Z^n|X^nY^n)}{P_{Z^n|Y^n}(Z^n|Y^n)}$, which we call the conditional mutual information spectrum-sup.

Theorem 1 For given $\mathbf{X}, \mathbf{Y}$ and D,

$$R(D) = \inf \overline{I}(\mathbf{X}; \mathbf{Z}|\mathbf{Y}),$$

where inf is over $\mathbf{Z}$ and $\{f_n(\cdot,\cdot)\}_{n=1}^{\infty}$ satisfy next a) and b),

a) $Y^n - X^n - Z^n$ is a Markov chain for $n = 1, 2, \cdots$, hence, $P_{X^nY^nZ^n}(\mathbf{x}, \mathbf{y}, \mathbf{z}) = P_{X^nY^n}(\mathbf{x}, \mathbf{y}) P_{Z^n|X^n}(\mathbf{z}|\mathbf{x})$ holds for all $n = 1, 2, \cdots$ and for all $\mathbf{x} \in \mathcal{X}^n, \mathbf{y} \in \mathcal{Y}^n$, and $\mathbf{z} \in \mathcal{Z}^n$.

b) there exists a sequence of function $\{f_n(\cdot,\cdot)\}_{n=1}^{\infty}, f_n : \mathcal{Y}^n \times \mathcal{Z}^n \to \hat{\mathcal{X}}^n$ such that $\hat{\mathbf{X}} = \{f_n(Y^n, Z^n)\}_{n=1}^{\infty}$, and $\overline{D}(\mathbf{X}, \hat{\mathbf{X}}) \le D$.

In order to specify the code, we need a function $F_n : \mathcal{X}^n \to \{\mathbf{z}_i\}_{i=1}^{M_n'} \subset Z^n$, where $M_n' \le e^{n(\overline{I}(\mathbf{X};\mathbf{Z})+\gamma)}$ and $\gamma > 0$. F_n is due to an extended version[3] of Lemma 4.3 of [4].

1. Generation of codebook: Let $M_n = e^{n(\overline{I}(\mathbf{X};\mathbf{Z}|\mathbf{Y})+2\gamma)}$, and make M_n bins. Randomly assign the $F_n(\mathbf{x}), \mathbf{x} \in \mathcal{X}^n$ to one of M_n bins using a uniform distribution over the bins.

2. Encoding $\varphi_n : \mathcal{X}^n \to \mathcal{I}_{M_n}$. Given a source output $\mathbf{x} \in \mathcal{X}^n$ from $\mathbf{X}$, the encoder looks for a $\mathbf{z}_i = F_n(\mathbf{x})$. Then, the encoder sends the index $j \in I_{M_n}$ of the bin such that $\mathbf{z}_i$ belongs one.

3. Decoding $\psi_n : \mathcal{I}_{M_n} \times \mathcal{Y}^n \to \hat{\mathcal{X}}^n$. Decoder receives an output $j = \varphi_n(\mathbf{x})$ from encoder and receives a output $\mathbf{y} \in \mathcal{Y}^n$ as the side information from $\mathbf{Y}$. If he can find a unique $\mathbf{z}_i$ which belongs bin of the index j and satisfies $(\mathbf{z}_i, \mathbf{y}) \in \left\{(\mathbf{y}, \mathbf{z}) \in \mathcal{Y}^n \times \mathcal{Z}^n \middle| \frac{1}{n} \log \frac{P_{Z^n|X^nY^n}(\mathbf{z}|\mathbf{x},\mathbf{y})}{P_{Z^n|Y^n}(\mathbf{z}|\mathbf{y})} < \overline{I}(\mathbf{X}; \mathbf{Z}|\mathbf{Y}) + \gamma\right\}$, then he has $\psi_n(j, \mathbf{y}) = f_n(\mathbf{y}, \mathbf{z}_i)$ by using $f_n(\cdot,\cdot)$ defined in property b). If he does not find such a unique $\mathbf{z}_i$, then he sets $\psi_n(j, \mathbf{y}) = \hat{\mathbf{x}}$ where $\hat{\mathbf{x}}$ is an arbitrary sequence in $\hat{\mathcal{X}}^n$.

The converse part is due to a modified version of Lemma 2.4 of [2].

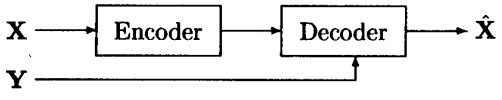


Figure 1: Wyner-Ziv type communication system.

Acknowledgments

The author thanks Dr. Jun Muramatsu and anonymous reviewer for their valuable comments in obtaining the results.

References

[1] A. D. Wyner and J. Ziv, "The rate-distortion function for source coding with side information at the decoder," *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 1-10, Jan. 1976.

[2] T. S. Han, "Information-spectrum methods in information theory," Baifuukan, Tokyo (in Japanese), Apr. 1998.

[3] S. Miyake and F. Kanaya, "Coding theorems on correlated general sources," *IEICE Trans. on Fundamentals*, vol. E78-A, pp. 1063-1070, Sept. 1995.

[4] A. D. Wyner, "On source coding with side information at the decoder," *IEEE Trans. Inform. Theory*, vol. IT-21, pp. 294-300, May 1975.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

General Formulas for Csiszár's Source Coding Cutoff Rates

Po-Ning Chen
Dept. of Communication Eng.
National Chiao Tung Univ.
Hsin Chu, Taiwan 30050, R.O.C.
email: poning@cc.nctu.edu.tw

Fady Alajaji
Dept. of Mathematics and Statistics
Queen's Univ., Kingston
Ontario K7L 3N6, Canada
email: fady@polya.mast.queensu.ca

Abstract — **In this work, Csiszár's fixed-length source coding β-cutoff rates are investigated for the class of arbitrary discrete sources with memory. It is demonstrated that the limsup and liminf Rényi entropy rates provide the formulas for the forward and reverse β-cutoff rates, respectively. Consequently, new fixed-length source coding operational characterizations for the Rényi entropy rates are established.**

I. Introduction

In [2], Csiszár establishes the concept of generalized fixed-length source coding cutoff rates (forward and reverse) for discrete memoryless sources. More specifically, given $\beta > 0$, he defines the forward β-cutoff rate for a source $\{X_i\}_{i=1}^{\infty}$ as the number R_0 that provides the best possible lower bound in the form $\beta(R - R_0)$ to the source reliability function. This definition implies that the source error probability is guaranteed to exponentially decay with a linear exponent of specified slope β for $R > R_0$. He also provides a similar definition for the reverse β-cutoff rate (where $\beta > 0$) with respect to the source unreliability function (the exponent of the vanishing probability of correct decoding). He then demonstrates that the forward and reverse β-cutoff rates are respectively given by $H_{1/(1+\beta)}(X_1)$ and $H_{1/(1-\beta)}(X_1)$, where $H_\alpha(X_1)$ denotes the Rényi entropy of order α.

In this work, we extend Csiszár's results [2] by investigating the β-cutoff rate for arbitrary (not necessarily, stationary, ergodic, etc.) discrete-time finite-alphabet sources $\mathbf{X} \triangleq \{X^n = (X_1^{(n)}, \ldots, X_n^{(n)})\}_{n=1}^{\infty}$ [3]. We demonstrate that the limsup and liminf Rényi entropy rates provide the expressions for the forward and reverse β-cutoff rates, respectively. These results also provide simple, and in certain cases, computable lower bounds to the source reliability and unreliability functions.

II. Main results

Definition 1 An (n, M) fixed-length source code for X^n is a collection of M n-tuples $\mathcal{C}_n = \{c_1^n, \ldots, c_M^n\}$. The error probability of the code is $P_e(\mathcal{C}_n) \triangleq P_{X^n}[X^n \notin \mathcal{C}_n]$.

Definition 2 Fix $e > 0$. $R > 0$ is *e-achievable* for a source $\mathbf{X}$, if there exists a sequence of (n, M_n) fixed-length source code $\mathcal{C}_n$ such that

$$\limsup_{n\to\infty} \frac{1}{n} \log M_n \le R \quad \text{and} \quad \liminf_{n\to\infty} -\frac{1}{n} \log P_e(\mathcal{C}_n) \ge e.$$

Fix $\beta > 0$. The *forward β-cutoff rate* for $\mathbf{X}$, denoted by $R_0^{(f)}(\beta|\mathbf{X})$, is defined as the *smallest* $R_0 \ge 0$ such that every $R > 0$ is $\beta(R - R_0)$-*achievable*.

This work was supported in part by Queen's University, NSERC of Canada and NSC of Taiwan, R.O.C.

Theorem 1 (Forward β-cutoff rate [1]) Fix $\beta > 0$. For an arbitrary source $\mathbf{X}$,

$$R_0^{(f)}(\beta|\mathbf{X}) = \limsup_{n\to\infty} \frac{1}{n} H_{1/(1+\beta)}(X^n),$$

where

$$H_\alpha(X^n) \triangleq \frac{1}{1-\alpha} \log \sum_{x^n \in \mathcal{X}^n} P_{X^n}^{\alpha}(x^n)$$

is the (n-dimensional) Rényi entropy of order α.

Definition 3 Fix $e > 0$. $R > 0$ is *reverse e-achievable* for a source $\mathbf{X}$, if there exists a sequence of (n, M_n) fixed-length source code $\mathcal{C}_n$ such that

$$\limsup_{n\to\infty} \frac{1}{n} \log M_n \le R \quad \text{and} \quad \liminf_{n\to\infty} -\frac{1}{n} \log(1 - P_e(\mathcal{C}_n)) \le e.$$

Fix $\beta > 0$. The *reverse β-cutoff rate* for $\mathbf{X}$, denoted by $R_0^{(r)}(\beta|\mathbf{X})$, is defined as the *largest* R_0 such that every $R > 0$ is *reverse* $\beta(R - R_0)$-*achievable*.

Theorem 2 (Reverse β-cutoff rate [1]) Fix $0 < \beta < 1$. For any source $\mathbf{X}$,

$$R_0^{(r)}(\beta|\mathbf{X}) = \liminf_{n\to\infty} \frac{1}{n} H_{1/(1-\beta)}(X^n).$$

III. Conclusions

In closing, we would like to make the following observations.

- It is important to point out that if the source $\mathbf{X}$ is a time-invariant Markov source of arbitrary order, then its Rényi entropy rate exists and can be computed [4]. Thus in this case, the β-cutoff rates for this source can be obtained.
- A convex lower bound can be obtained on the source reliability function. It consists of the supremum of all the support lines with slope β which pass through the point $(R_0^{(f)}(\beta|\mathbf{X}), 0)$, given by $\sup_{\beta>0}[\beta(R - R_0^{(f)}(\beta|\mathbf{X}))]$ for every $R > 0$. We can thus conclude that for the class of sources $\mathbf{X}$ for which the Rényi entropy rate can be calculated (e.g., the class of Markov sources), a computable lower bound to the source reliability function can also be obtained. A similar remark applies for the source unreliability function.

References

[1] P.-N. Chen and F. Alajaji, "Csiszár's Cutoff Rates for Arbitrary Discrete Sources," submitted, 1999.

[2] I. Csiszár, "Generalized cutoff rates and Rényi's information measures," *IEEE Trans. Inform. Theory*, pp. 26–34, Jan. 1995.

[3] T. S. Han, *Information-Spectrum Methods in Information Theory*, (in Japanese), Baifukan Press, Tokyo, 1998.

[4] Z. Rached, F. Alajaji and L. L. Campbell, "Rényi's divergence and entropy rates for finite alphabet Markov sources," submitted, 2000.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Coding Theorems on Shannon's Cipher System with a General Source

Hiroki Koga
Institute of Engineering Mechanics and Systems, University of Tsukuba
1-1-1 Tennoudai, Tsukuba-shi, Ibaraki 305-8573, Japan
e-mail: koga@esys.tsukuba.ac.jp

Abstract — **In this paper we analyze Shannon's cipher system with the general source [1]. We completely determine the achievable rate region of a cryptogram and a key required for encryption of an output of the sources with the one-point spectrum. An inner and an outer bounds are given for the other sources.**

I. Introduction

This paper attempts to analyze Shannon's cipher system [2] from a viewpoint of the information-spectrum method originating from [1]. Figure 1 shows Shannon's cipher system. For each $n \geq 1$ let S^n be a random variable from a source taking values in $\mathcal{S}^n$. The cardinality of alphabet $\mathcal{S}$ is either finite or countably infinite. Let E_n be the uniformly distributed random variable on a finite alphabet $\mathcal{E}_n$ from a key generator. The key E_n is transmitted to both an encoder and a decoder through a secret channel perfectly protected against wiretappers. The encoder encrypts S^n into a cryptogram $W_n \in \mathcal{W}_n$ under E_n as $W_n = f_n(S^n, E_n)$, where f_n is a deterministic function. The encoder transmits W_n to a decoder through a public channel in the presence of the wiretappers. Therefore, W_n is required not to reveal information on S^n. The decoder decrypts W_n under E_n and reproduces S^n with small decoding error probability by using a deterministic function $g_n : \mathcal{W}_n \times \mathcal{E}_n \to \mathcal{S}^n$.

In this paper we consider the case that the decoding error probability tends to zero as $n \to \infty$. We characterize achievable rates required for transmission of W_n and E_n subject to a new criterion on secrecy of the encryption.

II. Coding Theorems for Sources satisfying $\underline{H}(\mathbf{S}) = \overline{H}(\mathbf{S})$

Let $\mathbf{S} = \{S^n\}_{n=1}^{\infty}$ be the general source [1]. Here, the general source means an infinite sequence of random variables not required to satisfy the consistency condition. First we consider general sources with one-point spectrum, i.e., the general sources satisfying $\underline{H}(\mathbf{S}) = \overline{H}(\mathbf{S}) \stackrel{\text{def}}{=} H$, where $\underline{H}(\mathbf{S})$ and $\overline{H}(\mathbf{S})$ are the entropy spectrum-inf and the entropy spectrum-sup defined in [1]. Let $\mathbf{E} = \{E_n\}_{n=1}^{\infty}$ and $\mathbf{W} = \{W_n\}_{n=1}^{\infty}$.

For a given constant $h > 0$, we define the h-achievable region for (R_W, R_E) as follows:

Definition 1 *Let $h \geq 0$ be a given constant. A pair of rates (R_W, R_E) is called h-achievable if there exists a sequence of pairs of an encoder and a decoder $\{(f_n, g_n)\}_{n=1}^{\infty}$ satisfying*

$$\limsup_{n\to\infty} \frac{1}{n} \log_2 |\mathcal{W}_n| \leq R_W, \tag{1}$$

$$\limsup_{n\to\infty} \frac{1}{n} \log_2 |\mathcal{E}_n| \leq R_E, \tag{2}$$

$$\lim_{n\to\infty} \Pr\{g_n(f_n(S^n, E_n), E_n) \neq S^n\} = 0, \tag{3}$$

$$\underline{H}(\mathbf{S}|\mathbf{W}) \geq h, \tag{4}$$

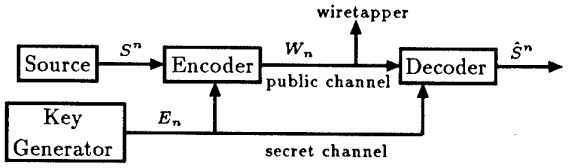


Fig. 1 Block diagram of Shannon's cipher system

where $\underline{H}(\mathbf{S}|\mathbf{W})$ denotes the liminf in probability of $\frac{1}{n}\log_2 \frac{1}{P_{S^n|W_n}(S^n|W_n)}$ and $P_{S^n|W_n}(S^n|W_n)$ denotes the conditional probability of S^n given W_n.

Intuitively, R_W and R_E mean the rates of the public channel and the secret channel for sufficiently large n. Note that (4) means that with probability close to one a pair of a source output $s^n \in \mathcal{S}^n$ and a cryptogram $w_n \in \mathcal{W}_n$ satisfies $P_{S^n|W_n}(s^n|w_n) \leq 2^{-n(h-\gamma)}$ if n is sufficiently large. If (4) is satisfied, a criterion proposed in [3] is always satisfied.

Definition 2 (Achievable Rate Region)

$$\mathcal{R} = \{(R_W, R_E) : (R_W, R_E) \text{ is achievable}\}. \tag{5}$$

Then, we have the following theorem on $\mathcal{R}$.

Theorem 1 *For an arbitrary $h \in (0, H)$,*

$$\mathcal{R} = \mathcal{R}^*,$$

where $\mathcal{R}^* \stackrel{\text{def}}{=} \{(R_W, R_E) : R_W \geq H \text{ and } R_E \geq h\}$.

III. Coding Theorem for General Sources

For encryption of general sources satisfying $\underline{H}(\mathbf{S}) \leq \overline{H}(\mathbf{S})$ we assume that uniformly distributed random variables $\mathbf{U} = \{U_n\}_{n=1}^{\infty}$, $U_n \in \mathcal{U}_n$, are available only to the encoder. We define the achievable region $\mathcal{R}$ for the triplet of R_W, R_E and R_U similarly to Definitions 1–2, where R_U specifies $|\mathcal{U}_n|$ by $\limsup_{n\to\infty} \frac{1}{n}\log_2 |\mathcal{U}_n| \leq R_U$. We have the following bounds:

Theorem 2 *For an arbitrary $h \in (0, \underline{H}(\mathbf{S}))$,*

$$\mathcal{R}_{in}^* \subseteq \mathcal{R} \subseteq \mathcal{R}_{out}^*,$$

where $\mathcal{R}_{in}^* \stackrel{\text{def}}{=} \{(R_W, R_U, R_E) : R_W \geq \overline{H}(\mathbf{S}), R_U \geq \overline{H}(\mathbf{S}) - \underline{H}(\mathbf{S}) \text{and } R_E \geq h\}$ and $\mathcal{R}_{out}^* \stackrel{\text{def}}{=} \{(R_W, R_U, R_E) : R_W \geq \overline{H}(\mathbf{S}), R_U \geq 0 \text{ and } R_E \geq h\}$.

References

[1] T. S. Han and S. Verdú, "Approximation theory of output statistics," *IEEE Trans. on Inform. Theory*, vol. IT-39, pp. 752–772, 1993.

[2] C. E. Shannon, "Communication theory of secrecy systems," *Bell Sys. Tech. J.*, vol. 28, pp. 565 – 715, 1949.

[3] H. Yamamoto, "Coding theorems for Shannon's cipher system with correlated source outputs, and common information," *IEEE Trans. on Inform. Theory*, pp. 85 – 95, 1994.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Adaptive Modulation Using Long Range Prediction for Flat Rayleigh Fading Channels[1]

Shengquan Hu, Alexandra Duel-Hallen*, Hans Hallen**

*North Carolina State University
Dept. of Electrical and Computer Engineering
Box 7914, Raleigh, NC 27695-7914
E-mail: shu@eos.ncsu.edu, sasha@eos.ncsu.edu

**North Carolina State University
Physics Department
Box 8202, Raleigh, NC 27695-8202
E-mail: Hans_Hallen@ncsu.edu

Abstract --- We theoretically analyze the statistical behavior of prediction errors generated by our previously proposed long range prediction algorithm, and investigate adaptive modulation design using predicted channel state information (CSI). Both numerical and simulation results show that accurate prediction of the fading channel far ahead makes adaptive transmission feasible for rapidly time-varying mobile radio channels.

1. Introduction

Adaptive modulation methods depend on accurate channel state information (CSI) that can be estimated at the receiver and sent to the transmitter via a feedback channel. This information would allow the transmitter to choose the appropriate transmitted signal. The feedback delay and overhead, processing delay and practical constraints on modulation switching rates have to be taken into account in the performance analysis of adaptive modulation methods. For very slowly fading channels (pedestrian or low vehicle speeds), *outdated* CSI is sufficient for reliable adaptive system design. However, for rapidly time variant fading that corresponds to realistic mobile speeds, even small delay will cause significant degradation of performance since channel variation due to large Doppler shifts usually results in a different channel at the time of transmission than at the time of channel estimation [1, 2]. To realize the potential of adaptive transmission methods, these channel variations have to be *reliably predicted* at least several milliseconds ahead.

Recently, we have investigated a *novel adaptive long-range fading channel prediction algorithm* in [3]. This algorithm characterizes the fading channel using an autoregressive (AR) model and computes the Minimum Mean Squared Error (MMSE) estimate of a future fading coefficient sample based on a number of past observations. The superior performance of this algorithm relative to conventional methods is due to its *low sampling rate* [3]. Given a *fixed model order*, the lower sampling rate results in *longer memory span*, permitting prediction further into the future. The prediction method is enhanced by an *adaptive tracking* method [3] that increases accuracy, reduces the effect of noise and maintains the robustness of long-range prediction as the physical channel parameters vary.

In this paper, we extend the application of long range channel prediction to adaptive modulation. First, we theoretically analyze the statistical behavior of prediction errors generated by our long range prediction algorithm, and consider adaptive modulation design based on this prediction error model using predicted CSI. Then, we evaluate the performance of adaptive modulation for flat Rayleigh fading channels. The extension of this method to our novel realistic non-stationary fading model and measured data are discussed in [3,4] and references therein.

2. Results

Consider the linear MMSE prediction of the future channel sample $\hat{c}_n$ based on p previous samples $c_{n-1}...c_{n-p}$ as [3]:

$$\hat{c}_n = \sum_{j=1}^{p} d_j c_{n-j} \qquad (1)$$

where the coefficients d_j are determined by the orthogonality principle. We assume that channel samples c_n are modeled as zero-mean complex Gaussian random variables, i.e., the channel is Rayleigh fading. Thus, the amplitude $\alpha = |c_n|$ and its predicted value $\hat{\alpha} = |\hat{c}_n|$ have a bivariate Rayleigh distribution. We define the prediction error β as the ratio of the actual fading gain α and the predicted fading gain $\hat{\alpha}$, i.e., $\beta = \alpha/\hat{\alpha}$. Then the probability density function (pdf) of β can be derived as:

$$p_\beta(x) = \frac{2x(\frac{1}{\lambda}x^2 + \lambda)(1-\rho)}{((\frac{1}{\lambda}x^2+\lambda)^2-4\rho x^2)^{1.5}}, \qquad (2)$$

where the correlation coefficient $\rho = \frac{Cov(\alpha^2,\hat{\alpha}^2)}{\sqrt{Var(\alpha^2)Var(\hat{\alpha}^2)}}$, $0 < \rho < 1$, $\Omega=E\{\alpha^2\}$, $\hat{\Omega} = E\{\hat{\alpha}^2\}$, and $\lambda = \sqrt{\Omega/\hat{\Omega}}$.

We consider the fixed power and modulation level-controlled scheme using Square Multilevel Quadrature Amplitude Modulation (MQAM) signal constellation for the target Bit Error Rate (BER_{tg})= 10^{-3}. We restrict ourselves to MQAM constellations of sizes M = 0, 2, 4, 16, 64. Given fixed transmitter power E_s (or the average Signal-to-Noise Ratio (SNR) level $\bar{\gamma} = E_s/N_0$), to maintain a target BER, we need to adjust the modulation size M according to the instantaneous channel gain $\alpha(t)$. In other words, the adaptive modulation scheme can be specified by the threshold values α_i, i = 1, ..., 4, defined as: when $\alpha(t) \geq \alpha_i$, M_i-QAM is employed, where $M_1 = 2$, $M_i = 2^{2(i-1)}$, i > 1. When perfect CSI $\alpha(t)$ is available, these thresholds can be directly calculated from the BER bound of MQAM for an Additive White Gaussian Noise (AWGN) channel [1]:

$$BER_M \leq 0.2 \exp(-1.5\gamma(t)/(M-1)) \text{ for } M>2, \text{ and}$$
$$BER_2 = Q(\sqrt{2\gamma}), \qquad (3)$$

where $\gamma(t)= \alpha^2(t)\bar{\gamma}$ is the instantaneous received SNR. However, when the predicted CSI $\hat{\alpha}(t)$ is used, the current channel condition is characterized by the distribution of $p(\alpha|\hat{\alpha})$ which can be calculated as:

$$p_{\alpha|\hat{\alpha}}(x) = \frac{1}{\hat{\alpha}} p_\beta(\frac{x}{\hat{\alpha}}) \qquad (4)$$

Then, the BER bound for predicted CSI $\hat{\alpha}$, say BER^*_M, can be obtained by evaluating the expectation of BER_M over β using $p_\beta(x)$ in (2) as:

$$BER^*_M = \int_0^\infty BER_M(\bar{\gamma}x^2\hat{\alpha}^2)p_\beta(x)dx \qquad (5)$$

This indicates that we need to use BER^*_M rather than BER_M to calculate thresholds when only the predicted CSI is available. In our study, we found that when our long range prediction is used for the realistic prediction range, there is small difference between the thresholds calculated using perfect CSI and predicted CSI [4]. This demonstrates that the long range prediction preserves the ideal bit rate while maintaining the target BER. However, from the results in [2], we found that even very small delay will cause great loss of bit rate for fast vehicle speeds when the strongly robust signaling design rule is used without long range prediction. Thus, *accurate long-range prediction is required to achieve the bit rate gain of adaptive MQAM for rapid vehicle speeds and realistic delays.*

References

[1] A. J. Goldsmith and S.G. Chua, "Variable-Rate Variable-power MQAM for Fading Channels",*IEEE Trans Comm*, vol. 45, No 10, pp 1218-1230, Oct 1997.

[2] D. L. Goeckel, "Adaptive Coding for Fading Channels using Outdated Channel Estimates", *Proceedings of VTC*, May 1998.

[3] A. Duel-Hallen, S. Hu, H. Hallen, "Long-range Prediction of Fading Signals: Enabling Adaptive Transmission for Mobile Radio Channels", to appear in *Signal Processing Magazine*, May 2000.

[4] S. Hu, A. Duel-Hallen, H. Hallen, "Long-Range Prediction Makes Adaptive Modulation Feasible for Realistic Mobile Radio Channels," *Proc. of 34rd Annual Conf. on Infor. Sciences and Systems*, March 2000, Vol I, pp.WP4-7~WP4-13.

[1] Support for this work was provided by NSF grants CCR-9725271 and CCR-9815002.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Multidimensional Signals with Correlated Frequencies for Noncoherent Detection over the Rayleigh Channel

Céline Durand, Elie Bejjani
Alcatel, 5 rue Noël-Pons
92734 Nanterre Cedex, France
e-mail: {durand,bejjani}@enst.fr

Joseph Boutros
ENST, 46 rue Barrault
75634 Paris Cedex 13, France
e-mail: boutros@enst.fr

Abstract — **The use of multidimensional alphabets with correlated tones and noncoherent detection over Rayleigh fading channels allows to increase the typically low spectral efficiency of noncoherent transmission and to compensate for the performance degradation due to the high correlation between the tones.**

I. Multidimensional Noncoherent Detection

Frequency shift keying (FSK) is a robust modulation scheme when noncoherent detection is processed. Particularly, any channel estimation becomes useless for Rayleigh fading channels. Noncoherent detection [1] –a measure of the signal envelope after matched filtering– of Q-ary FSK is usually made with Q orthogonal signals and a tone spacing Δf_0 equal to the inverse of the symbol period T. The bandwidth can be reduced if $\Delta f_0 < 1/T$ i.e. orthogonality is no longer satisfied. The performance degradation due to the use of correlated tones can be compensated by careful signal alphabet design ; for example high dimensional constellations. We build M-dimensional FSK alphabets of size N. All signals $S_m = (s_{m,1}, \ldots, s_{m,N})$, $m = 1, \ldots, M$ are similar to the ones treated in [2] for the Gaussian channel and have equal energy. The elementary component $s_{m,n}(t)$, derived from a Q-FSK, is given by $s_{m,n}(t) = \sqrt{1/T} e^{j2\pi m_n \Delta f_0 t}$ for $-T/2 \leq t < T/2$ and $1 \leq n \leq N$. m_n is the number of the transmitted tone on the n^{th} component of signal S_m, $m_n \in \{1, \ldots, Q\}$.

II. ML Performance Analysis

The channel is assumed to be frequency-nonselective and slowly fading. The optimal noncoherent demodulator, composed of a bank of Q matched filters and a signal envelope detector, carries out $Q \times N$ values $r_{q,n}$. For each signal S_m, the set $\{|r_{m_n,n}|^2\}_{n=1,\ldots,N}$ is a sufficient statistic to make a decision. Following an approach similar to [3], we derive a simplified structure of the Maximum A Posteriori (MAP) decoder. A decision is made in favor of S_m which maximises

$$\Lambda_m = \sum_{n=1}^{N} |r_{m_n,n}|^2 \qquad m = 1, \ldots, M \tag{1}$$

The pairwise error probability $P(S_i \to S_j)$ can be derived from (1) by $P(\Lambda_i < \Lambda_j)$ [3]. Finally, $P(S_i \to S_j)$ is given by

$$\sum_{n=1}^{N} \left\{ \left[1 - \Gamma \sqrt{\frac{1-|\mu_n|^2}{1-|\mu_n|^2\Gamma^2}} \right] \frac{0.5 \times \left(1-|\mu_n|^2\right)^{N-1}}{\prod_{i=1, i\neq n}^{N} \left(|\mu_i|^2 - |\mu_n|^2\right)} \right\} \tag{2}$$

where Γ is a signal-to-noise ratio and μ_n is the correlation between the n^{th} components of signals S_i and S_j. For all $k, l \in \{1, \ldots, N\}$, we suppose that $\mu_k \neq \mu_l$.

III. Multidimensional Alphabets Results

Two alphabets of dimension 4 are compared. Each component $s_{m,n}(t)$ is denoted by the number of the transmitted tone m_n. B_e is the bandwidth expansion, defined as the inverse of the spectral efficiency. The first alphabet is composed of two orthogonal BFSK signals with diversity 4 : $S_1 = (1,1,1,1)$ and $S_2 = (2,2,2,2)$. Its theoretical performance can be derived from equation (4.61) in [3] with $N = 4$ and $\mu_n = \mu = 0$ (orthogonal tones). The second alphabet of size $M = 8$, designed in a heuristic manner, is based on 8-FSK correlated signals.

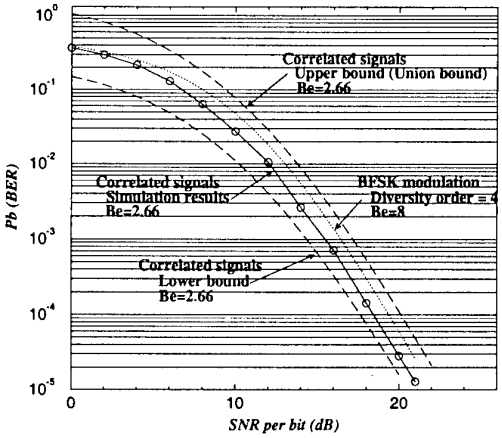


Fig. 1: 4-dimensional 8-FSK correlated signals vs. BFSK signals with order of diversity 4.

$$S_1 \to (1,2,1,2) \qquad S_5 \to (5,6,4,1)$$
$$S_2 \to (2,4,3,4) \qquad S_6 \to (6,8,6,3)$$
$$S_3 \to (3,1,5,6) \qquad S_7 \to (7,5,8,7)$$
$$S_4 \to (4,3,7,8) \qquad S_8 \to (8,7,2,5)$$

Notice that this set has also an order of diversity equal to 4 and that the most correlated signals are S_4 and S_7.

It can be easily shown that $P(S_4 \to S_7) \leq P_e \leq (M-1)P(S_4 \to S_7)$. The pairwise error probability values are derived from equation (2). The BER is given by $P_b = P_e/2$. Two main results are highlighted in figure 1. First, simulation results validate both upper and lower bounds. Moreover, the correlated signals alphabet exhibits excellent results when compared to the classical BFSK alphabet, although the spectral efficiency is three times larger.

References

[1] John G. Proakis, *Digital Communications*, 2nd and 3rd Editions, McGraw-Hill, 1989, 1995.

[2] C. Durand, E. Bejjani, J. Boutros, "Frequency Space Lattice Encoding for Noncoherent Detection with Correlated Signals", CWIT'99 Proceedings, Kingston, June 1999.

[3] E. Bejjani, *Techniques de transmission pour les canaux très dispersifs*, Ph.D Thesis Report, ENST, Paris, France, 1997.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Bandwidth-Efficient Exploitation of the Degrees of Freedom in a Multipath Fading Channel

Ashwin Ganesan[1]
ganesan@cae.wisc.edu

Akbar M. Sayeed[1]
akbar@engr.wisc.edu

Abstract — **Multipath propagation effects encountered in mobile wireless channels provide additional degrees of freedom that can be exploited via appropriate signaling and reception. In this paper, we propose a framework for spread-spectrum signaling and reception that allows manipulating these inherent degrees of freedom for maximum bandwidth efficiency. We present a simple approach for transforming a multipath channel with a single transmit and single receive antenna into a virtual multiple-input multiple-output system where space-time codes can be directly applied. Performance analysis suggests that simple signaling schemes based on our framework can yield significant capacity gains over existing spread spectrum systems.**

I. Summary

Time-varying multipath propagation effects encountered in mobile wireless channels provide additional degrees of freedom that can be exploited for bandwidth-efficient communication via appropriate signaling and reception. In spread-spectrum code division multiple access (CDMA) systems, signals of sufficiently high bandwidth and long time durations can be used with the RAKE receiver to exploit multipath-Doppler diversity [1]. In essence, uncorrelated time-varying multipath scattering provides degrees of freedom (DoFs) that can be exploited to enhance performance. However, conventional systems exploit all these DoFs for receiver diversity and provide diminishing returns as the DoFs increase.

Recent studies on antenna arrays have shown that the capacity of multiple-input multiple-output (MIMO) systems far exceeds that of single-input single-output (SISO), single-input multiple-output (SIMO) and multiple-input single-output (MISO) systems in a dense scattering environment. Motivated by these results, we propose a new transceiver structure for the multipath fading channel that allows manipulating the inherent degrees of freedom for bandwidth efficiency. In effect, we present a simple approach for transforming a multipath channel with L degrees of freedom (L independent paths) into a *virtual* transmit-receive antenna array system with M transmitters and N receivers, for any M and N such that $L = MN$.

We consider spread-spectrum signaling over a frequency-selective, slowly fading channel with multipath spread T_m. The transmitted signal is of duration T and bandwidth B. The impulse response of the channel is given by $\mathbf{h} = [h_1, h_2, ..., h_L]$, where $L = T_m B$ is the number of degrees of freedom available in the system. Since the dimensionality of the signal space is $K \approx TB$ [2], we can obtain a matrix formulation of the system by projecting onto K basis waveforms that capture the sufficient statistics. The system can be viewed as a K-input K-output system over the signal space and represented in the form $\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{w}$, where $\mathbf{x}$ is the transmitted signal vector, $\mathbf{y}$ is the received signal vector, $\mathbf{H}$ is the channel matrix and $\mathbf{w}$ is AWGN. When Nyquist sampling is done, the basis functions are sinc pulses and the channel matrix is block toeplitz. In our direct sequence CDMA system, we choose the basis functions to be circularly-shifted versions of an arbitrary signature waveform corresponding to a spreading code of length K. In this case, the components of $\mathbf{x}$ are modulated onto circularly-shifted versions of a signature waveform and transmitted. This choice of basis leads to a circulant $\mathbf{H}$. For this K-input K-output system, we study interesting special cases where the transmitter and receiver use only a subset of the K available dimensions.

In our framework, the conventional RAKE receiver corresponds to transmitting a single signature waveform and can be viewed as a 1-input L-output system. When $\mathbf{x} = [x_1, x_2, \ldots, x_M, 0, \ldots, 0]$ and the receiver looks only at $[y_M, y_{2M}, \ldots, y_{NM}]$, where $L = MN$, the multipath channel can be viewed as a virtual M-input N-output system. The $N \times M$ matrix $\mathbf{H}$ contains the L channel coefficients as its elements. In an *uncorrelated scattering* Rayleigh fading model, the elements of $\mathbf{H}$ are uncorrelated. The system is equivalent to an antenna array system with M transmitters, N receivers and independent coupling between antenna pairs. Existing space-time codes such as those in [3] can be directly applied to this system.

We consider outage capacity as the performance measure. Transforming the $(1, L)$ system into a (M, N) system provides clear capacity gains due to an increase in the number of parallel channels. For example, at the 1%, 5% and 10% outage levels and for high SNR (larger than 20 dB), the improvement in performance of $(2, 2)$ over $(1, 4)$ is almost 5 dB, and the improvement of $(2, 3)$ over $(1, 6)$ is more than 7 dB. The (M, N) systems we propose also have a low complexity transceiver structure and existing space-time codes can be directly employed. These results suggest that simple modifications based on our framework can significantly improve the capacity of existing single-antenna spread spectrum systems that employ the RAKE receiver.

References

[1] A. M. Sayeed and B. Aazhang, "Joint multipath-Doppler diversity in mobile wireless communications," *IEEE Transactions on Communications*, vol. 47, pp. 123-132, Jan. 1999.

[2] D. Slepian, "On bandwidth," *Proc. IEEE*, vol. 64, pp. 292-300, Mar. 1976.

[3] V. Tarokh, N. Seshadri and A.R.Calderbank, "Space-time codes for high data rate wireless communications: Performance criterion and code construction," *IEEE Transactions on Information Theory*, vol. 44, No. 2, pp 744-765, March 1998.

[1]The authors are with the Department of Electrical and Computer Engineering, University of Wisconsin-Madison, 1415 Engineering Drive, Madison, WI 53706. This research is supported in part by Wisconsin Alumni Research Foundation and by NSF under Grant No. CCR-9875805.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Performance of TETRA under Quasi-Synchronous Transmission over Rayleigh Fading Channels with Equalization

Michael Yip Ming and Francis C. M. Lau

ABSTRACT NOT AVAILABLE AT THE TIME OF PRINT

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Complex Spherical Modulation for Noncoherent Communications

Mahesh K. Varanasi and Michael L. McCloud
Department of Electrical and Computer Engineering
University of Colorado, Boulder, CO 80309-0425 USA
Email:*varanasi@schof.colorado.edu* *mccloud@ucsu.colorado.edu*

Abstract — **We examine the problem of designing complex, equal energy, signal constellations for the noncoherent additive white Gaussian noise communication channel. We derive an asymptotic performance criterion that may be used as a constraint in building correlated signals set for use with the maximum likelihood noncoherent detector. We present an iterative update design procedure for obtaining bandwidth-efficient signal sets under a constraint on the dimension of the signal space.**

I. Introduction

On noncoherent communication channels, orthogonal multi-pulse modulation (OMM) is typically employed wherein the user transmits one of M orthogonal signals during each baud interval [1]. The most common implementation of OMM is frequency shift-keying (FSK). The chief advantage of OMM is the simple implementation (envelope detection) of the receiver. The major drawback to OMM is its poor spectral efficiency. Non-orthogonal multi-pulse modulation (NMM) combats this drawback by allowing correlation among the signals.

II. Problem Statement

In NMM, an M-ary symbol is sent by transmitting one of M equal-energy, complex-valued signals that lie in an N-dimensional signal space. The minimum bandwidth B needed to generate such signals is N/T Hz, where T is the baud interval. The discrete-time model for NMM signaling over the additive white Gaussian noise (AWGN) channel is hence

$$\mathbf{y} = \sqrt{E}e^{j\phi_m}\mathbf{h}_m + \mathbf{n}, \tag{1}$$

when $m \in \{1, \cdots, M\}$ is the transmitted symbol and the corresponding signal $\mathbf{h}_m$ is a unit-norm complex vector lying in $\mathbb{C}^{N\times 1}$; E is the received energy for each symbol; ϕ_m is an unknown phase, modeled as a uniform random variable on $[0, 2\pi)$; and $\mathbf{n}$ is a zero mean complex normal random vector with correlation $E[\mathbf{n}\mathbf{n}^*] = \sigma^2\mathbf{I}$, where $*$ denotes complex-conjugate transpose.

Assuming equi-probable symbols, the optimum detector selects the signal that maximizes the magnitude of its inner product with the received signal:

$$\hat{m} = \arg\max_m |\mathbf{y}^*\mathbf{h}_m|. \tag{2}$$

This detector has a probability of error which is asymptotically a monotonic function of the largest magnitude of the cross-correlation coefficient $\rho = \max_{m\neq l}|\mathbf{h}_m{}^*\mathbf{h}_l|$. Define the signal correlation matrix $\mathbf{R}$ with $\mathbf{R}_{ml} = \mathbf{h}_m{}^*\mathbf{h}_l$.

We formulate the problem of designing a bandwidth-efficient modulation scheme purely in terms of $\mathbf{R}$ as follows:

Problem Statement: Given $N \in \mathbb{N}$ and $0 \leq \rho \leq 1$, find the largest $M \in \mathbb{N}$ for which the corresponding $\mathbf{R} \in \mathbb{C}^{M\times M}$ satisfies **C1**: $\mathrm{diag}(\mathbf{R}) = \mathbf{I}$, **C2**: $|\mathbf{R}_{i,j}| \leq \rho$ for $i \neq j$, **C3**: $\mathbf{R} \geq 0$, **C4**: $\mathrm{rank}(\mathbf{R}) \leq N$. The noncoherent signal set is then formed (non-uniquely) from the eigen-decomposition of $\mathbf{R}$, $\mathbf{R} = \mathbf{U}\mathbf{\Lambda}\mathbf{U}^*$, via $\mathbf{H} = \mathbf{\Lambda}^{1/2}\mathbf{U}^*$.

III. Successive Updates of the Correlation Matrix

We consider a successive update procedure whereby a matrix $\mathbf{R}_k$ satisfying **C1-C4** is updated with a vector $\mathbf{x}$ via

$$\mathbf{R}_{k+1} = \begin{bmatrix} 1 & \mathbf{x}^* \\ \mathbf{x} & \mathbf{R}_k \end{bmatrix}, \tag{3}$$

with $\mathbf{R}_{k+1}$ also satisfying **C1-C4**. It turns out that we can guarantee that $\mathbf{R}_{k+1}$ is positive semidefinite if $\mathbf{x}^*\mathbf{R}_k^+\mathbf{x} \leq 1$, and that the rank of $\mathbf{R}_{k+1}$ is equal to that of $\mathbf{R}_k$ when this condition is met with equality. In our designs, we started with a two-dimensional $\mathbf{R}_1$, and successively added signals until the constraint could not be met with equality. At this point, the rank of the matrix was allowed to grow by one and the process repeated. At each iteration, we maximized the norm, $||\mathbf{x}||^2$, under the constraint that $\max|\mathbf{x}_k| \leq \rho$. This is a nonlinear optimization problem and was solved using a modified Fletcher-Powell optimization algorithm employed through the FSQP[2] optimization package.

IV. Results

In Figure 1, we plot the spectral efficiency ($\log_2 M/N$) of our designs versus the SNR-per-bit required to achieve a probability of bit error of 10^{-5}. For the NMM designs, we held the dimensionality, N, fixed and varied the maximum cross-correlation, ρ. For comparison, we also plot the spectral efficiencies of coherent PAM and QAM modulation as well as the capacity curve for the coherent channel. We also plot the spectral efficiency of one-sided PAM [3, problem 4.16], a scheme in which a fixed waveform has its energy varied to transmit information. These results show that we can map out new portions of the energy/spectral efficiency plane through our signal designs, and that NMM can be made significantly more bandwidth-efficient than OMM.

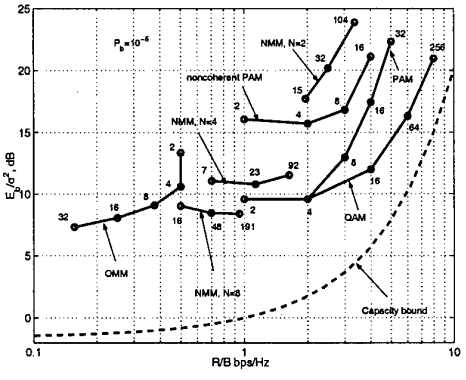


Fig. 1. Energy versus spectral efficiency of the noncoherent designs.

References

[1] J. Proakis, *Digital Communications*, McGraw-Hill Inc., New York, NY, 1995.
[2] C. Lawrence, J. Zhou, and A. Tits, *User's Guide for CFSQP Version 2.5: A C Code for solving (Large Scale) Constrained Nonlinear (Minimax) Optimization Problems, Generating Iterates Satisfying All Inequality Constraints*, University of Maryland, College Park, MD, 1997.
[3] S. Benedetto, E. Biglieri, and V. Castellani, *Digital transmission theory*, Prentice-Hall, Englewood Cliffs, NJ, 1987.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Orbital Spherical 11-Designs whose Initial Point is Root of an Invariant Polynomial

Sidel'nikov V.M.
Moscow State University
sid@vertex.inria.msu.ru

By definition, a spherical $t-$design in $N-$dimensional Euclidean space $\mathbf{R}^N$ is any nonempty finite set $X \subset S_{N-1}$ which for any polynomial f of degree at most t satisfies

$$\frac{1}{|S_{N-1}|}\int_{S_{N-1}} f(\mathbf{x})d\mu(\mathbf{x}) = \frac{1}{|X|}\sum_{\mathbf{x}\in X} f(\mathbf{x})$$

where $S_{N-1} := \{(x_1,\ldots,x_N) \in \mathbf{R}^N; x_1^2+\ldots+x_N^2 = 1\}$ is the unit sphere in $\mathbf{R}^N$, $\mu(\mathbf{x})$ is the standard Euclidean measure on S_{N-1} (i.e. μ is invariant under the orthogonal group $O(N)$) and $|S_{N-1}| := \int_{S_{N-1}} d\mu(\mathbf{x})$ is the surface area of S_{N-1}. For the basic properties of $t-$designs, we refer the reader to the papers [1-3].

We denote by $\mathrm{Hom}(k)$ the space of all homogeneous N-variate polynomials of degree k over $\mathbf{R}$ and by $\mathrm{Harm}(k)$ the space of homogeneous N-variate harmonic polynomials of degree k, i.e. the space of homogeneous polynomials $y = y(\mathbf{x})$ satisfying the Laplace equation $\frac{\partial^2 y}{\partial x_1^2}+\ldots+\frac{\partial^2 y}{\partial x_N^2} = 0$.

Let G be a finite group of orthogonal matrices, and let $\mathbf{a}$ be a point on S_{N-1}. All designs of the form $X := G\mathbf{a} := \{g\mathbf{a}|g \in G\}$ (X, i.e, X is an orbit of an initial point $\mathbf{a}$ constitute a natural class of designs. In [2] it was proved that the orbit $G\mathbf{a}$ is a $t-$design for any $\mathbf{a} \in S_{N-1}$ if and only if $H(t) =: \mathrm{Harm}(1)+\ldots+\mathrm{Harm}(t)$ there is no $G-$invariant harmonic polynomial. Moreover, in the cited paper it was shown that if $H(t)$ contains some $G-$invariant harmonic polynomials, then they can be "killed" by choosing their common root as initial point $\mathbf{a}$. In this case, the orbit $G\mathbf{a}$ is a $t-$design.

In the present paper we state the results discussed above in a somewhat more general and convenient form.

As an example, we consider the following well-known results. The orbit .0$\mathbf{a}$ of the Conway group .0 of all orthogonal transformations that fix the Leech lattice is an 11-design for any initial vector $\mathbf{a}$, because the first .0$-$invariant polynomial with zero mean has degree 12. If we take the vector $\mathbf{e} = 32^{-1/2}(-3,1^{23}) \in S_{23}$ (see [5], Chapter 4, §11) as $\mathbf{a}$, we obtain an 11-design consisting of 196560 elements. Observe that $2\mathbf{e}$ is one of the vectors of minimal length in the Leech lattice. The total number of such vectors is 196560 and the group .0 acts transitively on the set of these vectors [5].

The main result of the present paper is an explicit construction of an infinite family of 11-designs in the 2^n-dimensional Euclidean space on the top of the groups $\Phi_{n,2}$ and $\Sigma_{n,2}$, $n = 1,2,\ldots$, of orthogonal $(2^n\times 2^n)-$matrices; these groups were introduced in [6]. The same construction is proposed also for 9-designs. The group $\Phi_{n,2}$ is a subgroup of index 2 of the group $\Sigma_{n,2}$.

For $n = 2$, the group $\Phi_{n,2}$ is of order 1152 and is generated by the 16 matrices $\mathrm{diag}(\pm1,\pm1,\pm1,\pm1)$, the Hadamard matrix $H = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{pmatrix}$, and the 24 permutation matrices P_π corresponding to the affined mapping $\mathbf{x} \xrightarrow{\pi} Q\mathbf{x}+\alpha$ of the space $\mathbf{F}_2^2$ into itself (here $Q \in M_n(\mathbf{F}_2)$ is a nonsingular matrix and $\alpha \in \mathbf{F}_2^2$).

We prove that the space of $\Phi_{n,2}$-invariant harmonic polynomials $f(\mathbf{x})$ of degree at most 9 with zero mean is one-dimensional and possesses a generator $\Lambda^{(n)}(\mathbf{x})$ of degree 8. The space of $\Sigma_{n,2}-$invariant harmonic polynomials $f(\mathbf{x})$ of degree at most 11 with zero mean is also one-dimensional and has the same generator $\Lambda^{(n)}(\mathbf{x})$. Therefore, for any root $\mathbf{a}$ of the polynomial $\Lambda^{(n)}(\mathbf{x})$ the orbit $\Phi_{n,2}\mathbf{a}$ is a 9-design and the orbit $\Sigma_{n,2}\mathbf{a}$ is an 11-design.

Note that $\Lambda^{(2)}(\mathbf{x}) = \sum_{i=0}^4 x_{\alpha_i}^8 + 7\sum_{\alpha_i\neq\alpha_j} x_{\alpha_i}^4 x_{\alpha_j}^4 + 168\prod_{i=1}^4 x_{\alpha_i}^2 - 7/10(\sum_{i=1}^4 x_{\alpha_i}^2)^4$, where the variables are labeled by the elements of the two-dimensional space $\mathbf{F}_2^2 = \{\alpha_1,\alpha_2,\alpha_3,\alpha_4\}$ over the field $\mathbf{F}_2$.

The vector $\mathbf{c}(x_0)$, where $\mathbf{c}(x) = \frac{\sin x}{\sqrt{3}}(0,1,1,1) + \cos x(1,0,0,0)$ and x_0 is a root of the equation $\Lambda^{(2)}(\mathbf{c}(x)) = \cos^8 x + \frac{14}{3}\cos^4 x\sin^4 x + \frac{56}{9}\cos^2 x\sin^6 x + \frac{5}{9}\sin^8 x - \frac{7}{10} = 0$, is one of the roots of the polynomial $\Lambda^{(2)}(\mathbf{x})$. The orbit codes $\Phi_{n,2}\mathbf{c}(x_0)$ and $\Sigma_{n,2}\mathbf{c}(x_0)$ contain 96 and 192 points, respectively, and are 9- and 11-designs in 4-dimensional Euclidean space.

Similar methods can be used to construct 9- and 11-designs on sphere in the 8-dimensional Euclidean space. The resulting designs consist of 15360 and 30720 points, respectively.

[1]This work was supported by the Russian Foundation for Basic Research (grant no. 99-01-00941).

References

[1] P.Delsarte, J.M.Goethals, J.J. Seidel, Spherical Codes and Desings, Geometriae Dedicata, 6(1977), 263 – 288.

[2] J.M. Goethals, J.J. Seidel, Cubature Formulae, Polytopes, and Spherical Designs, in Geometric Vein (C. Devis, B. Grunbaum, and F.A. Sherk, Eds.), Springer-Verlag, Berlin, (1981), 203-218.

[3] E. Bannai, Spherical t-designs which are orbits of finite groups, J. Math. Soc. 36, No 2 (1984), 341-354.

[4] W. C. Huffman, N.J.A. Sloane, Most primitive groups have messy invariants. Advances in Math. 32 (1979), 18-127.

[5] J.H. Conway and N.J.A Sloane, Sphere packings, lattices, and groups. Grundlehren Math. Wiss., Bd. 390, Springer-Verlag New York-Berlin, 1988.

[6] V. M. Sidelnikov, On one finite matrix group and codes on Euclidean sphere, Problems of Information Transmission, Vol 33, No 1, (1997), 35-54.

[7] L.S. Kazarin, On the groups proposed Sidel'nikov, Sbornik: Mathematics, 189:7 (1998), 1087-1100.

[8] V.M. Sidelnikov, Spherical 7-designs in 2^n-dimensional Euclidean space. J. of Alg. Combinatorics, 10 (1999), 279-288.

[9] V.M. Sidelnikov, Orbital spherical 11-designs whose initial point is a root of an invariant polynomial, St. Peterburg Math. J. Vol 11 (2000), No 4.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Constellation Mappings For Two-Dimensional Non-Uniform Signaling

Glen Takahara*, Fady Alajaji*†, Hongyan Kuai* and Norman C. Beaulieu†*
*Dept. of Mathematics and Statistics and †Dept. of Electrical & Computer Engineering
Queen's University, Kingston, Ontario K7L 3N6, Canada

Abstract — **In this work we investigate the design of constellation mappings for the transmission of non-uniform memoryless sources over AWGN channels via M-ary modulation schemes. We show that constellation mappings which minimize the average symbol energy and, given this, maximize the decoding probability of the most likely signals, can yield SER and BER performance that is better than Gray encoding maps. We also find that for highly non-uniform sources, 16-QAM can perform better than 2-QAM, in terms of *both* throughput and BER.**

I. Introduction

For equally likely signals, Gray mapping in two-dimensional signaling is generally accepted as optimal for minimizing bit error rate (BER). However, many data sources generate non-uniformly distributed symbols, often with memory (e.g. image or speech signals). Thus, they contain a substantial amount of (natural or residual) redundancy which, after transmission over a noisy channel, can be appropriately exploited by a maximum-a-posteriori (MAP) detector to improve the overall error resilience of the communication system [1].

In this work we propose criteria for constructing mappings from a set of signals to points of a two-dimensional constellation. We show that for non-uniform sources Gray mapping is not necessarily optimal for minimizing BER or symbol error rate (SER). We illustrate this in the context of an uncoded communication system with QAM modulated, non-uniform signals sent over an AWGN channel, and decoded using MAP decoding. We also illustrate that, when using MAP decoding for highly non-uniform signals, the BER performance of 16-QAM can be better than that of 2-QAM, even though 16-QAM has four times higher throughput.

II. Constellation Mappings for MAP Decoding

We propose the following criteria (listed in order of priority) for constructing mappings from a set of M non-uniformly distributed symbols to the points of a two-dimensional constellation: (i) minimize the average energy per symbol for the M given symbol probabilities, and (ii) successively minimize the conditional symbol decoding error probabilities, going from the most likely to the least likely symbol. The following determines the mapping which satisfies criterion (i), up to permutations within sets of symbols with the same energy: given M symbol probabilities $\{p_i\}_{i=1}^M$ with energies $E_1 \leq \ldots \leq E_M$, any permutation π of $\{1, 2, \ldots, M\}$ which satisfies $p_{\pi(1)} \geq \ldots \geq p_{\pi(M)}$ minimizes $\sum_{i=1}^M E_i p_{\pi(i)}$.

Subject to criterion (i), we next consider criterion (ii). Let $s_1, \ldots, s_M$ denote the signals listed from most likely to least likely. We propose a simple heuristic for successively minimizing the conditional probabilities $P(\text{Symbol Error}|s_i \text{ sent})$. Starting with symbol s_1, and subject to not violating criterion (i), choose neighbours of s_1 to be least likely signals to maximize the area of the decoding region of signal s_1. Continue to allocate signals in this way until there are no signals left to allocate.

This work was supported in part by NSERC of Canada.
Email: takahara@glen.mast.queensu.ca.

III. Numerical Results

We consider a Bernoulli(p) source sent over an AWGN channel with 16-QAM modulation and MAP decoding. BER calculations were done using the upper and lower bounds in [2], which coincide with each other when plotted. Fig. 1 shows a 16-QAM constellation with a mapping M_1. For $p > 0.5$, the mapping M_1 minimizes the average symbol energy (criterion (i)) and, subject to this, for any noise variance $N_0/2$, the mapping M_1 also maximizes the conditional probability that symbol 0000 (the most likely symbol) is decoded, given that 0000 is sent. This is due to the fact that symbol 0000 has the least likely neighbours, subject to criterion 1; thus the decision region for 0000 is maximized. The remaining symbols are placed in the constellation to successively maximize the decoding regions of 0001, 0100, and 0010, in that order.

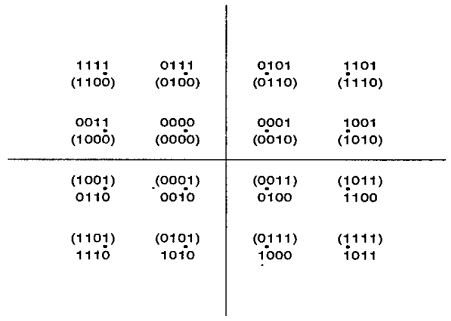


Figure 1: Mappings M_1 and Gray (in parentheses).

Under the mapping M_1, 16-QAM modulation with $p = 0.9$ and MAP decoding performs better than the usual Gray mapping, gaining roughly 1 dB and 0.75 dB in E_b/N_0 (at error rates between 10^{-5} and 10^{-2}) for SER and BER, respectively. We also note that 16-QAM with the mapping M_1 achieves around 1 dB gain over 2-QAM for $p = 0.9$ and the same BER. This leads us to the interesting observation that while the conventional wisdom for equally likely signals is that there is a tradeoff between throughput and BER, with non-uniform signals there need not be such a tradeoff. Indeed, in this example 16-QAM achieves *both* four times the throughput and better BER performance than 2-QAM when $p = 0.9$.

References

[1] F. Alajaji, N. Phamdo and T. Fuja, "Channel codes that exploit the residual redundancy in CELP-encoded speech," *IEEE Trans. Speech and Audio Processing*, pp. 325-336, Sept. 1996.

[2] H. Kuai, F. Alajaji and G. Takahara, "Performance bounds of non-uniform signaling over AWGN channels," *Proc. CTMC'99*, Vancouver, pp. 96-100, June 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

PAR Reduction via Constellation Shaping

Henry Kwok and Douglas Jones[1]
University of Illinois at Urbana-Champaign
1308 W. Main St., Urbana, IL 61801
e-mail: henry@ifp.uiuc.edu

Abstract — **In this paper, we introduce a novel scheme using a constellation shaping approach to reduce the peak-to-average ratio (PAR) in orthogonal frequency-division multiplexing (OFDM) systems. In the time domain, the peak power bound traces out a hypercube boundary. We map this square time-domain boundary back to the frequency domain via the DFT and construct a method for indexing the OFDM constellation points. The encoding and decoding of the constellation use generators and relations from group theory. The end result is a coding scheme with nearly 20 dB of PAR reduction with no reduction in data rate or performance.**

I Introduction

In an orthogonal frequency division multiplex (OFDM) system, the output time samples are generated by the inverse FFT of the constellation points. When each channels takes on a constellation point with the maximum power, the peak power is N times of the average power. Thus, the time samples may occasionally have very high output levels, which leads to the requirement of an expensive, highly linear, and power-inefficient analog front end (AFE) and/or a clipping mechanism to limit the time sample magnitude, which leads to impulsive noise and performance degradation. High PAR is arguably the greatest drawback of OFDM.

Numerous methods have been proposed to reduce the PAR of OFDM. They tend to be tradeoffs between PAR and data rate or distortion. We propose a method for peak power reduction in OFDM systems based on constellation shaping [1] which can provide nearly 20 dB of PAR reduction while maintaining equivalent data rate and performance. In addition, it can be combined with other existing methods to further increase the PAR reduction.

II Constellation Shaping

OFDM systems can operate either in baseband (as in the ADSL standard) or in passband; we examine only the baseband case here, although the method applies to both variations. We restrict $x = \begin{bmatrix} x_0 & \cdots & x_{N-1} \end{bmatrix}$ to be real. This allows us to define $\mathbf{X} = \begin{bmatrix} \mathrm{Re}\, Y_0 & \cdots & \mathrm{Re}\, Y_{\frac{N}{2}} & \mathrm{Im}\, Y_1 & \cdots & \mathrm{Im}\, Y_{\frac{N}{2}-1} \end{bmatrix}$ and $\mathbf{A}_N$ as columns of $\sin\left(2\pi\frac{nk}{N}\right)$ and $\cos\left(2\pi\frac{nk}{N}\right)$, and we have $\mathbf{x} = \mathbf{A}_N\mathbf{X}$.

[0]This work was supported by a Tellabs Fellowship at the University of Illinois and by the National Science Foundation, grant no. CCR 99-79381.

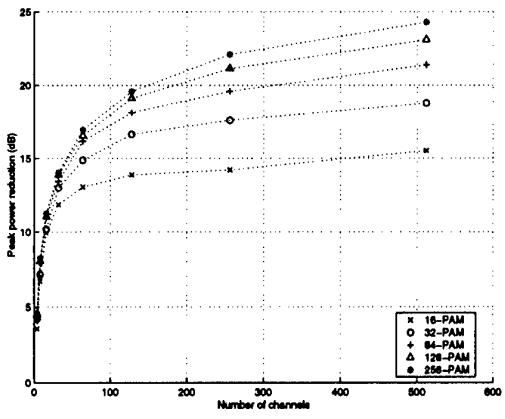


Figure 1: The PAR reduction versus the number of channels and constellation size.

The constellation boundary is usually determined by the metric that we want to optimize. In the problem of PAR reduction in OFDM systems, we use the ∞-norm, $\|\cdot\|_\infty$, in the time domain. This metric traces out a square boundary, defined by $\|\mathbf{x}\|_\infty = \beta$. In the frequency domain, we get: $\|\mathbf{x}\|_\infty = \|\mathbf{A}_N\mathbf{X}\|_\infty = \beta$. This is an N-D parallelotope in the frequency domain defined by $\mathbf{A}_N^{-1}$. To encode and decode the constellation points inside this new boundary, we use group theory to compute the generators for indexing these points.

We present some results using this algorithm. Figure 1 shows the total amount of peak-power reduction using this constellation shaping with various numbers of channels and constellation sizes. We see that reduction of over 20 dB is possible when the constellation size is large. Even with a typical constellation size, a peak power reduction of over 15 dB is easily realized.

References

[1] G. D. Forney, and L. Wei, "Multidimensional Constellations - Part I: Introduction, Figures of Merit, and Generalized Cross Constellations," *IEEE Journal on Selected Areas in Communications*, vol. 7, no. 6, August 1989, pp. 877-892.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Duadic Z4-Codes

Patrick Sole' and Philippe Langevin

ABSTRACT NOT AVAILABLE AT THE TIME OF PRINT

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Results relating to code construction on a tower of function fields meeting the Drinfeld-Vlăduţ bound

I. Aleshnikov and H. Stichtenoth
Universität GH Essen
D-45117 Essen, Germany
e-mail:
mat314@sp2.power.uni-essen.de
mat310@sp2.power.uni-essen.de

V. Deolalikar
Hughes Network Systems
San Diego, CA 92121
e-mail: vdeolalikar@hns.com

P. V. Kumar and K. Shum
University of Southern California
Los Angeles, CA 90089-2565
e-mail: vijayk@usc.edu
kshum@usc.edu

Abstract — **In this paper, a convenient set of functions is identified whose span includes all functions in a tower of function fields of Garcia and Stichtenoth that have poles only at the place at infinity. The latter set is of interest in the construction of long and efficient AG codes.**

I. Introduction

The Gilbert-Varshamov (G-V) bound is commonly used to assess the performance of long codes. While it is known that there exist long alternant and concatenated codes that meet the G-V bound, no explicit description of these codes exists.

Around 1980, V. D. Goppa used the theory of algebraic curves to construct a new family of codes, now referred to as algebraic geometric (AG) codes. Code performance depends upon the ratio N/g of two curve parameters, the genus g and the number of (rational) points N. Good codes result in cases where the ratio N/g is large and the Drinfeld-Vlăduţ (D-V) bound $\limsup_{g\to\infty} N/g \leq \sqrt{q}-1$ places an upper bound on the ratio.

In 1982, Tsfasman, Vlăduţ and Zink (T-V-Z) showed the existence of curves whose N/g ratio achieved the D-V bound. The resulting AG codes had performance exceeding that of the Gilbert-Varshamov bound – a feat that until then was considered unattainable.

However, the T-V-Z result is existential in nature. In 1996, Garcia and Stichtenoth (G-S) showed that two families of curves having an explicit description as a tower of function fields, also achieve the D-V bound. Identifying the generator matrices for "one-point" AG codes constructed on these curves requires the determination of a basis for the vector spaces $\mathcal{L}(rP)$, which comprise functions having poles only at a specified point P. The results in this paper present an important step towards determining this basis. A simply described set of functions whose span includes the vector spaces $\mathcal{L}(rP)$ is provided.

In [6], the authors provide generator matrices for codes constructed on the first three function fields in the first G-S tower. Haché extends this result to the fourth function field over $GF(16)$. The Weierstrass semigroup at P is determined in [4]. Other examples of asymptotically optimal towers are provided in [1].

II. Results

Let q be the power of a prime p and consider the G-S tower of function fields given by $T_1 = \mathbb{F}_{q^2}(x_1)$ and for $n \geq 2$,

$$T_n = T_{n-1}(x_n) \text{ where } x_n^q + x_n = \frac{x_{n-1}^q}{x_{n-1}^{q-1}+1}.$$

Let $P_\infty^{(n)}$ denote the unique place in T_n lying above P_∞ and set $g_1 := (x_1^{q-1}+1)$,

$$\mathcal{S} = \{1\} \bigcup \{ g_1 \prod_{i=2}^{n} x_i^{e_i} \mid 0 \leq e_i \leq q-1, \text{ some } e_i \neq 0\}.$$

The main result can now be stated.

Theorem 1 *Every function in T_n whole poles are confined to $P_\infty^{(n)}$ can be expressed as a linear combination of functions in the set $\mathcal{S}$, with coefficients of the form $p(x_1)/x_1^i$, where $p(x_1)$ is a polynomial in x_1 and $i \geq 0$.*

The talk will provide examples as well as other results relating to the function field tower.

Acknowledgments

V. Deolalikar, P. V. Kumar and K. Shum would like to acknowledge the help accorded by (the late) Prof. Dennis Estes as well as helpful discussions with Joe Wetherell and Kyeongcheol Yang.

References

[1] N. Elkies, "Explicit modular towers," *Proc. 35th Annual Allerton Conference on Commun., Control and Computing*, Urbana, IL, 1997.

[2] Arnaldo Garcia and Henning Stichtenoth, "On the asymptotic behavior of some towers of function fields over finite fields," *Journal of Number Theory*, vol. 61, No. 2, December 1996, pp. 248-273.

[3] Haché, G. *Construction effective des codes géométriques*, Thèse, Paris, VII 1996.

[4] R. Pellikaan, H. Stichtenoth and F. Torres, "Weierstrass semigroups in an asymptotically good tower of function fields," preprint, 1998.

[5] Henning Stichtenoth, *Algebraic function fields and codes*, Springer-Verlag, 1991.

[6] C. Voss and T. Hoholdt, "An explicit construction of a sequence of codes attaining the Tsfasman-Vlăduţ-Zink bound," *IEEE Trans. Inform. Theory*, vol. 43, Jan. 1997, pp.128-135.

[1] This work was supported by the National Science Foundation under Grant CCR-9714626.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

A Dual of Well-Behaving Type Designed Minimum Distance

Tomoharu Shibuya and Kohichi Sakaniwa
Dept. of Electrical and Electronic Eng., Tokyo Inst. of Technology,
2-12-1, Ookayama, Meguro-ku, Tokyo, 152-8552 Japan,
e-mail: tshibuya@ss.titech.ac.jp

Abstract — **We propose a lower bound for the minimum distance of $[n,k]$ linear codes which are specified by generator matrices whose rows are k vectors of a given sequence of n linearly independent vectors over a finite field. Note that the Feng-Rao and the order bounds give lower bounds for the minimum distance of the dual codes.**

I. Introduction

Various kinds of bounds for the minimum distance of linear codes have been investigated in the history of coding theory. Among them, the *Feng-Rao bound* is one of the most distinguished [1].

Let F be a finite field and n a positive integer. We denote by $B := (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ a sequence of n linearly independent vectors in F^n. For $\boldsymbol{u} = (u_1, u_2, \ldots, u_n)$ and $\boldsymbol{v} = (v_1, v_2, \ldots, v_n)$ in F^n, $\boldsymbol{u} * \boldsymbol{v} := (u_1 v_1, u_2 v_2, \ldots, u_n v_n)$.

For B and a subset G of B with $|G| = k$ $(1 \le k \le n)$, we define a code $C(B,G)$ over F by $C(B,G) := \mathrm{span}\{\boldsymbol{b} : \boldsymbol{b} \in G\}$ and denote its dual by $C^{\perp}(B,G)$. $C(B,G)$ (resp. $C^{\perp}(B,G)$) is an $[n,k]$ (resp. $[n,n-k]$) linear code. We denote by $d(C)$ the minimum distance of a linear code C.

We denote by L_ℓ $(1 \le \ell \le n)$ the linear space over F spanned by $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_\ell$ and let $L_0 := \{\boldsymbol{0}\}$. For $\boldsymbol{v} \in F^n \setminus \{\boldsymbol{0}\}$, let $\rho(\boldsymbol{v})$ denote the index ℓ such that $\boldsymbol{v} \in L_\ell \setminus L_{\ell-1}$ holds and $\rho(\boldsymbol{0}) := 0$. A pair $(\boldsymbol{b}_i, \boldsymbol{b}_j)$ $(\boldsymbol{b}_i, \boldsymbol{b}_j \in B)$ is said to be *well-behaving* (WB) if $\rho(\boldsymbol{b}_u * \boldsymbol{b}_v) < \rho(\boldsymbol{b}_i * \boldsymbol{b}_j)$ for all u and v with $1 \le u \le i$, $1 \le v \le j$ and $(u,v) \ne (i,j)$.

Proposition 1 [2, §4] For B and G, let

$$\mathcal{A}_\ell := \{(i,j) : \rho(\boldsymbol{b}_i * \boldsymbol{b}_j) = \ell \text{ and } (\boldsymbol{b}_i, \boldsymbol{b}_j) \text{ is WB}\},$$

for $\ell = 1, 2, \ldots, n$ and define $\delta(B,G) := \min\{|\mathcal{A}_\ell| : \boldsymbol{b}_\ell \in B \setminus G\}$. Then $d(C^{\perp}(B,G)) \ge \delta(B,G)$. □

$\delta(B,G)$ is known as the Feng-Rao bound for $d(C^{\perp}(B,G))$. In this paper, we introduce a lower bound for the minimum distance of $C(B,G)$ instead of $C^{\perp}(B,G)$, by using the map ρ and the concept of well-behaving as in Proposition 1.

II. A lower bound for $d(C(B,G))$

Theorem 1 For B and G, let

$$\mathcal{B}'_i := \{\ell : \rho(\boldsymbol{b}_i * \boldsymbol{b}_j) = \ell \text{ for some } \boldsymbol{b}_j \in B \text{ s.t. } (\boldsymbol{b}_i, \boldsymbol{b}_j) \text{ is WB}\}, \quad i = 1, 2, \ldots, n$$

and $\mathcal{B}_i := \{\nu : \boldsymbol{b}_\nu \in B \setminus G\} \setminus \mathcal{B}'_i$. Define $t(B,G) := \max\{|\mathcal{B}_i| : \boldsymbol{b}_i \in G\}$. Then $d(C(B,G)) \ge n - k + 1 - t(B,G)$. □

This theorem follows from the duality theorem of generalized Hamming weights [6] and the following proposition.

Proposition 2 Let $d_t(C)$ denote the t-th generalized Hamming weight of the code C, then $d_t(C^{\perp}(B,G)) = k + t$ for all t with $t(B,G) + 1 \le t \le n - k$. □

This proposition was first shown for $G = \{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k\}$ [3, Theorem 2] while it is shown to hold for an arbitrary subset G of B with $|G| = k$.

For given B and an integer τ, let $G' := \{\boldsymbol{b}_\ell : |\mathcal{B}_\ell| \le \tau\}$. Then $t(B,G') \le \tau$ and therefore $d(C(B,G')) \ge n - k + 1 - \tau$ by Theorem 1. Moreover if $t(B,G') = t(B,G)$ then $G \subset G'$. Thus if $t(B,G') = \tau$, then $C(B,G') \supset C(B,G)$ for all $G \subset B$ with $t(B,G) = \tau$. This means that for fixed B and τ, the dimension of $C(B,G')$ is $|G'|$ and is the largest among all dimensions of codes $C(B,G)$ with $t(B,G) = \tau$. This idea to define G' corresponds to the *improved geometric Goppa codes* for $C^{\perp}(B,G)$ [2, §4.3].

III. Applications

For Reed-Solomon and Reed-Muller codes, we can show that Theorem 1 gives the true minimum distance [3, 4].

For one point algebraic geometry (AG) codes on C_{ab} curves [5], if a C_{ab} curve is non-singular and absolutely irreducible, then we can show that $t(B,G) \le g$ [3] where g is a genus of the C_{ab} curve, and B and G are determined so that $C(B,G)$ becomes an L-type AG code on the C_{ab} curve. Since an L-type AG code is an $[n,k,d]$ code with $d \ge n - k + 1 - g =: d^*$ [2, Theorem 2.65], this result implies that the lower bound given in Theorem 1 is better than d^*.

For evaluation codes [2, §4], a lower bound based on the *weight function* has been investigated [2, §5]. When the one point AG codes on C_{ab} curves considered above are regarded as evaluation codes, this bound is equal to d^* and therefore the proposed bound is better. For other evaluation codes, relations between the two bounds are left for further study.

References

[1] G. L. Feng and T. R. N. Rao, "Decoding Algebraic-Geometric Codes up to the Designed Minimum Distance," *IEEE Trans. Inform. Theory*, vol.IT-39, No.1, pp.37–45, 1993.

[2] T. Høholdt, H. van Lint and R. Pellikaan, "Algebraic Geometry Codes," *Handbook of Coding Theory*, Chapter 10, North-Holland, 1998.

[3] T. Shibuya, R. Hasegawa and K. Sakaniwa, "A Lower Bound for Generalized Hamming Weights and Condition for t-th Rank MDS," *IEICE Trans. Fundamentals*, vol.E82–A, No.6, pp.1090–1101, 1999.

[4] T. Shibuya and K. Sakaniwa, "Generator Matrix Oriented Well-Behaving Bound for the Minimum Distance," *Proc. of 22nd SITA*, vol.2, pp.653–656, 1999.

[5] S. Miura, "Algebraic Geometric Codes on Certain Plane Curves," *IEICE Trans. Fundamentals*, vol.J75-A, No.11, pp. 1735–1745, Nov. 1992. (in Japanese)

[6] V. K. Wei, "Generalized Hamming Weights for Linear Codes," *IEEE Trans. Inform. Theory*, vol.IT-37, No.5, pp.1412–1418, 1991.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Bounds on the State Complexity of Geometric Goppa Codes

Tim Blackmore
Algebraic Coding Research Group
Centre for Communications Research
University of Bristol
Bristol, England
tim.blackmore@bristol.ac.uk

Graham H. Norton
Algebraic Coding Research Group
Centre for Communications Research
University of Bristol
Bristol, England
graham.norton@bristol.ac.uk

Abstract — **We give lower bounds on the state complexity of geometric Goppa codes. For Hermitian codes we calculate the DLP bound, ∇, and determine when ∇ is tight and when it is not.**

I. Introduction

Geometric Goppa codes (also called algebraic-geometric codes) are a family of powerful codes that can be longer than Reed-Solomon codes. Hermitian codes are a particularly good family of geometric Goppa codes. State complexity (SC) is used as a measure of the complexity of soft-decision decoding algorithms, such as the Viterbi algorithm. The SC of a code varies with coordinate orders. We refer to the lowest SC over all coordinate orders as absolute state complexity (ASC). According to Massey, determining an order that achieves ASC is 'the art of trellis decoding'. The DLP bound, ∇, is an order-free lower bound on SC. In particular, if an order attains ∇ then it achieves ASC.

II. On the SC of Geometric Goppa Codes

Our notation and terminology for geometric Goppa codes follow Stichtenoth's book. We fix a function field $F/\mathbb{F}_q$ of genus g and an $[n,k]$ geometric Goppa code $C_{\mathcal{L}}(D,G)$ from $F/\mathbb{F}_q$, where $D = \sum_{j=1}^{n} P_j$. The abundance of $C_{\mathcal{L}}(D,G)$ is $a = \dim(G-D)$. The usual expression for state space dimension at depth i in terms of dimensions of past and future truncated codes becomes

$$s_i(C_{\mathcal{L}}(D,G)) = k + 2a - \dim(G - D_i^-) - \dim(G - D_i^+) \quad (1)$$

where $D_i^- = \sum_{j=1}^{i} P_j$, $D_i^+ = D - D_i^-$ and $0 \le i \le n$. As usual $s(C_{\mathcal{L}}(D,G)) = \max_{0\le i\le n}\{s_i(C_{\mathcal{L}}(D,G))\}$.

Almost immediately from (1) we get that the SC of $C_{\mathcal{L}}(D,G)$ reaches Wolf's upper bound, $\min\{k, n-k\}$, if $\deg G < \frac{n-1}{2}$ or $\deg G > \frac{n-3}{2} + 2g$. *For the rest we assume that* $\frac{n-1}{2} \le \deg G \le \frac{n-2}{2} + g$. (The results for $\frac{n-1}{2} + g \le \deg G \le \frac{n-3}{2} + 2g$ follow by duality.) A first lower bound on SC can be deduced from Clifford's Theorem.

Result 1 (Clifford Bound) $s(C_{\mathcal{L}}(D,G)) \ge k + 2a - \deg G + \lceil \frac{n-3}{2} \rceil$.

Two other lower bounds can be derived in terms of the gonality sequence, $(g_k)_{k\ge 1}$, of $F/\mathbb{F}_q$. The gonality sequence is known from g and the degree of $F/\mathbb{F}_q$, [2]. One of these bounds is derived from a known bound on the generalised weight hierarchy of $F/\mathbb{F}_q$, [1, 3]; the other is derived directly from (1). Often the two bounds are equal and then

Result 2 (GS Bound) $s(C_{\mathcal{L}}(D,G)) \ge \max_{0\le i\le n}\{k + 2a - |\{r : g_r \le \deg G - i\}| - |\{r : g_r \le \deg G + i - n\}|\}$.

Example 3 *When $F/\mathbb{F}_q$ is hyperelliptic the Clifford bound and the GS bound agree.*

III. Towards the ASC of Hermitian Codes

Hermitian codes are defined from the Hermitian function field, $H/\mathbb{F}_{q^2}$ of genus $g = \binom{q}{2}$. For Hermitian codes $n = q^3$ and $G = mQ_\infty$, where Q_∞ is the place of degree one at infinity. We put $C_m = C_{\mathcal{L}}(D, mQ_\infty)$ and $k_m = \dim(C_m)$. We are interested in $\frac{n-1}{2} \le m \le \frac{n-2}{2} + g$. By results of [2, 3], the DLP bound of an Hermitian code is equal to the GS bound.

Result 4 (DLP Bound for Hermitian Codes) *With $n - 2m + 4g + q - 2 = uq + v$, where $0 \le v \le q-1$,*

$$\nabla(C_m) = k_m - \binom{q - \lfloor \frac{u}{2} \rfloor}{2} - \binom{q - \lceil \frac{u}{2} \rceil}{2} - \min\left\{q - \left\lceil \frac{u}{2} \right\rceil, q - v\right\}.$$

In some cases we can improve on the DLP bound. We write

$$m = \left\lfloor \frac{q^2}{2} \right\rfloor q + M^\bullet(q+1) + M^\circ, \text{ where } 0 \le M^\circ \le q.$$

Result 5 *With $q_2 \equiv q \bmod 2$, $s(C_m) - \nabla(C_m)$ is at least*

$$\begin{cases} 1 + M^\bullet + M^\circ - \lfloor \frac{q}{2} \rfloor & \text{if } \lfloor \frac{q}{2} \rfloor - M^\bullet \le M^\circ \le \frac{q - M^\bullet - 1}{2} \\ \lceil \frac{q}{2} \rceil - M^\circ & \text{if } \frac{q - M^\bullet}{2} \le M^\circ \le \lceil \frac{q-2}{2} \rceil \\ 1 + M^\bullet + M^\circ - q & \text{if } q - M^\bullet \le M^\circ \le q - \frac{M^\bullet + 1}{2} \\ 1 + q - q_2 - M^\circ & \text{if } q - \frac{M^\bullet}{2} \le M^\circ \le q - q_2. \end{cases}$$

In particular the DLP bound cannot be tight if $\lfloor \frac{q}{2} \rfloor - M^\bullet \le M^\circ \le \lceil \frac{q-2}{2} \rceil$ or $q - M^\bullet \le M^\circ \le q - q_2$.

We have found a coordinate order on C_m that achieves the DLP bound whenever this is not ruled out by Result 5. Thus this determines exactly when the DLP bound for the SC of Hermitian codes is tight.

However, when the DLP bound is not tight, the coordinate order does not always achieve the bound of Result 5. In these cases we have not ascertained the ASC of C_m. The first values of m for which this is the case are $q = 5$ and $m = 70$, $q = 7$ and $m \in \{182, 189, 190\}$ and $q = 8$ and $m \in \{268, 272, 276, 277, 280, 281\}$.

This work was supported by EPSRC grant L88764.

References

[1] C. Munuera, "On the generalized Hamming weights of geometric Goppa codes," *IEEE Trans. Information Theory*, vol. 40, pp. 2092–2099, 1994.

[2] R. Pellikaan, "On special divisors and the two variable zeta function of algebraic curves over finite fields," *Arithmetic, Geometry and Coding Theory 4*, Luminy, 1993.

[3] K. Yang, P. V. Kumar and H. Stichtenoth, "On the weight hierarchy of geometric Goppa codes," *IEEE Trans. Information Theory*, vol. 40, pp. 913–920, 1994.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Iterative Decoding and Channel Estimation

Paul Alexander
Southern Poro Communications
355A Young Street, Annandale
NSW 2038, Australia

Alex Grant
Institute for Telecommunications Research
University of South Australia
Mawson Lakes Boulevard, Mawson Lakes
SA 5095, Australia

Abstract — **We investigate iterative decoding and channel estimation for multiple-access channels. Results are obtained concerning the fixed points of such iterations.**

I. Iterative Receiver Principle

In [1] an iterative receiver was proposed for the linear multiple access channel. We now consider an approach for integration of channel estimation into this technique whereby we use the a-posteriori probabilities of the information symbols as uncertain training sequences for the purposes of channel estimation. We investigate the properties of fixed points of such iterations.

Let $\mathcal{S}$ be a vector space. Unconstrained sequences can take any value $u \in \mathcal{S}$ as opposed to constrained sequences $x \in \mathcal{C} \subset \mathcal{S}$. We are interested in low-complexity joint detection (or estimation) for sets of constrained sequences observed according to known transition probabilities. These probabilities are defined by some combination of deterministic mappings (e.g. linear combining) and non-deterministic perturbations (e.g. noise).

Suppose that the sequences x_k, $k = 1, \ldots, n$ are each produced by a mapping $\mathcal{C}_k$ of an unconstrained sequence u_k. The random sequence y is observed according to $p(y \mid x_1, \ldots, x_n)$. The u_k may or may not be independent, but are conditionally dependent given y. This model can be thought of as a multiple-access communications system (the x_k are coded information sequences), but is rich enough to describe other systems of interest, such as inter-symbol interference channels (by allowing some of the x_k to represent the sequence of channel taps, obeying known spectral constraints) and space-time diversity channels.

Optimal detection means the determination of either the posterior density $p(u_1, u_2, \ldots, u_n \mid y)$, or its marginals, taking into account the constraints. This is usually an NP-complete problem and we propose a reduced complexity iterative algorithm. The basic principle that we propose for design of such algorithms may be stated concisely as follows.

1. Incorporate dependence, ignore constraints.
2. Incorporate constraints, ignore dependence.

We iteratively update the distributions $p_k(u_k)$. Ideally p_k converges over iteration to the k-th marginal of the true posterior distribution $p(u_1, u_2, \ldots, u_n \mid y)$. The principle also applies to estimation problems, in which case the distributions are replaced with the current estimates, which we hope converge to some desired estimator e.g. MMSE.

Let $p = \{p_1(u_1), p_2(u_2), \ldots, p_n(u_n)\}$ be the sequence priors. At the conclusion of any iteration step, the *unconstrained joint detector*, using as priors the current set of marginal distributions p, produces a new set p^+, taking into account only the conditional dependencies. All the constraints are relaxed. This results in a p^+ that may place mass on "impossible" events. Relaxation of (especially integer) constraints can result in low-complexity heuristics. An example of this is applying the decorrelator or MMSE filter for detection with a linear model with integer constraints.

A bank of *constrained detectors* ignores the interdependencies between the u_k. The detector for u_k updates the current prior marginal p_k based on the constraint $\mathcal{C}_k$ and $p(y \mid u_k)$. For convolutionally coded data, we may use the forward-backward algorithm. For a sequence of channel taps we may use a Kalman filter.

II. Convergence Analysis

We shall now consider an asynchronous K user CDMA system in the absence of multipath fading. Identical convolutional codes with free distance d_{free} are used by each transmitter.

We are interested in the effective noise variance at the output of each iteration. Considering an input noise variance v to the constrained data estimator (Viterbi decoder), we may bound the output noise variance v_d.

$$v_d \geq f(v) = 4d_{\text{free}} Q\left(\sqrt{2d_{\text{free}}/v}\right)$$

For a given spreading factor $\beta = K/N$, input variance v_d and thermal noise variance σ^2, the unconstrained joint detector described in [1] is characterized by $v_d = \beta v + \sigma^2$. This leads to the recurrence

$$v_d^{(m+1)} = F(v_d^{(m)}) \triangleq 4d_{\text{free}} Q\left(\sqrt{\frac{2d_{\text{free}}}{\beta v_d^{(m)} + \sigma^2}}\right),$$

In operating regions of interest, we may use the solutions to the fixed point equation $v_d = F(v_d)$ to accurately predict the performance. Furthermore $v_d^{(m)}$ may be used to predict the performance for finite number of iterations, m.

Given a fixed point solution x, we have the following sufficient condition for stability

$$0 < x < \frac{1}{\beta}\left(\frac{2d_{\text{free}}}{3\ln d_{\text{free}} - \ln\frac{4}{\pi}} - \sigma^2\right) \implies F'(x) < 1.$$

In practice, we have observed the existence of a stable fixed point close to the single user operating point and it is possible to derive an expression for the loss compared to single user for this point. Decoder failure occurs when a second fixed point appears at high noise variance. It can be shown that for high SNR this occurs for a critical value of β given by

$$\beta_{\text{crit}} = (2 - v)/f^{-1}(2).$$

We have verified this behavior with simulations.

References

[1] P. D. Alexander, A. J. Grant, and M. C. Reed, "Iterative detection on code-division multiple-access with error control coding," *European Transactions on Telecommunications*, vol. 9, no. 5, pp. 419–426, Sept.-Oct. 1998.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Iterative Decoding of Non-Systematic Turbo-Codes[1]

Oliver M. Collins
Department of Electrical Engineering
University of Notre Dame
Notre Dame, IN 46656
e-mail: Collins.62@nd.edu

Oscar Y. Takeshita
Department of Electrical Engineering
The Ohio State University
Columbus, OH 43210
e-mail: Takeshita.3@osu.edu

Daniel J. Costello, Jr.
Department of Electrical Engineering
University of Notre Dame
Notre Dame, IN 46656
e-mail: Costello.2@nd.edu

Abstract — **Parallel concatenated convolutional codes (PCCC's) are usually constructed using systematic recursive convolutional codes (SRCC's) as constituent codes. In this paper, we introduce a new version of parallel concatenation that uses non-systematic recursive convolutional codes (NSRCC's) as constituent codes. A systematic constituent code then becomes a particular case of this general scheme. The use of this larger class of constituent codes enhances the number of possible codes in the search space, thus allowing the possibility of finding better codes. We also introduce a modified iterative decoding method for this more general form of parallel concatenation. The decoding technique is no more complex than the standard iterative decoding algorithm.**

I. Introduction

The usual view of parallel concatenation is two systematic recursive convolutional codes (SRCC's) linked by an interleaver [1]. The systematic bits that are identical to both constituent codes are transmitted only once, and the two decoders "share" the noisy received systematic symbols. Iterative decoding is then accomplished by exchanging extrinsic reliability information about the systematic bits between the two decoders.

In this paper we propose a class of parallel concatenated convolutional codes (PCCC's) that uses non-systematic recursive convolutional codes (NSRCC's) as constituent codes for PCCC's. This class of NSRCC's contains the usual SRCC's as a particular case. We also propose a modified iterative decoding method for these more general PCCC's.

We define an NSRCC as a convolutional code with generator matrix $[n_3(D)/d_3(D)\ n_4(D)/d_3(D)]$. (Note that this NSRCC becomes systematic if $n_3(D) = d_3(D)$ or $n_4(D) = d_3(D)$.)

We now propose a PCCC scheme as shown in Fig. 1. The first constituent code is a rate 1/2 NSRCC in the previously described form and the second constituent code is similar to the usual PCCC's, i.e., the systematic bits are not transmitted.

The block diagram of the decoder is shown in Fig. 2. For each a posteriori probability (APP) decoder we use the standard BCJR [2] algorithm.

When y_1 or y_2 is a systematic bit, this algorithm gives a result that is identical to the classical PCCC iterative decoding algorithm. In the classical PCCC iterative decoding algorithm, besides $\tilde{y}_3$ and the extrinsic a priori likelihood ratios of the systematic bits provided by APP1, APP2 also received

[1]This work was supported by NSF Grants NCR95-22939 and NCR96-96065 and NASA Grants NAG5-557 and NAG5-8355.

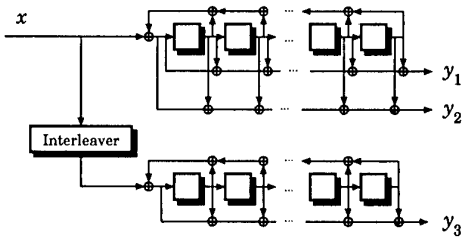


Figure 1: A general PCCC.

noisy systematic symbols ($\tilde{y}_1$ or $\tilde{y}_2$) as inputs. For the new decoder shown in Fig. 2, the received noisy systematic symbols are included in the information sent from APP1 to APP2 when the code is systematic. The feedback from APP2 to APP1, however, is identical to classical PCCC iterative decoding, i.e., only "extrinsic" likelihood ratios are sent in this case.

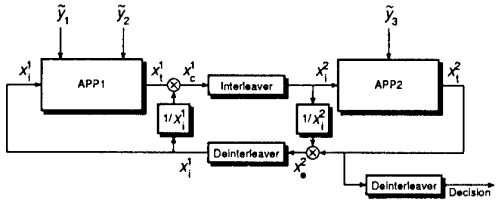


Figure 2: Block diagram of the decoder.

Because we have lifted the restriction of using SRCC's as constituent codes, the number of possible constituent codes is now much larger than for classical PCCC's. We have attempted a limited search for good PCCC's using NSRCC's as constituent codes. A PCCC with generator matrices $[1+D/1+D+D^2\ 1+D+D^3/1+D+D^2]$ and $[1+D^3+D^4/1+D+D^2]$ has been identified as a good choice. Its BER performance is nearly the same as the original turbo-code in [1] for an information block length of 1024 and rate 1/3. Note, however, that this non-systematic code has a smaller state complexity.

References

[1] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: turbo-codes," in *Proc. IEEE Int. Conf. on Commun.*, May 1993, pp. 1064–1070.

[2] L. R. Bahl, J. Cocke, F. Jelinek, and J. Raviv, "Optimal decoding of linear codes for minimizing symbol error rate," *IEEE Trans. on Inform. Theory*, vol. IT-20, pp. 284–287, Mar. 1974.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Iterative Source-Channel Decoding using Soft-In/Soft-Out Decoders

Norbert Görtz
Institute for Circuits and Systems Theory
University of Kiel
Kaiserstr. 2, 24143 Kiel, Germany
e-mail: ng@techfak.uni-kiel.de

Abstract — **The concept of iterative decoding of concatenated channel codes is applied to joint source-channel decoding (JSCD). Extrinsic information from the soft-in/soft-out channel decoder is used as a-priori information for the new soft-in/soft-out source decoder and vice versa. In this novel iterative approach the redundancies within the data-bits and the channel codewords are alternately exploited in order to approximate the highly complex optimal JSCD.**

Iterative Source-Channel Decoding

Consider the problem of transmitting a set of M signal-vectors $X_k^{(1)}, ..., X_k^{(M)}$ at each time k (fig. 1). The vectors are source-encoded (quantized) by the indices $I_k^{(j)}$, $j = 1, .., M$. The index-bits are interleaved, commonly channel-encoded, and the codewords V_k are transmitted. Since source encoding is never "perfect", some dependencies (modeled by first-order Markov-processes) remain between adjacent indices $I_{k-1}^{(j)}, I_k^{(j)}$.

The basic idea of *iterative source-channel decoding* is adopted from iterative channel decoding [1]: The redundancies, which are contained in the channel codewords and in the source-encoder indices, are alternately exploited by separate soft-in/soft-out decoders (SISO decoders). Each SISO decoder computes the new (extrinsic) part of information on the data-bits, which is based only on *one* type of redundancy. The extrinsic information is forwarded to the other SISO decoder as a-priori information. This process is iteratively repeated to improve the reliability of the index-bits step by step. A block-diagram of such an iterative source-channel decoder, which directly fits into figure 1, is depicted in figure 2.

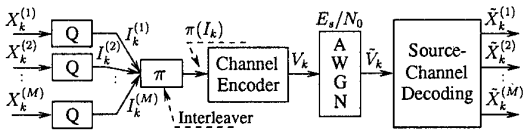


Fig. 1: Transmission system

The *SISO channel decoder* (e.g. BCJR-algorithm [1], [2]) processes a-priori information $L_a^{(C)}(\pi(\hat{I}_k))$ of the index-bits, the received channel-L-values $L_c \cdot \tilde{V}_k$ of the transmitted bits, and it computes the output L-values $L^{(C)}(\pi(\hat{I}_k))$ and the extrinsic information $L_e^{(C)}(\pi(\hat{I}_k))$ for the index-bits. The latter contains the *new* part of information that has been computed by only exploiting the redundancies within the channel code.

SISO source decoding is performed by Optimal-Estimation (OE) [3]. The channel-values $\tilde{I}_k$ of the index-bits, the a-priori information $L_a^{(S)}(\hat{I}_k)$, which equals the extrinsic information $L_e^{(C)}(\hat{I}_k)$ from the channel-decoder, the transition probabilities of the Markov-models and the a-posteriori probabilities (APPs) from the previous time $k-1$ are processed in order to compute the APPs of all possibly transmitted *indices* at time k by the recursion given e.g. in [3]. The APPs are used to estimate the receiver-outputs $\tilde{X}_k^{(j)}$ after the last iteration. Within the iterations the SISO decoder for a binary channel code requires a-priori informations for single bits. Since OE computes APPs of *indices* a conversion has to be carried out to L-values for the *bits*, which can be realized by summing up the APPs over all possible indices having a "1" or "0" at the bit-position under consideration. The L-values of the index-bits are converted to the output-L-values $L^{(S)}(\hat{I}_k)$ of the SISO source decoder by multiplexing, and the extrinsic information $L_e^{(S)}(\hat{I}_k)$ is computed. It is interleaved and forwarded to the SISO channel decoder as the a-priori information $L_a^{(C)}(\pi(\hat{I}_k))$.

Simulation results show that the iterative source-channel decoding works better than the non-iterative sequential channel and source decoding with the same component algorithms. A gain of about 1 dB in E_b/N_0 is achieved by only two iterations on moderately corrupted channels at the same quality of transmission.

References

[1] C. Berrou and A. Glavieux, "Near optimum error correcting coding and decoding: Turbo-codes," *IEEE Transactions on Communications*, vol. 44, no. 10, pp. 1261–1271, Oct. 1996.

[2] J. Hagenauer, E. Offer, and L. Papke, "Iterative decoding of binary block and convolutional codes," *IEEE Transactions on Information Theory*, vol. 42, no. 2, pp. 429–445, Mar. 1996.

[3] N. Görtz, "Joint source-channel decoding by channel-coded optimal estimation," in *Proc. of the 3rd ITG Conf. Source and Channel Coding*, Munich, Germany, Jan. 2000, pp. 267–272.

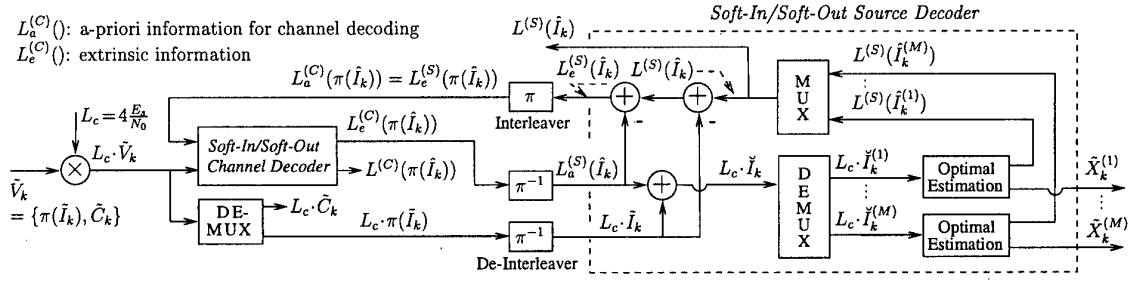


Fig. 2: Iterative source-channel decoding. Information is passed by log-likelihood ratios for single bits [2] being grouped into vectors.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Iterative Decoding Algorithms Updating Likelihood and Channel Values Based on Interim Hard Decision Results

Masayuki Ariyoshi and Iwao Sasase
Dept. of Information and Computer Science, Keio University, Yokohama, 223-8522 Japan
Email: ariyoshi@sasase.ics.keio.ac.jp

Abstract **— This paper presents novel decoding algorithms for turbo codes, in which the likelihood and channel values are updated in order for those values to become closer to the true values thorough the iterative decoding procedure. The criteria for updating the likelihood and channel values are proposed, those are based on the simple means to compare the interim hard decision results from each of component decoders.**

I. INTRODUCTION

Parallel concatenated convolutional (turbo) codes and iterative decoding achieve error performances close to Shannon limit[1]. The principle of the iterative decoding is that the component decoders exchange their outputs of the likelihood values each other, and update them though the iterative procedures. In the conventional decoding algorithms, only the likelihood values for systematic parts are treated to be updated[1,2].

Here we propose novel decoding algorithms which update both likelihood and channel values based on the interim hard decision results in order to minimize the effects of the error contained in those values.

II. THE ALGORITHMS

The iterative decoder in accordance with the proposed algorithm is shown in Fig. 1. Since the likelihood values show the log-likelihood ratio (LLR) of the decoded digit, the hard decision results of LLR values will be the final decoded results. Therefore, if the signs of LLR values output from the component decoders are different each other, it is obvious that either of them contains error. Based on this, when an error is detected on LLR values (L_1 or L_2), it should be updated more reliably. We here take a simple method to update LLR values by averaging them, as shown in Fig. 2. This makes the absolute value of updated LLR smaller, thus the effects of LLR errors can be minimized.

The systematic part of the channel value U is similarly updated by comparing it with the corresponding LLR values. Further, regarding the updating of redundant part of the channel values Y_1, Y_2, the LLR values are re-encoded in soft value (using log-likelihood addition) to be compared with. Then they are compared to detect errors, and updated in the same way.

III. PERFORMANCE EVALUATION

The performance of the proposed algorithm is evaluated with the parameters specified in IMT-2000 draft[3], i.e., r=1/3, K=3, multi-stage interleaver, etc. The results are shown in Figs. 3 and 4, where SOVA[2] based component decoders are employed.

It is shown that the proposed algorithm improves BER performance as iterations go on. Also, the achievable BER limit is improved by the effective updating method. Moreover, it is possible with the proposed algorithm to reduce the decoding process time by stopping the iterations much earlier.

IV. CONCLUSIONS

Novel decoding algorithms for turbo codes to update the likelihood and channel values based on the interim hard decision results have been presented. By updating those values more reliably, the proposed algorithms improve BER performance, and reduce the iterations.

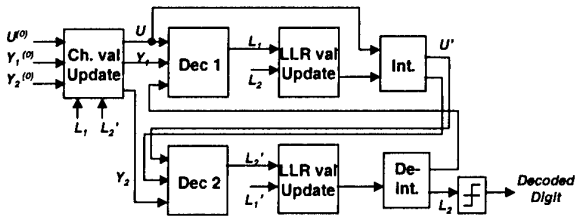


Fig.1 Iterative decoder updating LLR and channel values

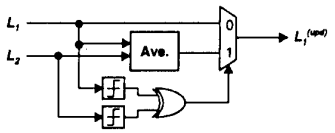


Fig.2 Likelihood value updating (ex. following Dec 1)

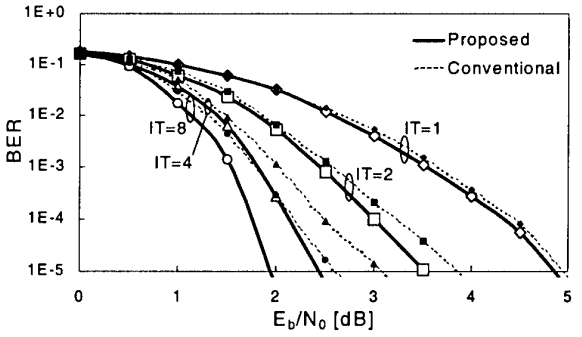


Fig.3 Bit error rate as a function of E_b/N_0 (AWGN)

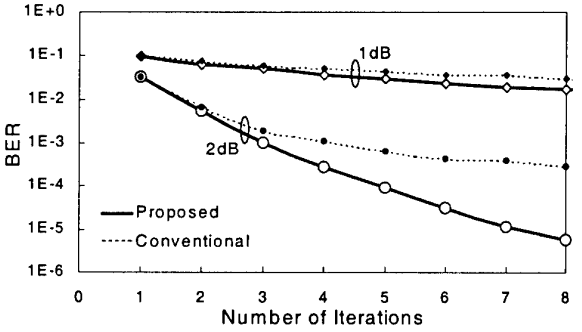


Fig.4 Bit error rate as a function of iterations (AWGN)

REFERENCES

[1] C. Berrou, et. al., "Near Shannon Limit Error-Correcting Coding and Decoding: Turbo Codes(1)," *Proc. ICC 93.*

[2] J. Hagenauer, et. al., "Iterative Decoding of Binary Block and Convolutional Codes," *IEEE Trans. Info. Theory, vol.42, no.2, 1996.*

[3] 3GPP, TS25.212 v0.0.1, "Multiplexing and Channel Coding (FDD)," Feb., 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Asymptotic Performance of Multiple Description Lattice Quantizers

Vinay A. Vaishampayan
AT&T Shannon Laboratory
180 Park Avenue, Florham Park, NJ 07932
e-mail: vinay@research.att.com

N. J. A. Sloane
AT&T Shannon Laboratory
180 Park Avenue, Florham Park, NJ 07932
e-mail: njas@research.att.com

Sergio D. Servetto
Ecole Polytechnique Fédérale de Lausanne
CH-1015 Lausanne, Switzerland
e-mail:
servetto@lcavsun1.epfl.ch

Abstract — **The high-rate squared-error distortions of a balanced multiple description lattice vector quantizer are analyzed for a memoryless source with probability density function p, differential entropy $h(p) < \infty$, and lattice codebook Λ. For any $a \in (0,1)$ and rate pair (R,R), it is shown that the two-channel distortion $\bar{d}_0$ and the channel 1 (or channel 2) distortion $\bar{d}_s$ satisfy**

$$\lim_{R\to\infty} \bar{d}_0 2^{2R(1+a)} = G(\Lambda)2^{2h(p)}/4$$

and

$$\lim_{R\to\infty} \bar{d}_s 2^{2R(1-a)} = G(S_L)2^{2h(p)},$$

where $G(\Lambda)$ is the normalized second moment of a Voronoi cell of the lattice Λ and $G(S_L)$ is the normalized second moment of a sphere in L dimensions.

I. Introduction

We consider a two-channel multiple description quantization system for a discrete-memoryless source with differential entropy $h(p)$. The quantizer transmits information on each channel at rate R bits/sample. The mean-squared error when both channels work is denoted by $\bar{d}_0$ and when either channel works is denoted by $\bar{d}_s$.

It has been shown [1] that for a uniform entropy-coded multiple description quantizer and any $a \in (0,1)$ the distortions satisfy

$$\begin{aligned} \lim_{R\to\infty} \bar{d}_0(R)2^{2R(1+a)} &= \frac{1}{4}\left(\frac{2^{2h(p)}}{12}\right), \\ \lim_{R\to\infty} \bar{d}_s(R)2^{2R(1-a)} &= \left(\frac{2^{2h(p)}}{12}\right). \end{aligned} \quad (1)$$

On the other hand, by using a random quantizer argument it was shown [2] that by encoding vectors of infinite block length, it is possible to achieve distortions

$$\begin{aligned} \lim_{R\to\infty} \bar{d}_0(R)2^{2R(1+a)} &= \frac{1}{4}\left(\frac{2^{2h(p)}}{2\pi e}\right), \\ \lim_{R\to\infty} \bar{d}_s(R)2^{2R(1-a)} &= \left(\frac{2^{2h(p)}}{2\pi e}\right). \end{aligned} \quad (2)$$

Thus in multiple description quantization it is possible to achieve a reduction in the granular distortion by 1.53 dB, simultaneously for the two-channel and the side distortion.

The goal of this paper is to analyze constructions given in [3] for closing this "1.53 dB" gap. The system to be analyzed is illustrated in Fig. 1. Our approach is as follows. From classical quantization theory, we know that the gap between scalar quantization and the rate distortion bound may be closed by using vector quantizers with lattice codebooks. Certainly, by following this approach we can also close the gap between the two-channel distortion and the rate-distortion bound. In particular, this will allow us to replace the factor (1/12) in the expression for $\bar{d}_0$ in (1) with $G(\Lambda)$, the normalized second moment of the Voronoi region of a lattice point. The main question we address here is that of simultaneously reducing $\bar{d}_1$. How can such a reduction be achieved and what is the quantity that will replace the factor (1/12) in the expression for $\bar{d}_1$ in (1)? We will show through a constructive procedure that the distortion $\bar{d}_1$ can be reduced by solving a specific labeling problem. To our surprise, the quantity that replaces (1/12) is $G(S_L)$, the normalized second moment of a *sphere* in L dimensions.

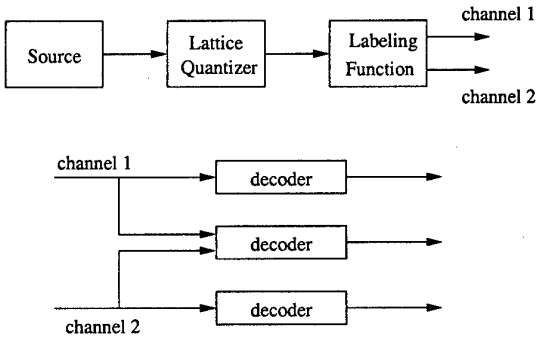


Figure 1: A multiple description vector quantizer with a lattice codebook.

For details the reader is referred to the full paper [4], which will be published elsewhere.

References

[1] V. Vaishampayan and J.-C. Batllo, "Asymptotic analysis of multiple description quantizers," *IEEE Trans. Inform. Th.*, vol. 44, pp. 278–284, Jan. 1998.

[2] V. Vaishampayan, J.-C. Batllo and A. R. Calderbank, "On reducing granular distortion in multiple description quantization," in *Abstracts of Papers, IEEE Int. Symp. Inform. Theory*, Cambridge, MA, August 1998.

[3] S. D. Servetto, V. A. Vaishampayan and N. J. A. Sloane, "Multiple Description Lattice Vector Quantization", in *Proceedings 1999 Data Compression Conference*, pp. 13–22, IEEE Press, 1999.

[4] V. Vaishampayan, N. J. A. Sloane and Sergio D. Servetto, "Multiple description vector quantization with lattice codebooks: design and analysis," (submitted).

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On Optimal Frame Expansions for Multiple Description Quantization

Sanjeev Mehrotra
Stanford Univ./Microsoft Corp.
One Microsoft Way
Redmond, WA 98052
sanjeevm@ieee.org

Philip A. Chou
Microsoft Corp.
One Microsoft Way
Redmond, WA 98052
pachou@microsoft.com

Abstract — **We study the problem of finding the optimal overcomplete (frame) expansion and bit allocation for multiple description quantization of a Gaussian signal at high rates over a lossy channel.**

I. Introduction

The setup is shown in Figure 1. In multiple description quantization using overcomplete (frame) expansions [1, 2], an input signal $\boldsymbol{x} \in \mathbb{R}^K$ is represented by a vector $\boldsymbol{y} = \boldsymbol{F}\boldsymbol{x} \in \mathbb{R}^N$, $N > K$. $\boldsymbol{F}$ is a $N \times K$ matrix, called the frame operator. It is assumed any K rows of $\boldsymbol{F}$ span $\mathbb{R}^K$. The coefficients of $\boldsymbol{y}$ are scalar quantized to obtain $\hat{\boldsymbol{y}}$, and are then independently entropy coded using on average a total of R bits allocated among the N coefficients. In channel state s, the decoder receives $N_{r,s} \leq N$ coefficients after potential erasures, and reconstructs the signal $\hat{\boldsymbol{x}}$ from the received coefficients. The number of channel states is 2^N since each coefficient can be either received or lost. For a given distribution over channel states, we wish to find the frame operator $\boldsymbol{F}$ and the bit allocation for the transform coefficients that minimizes the expected squared error $D = E[\|\boldsymbol{x} - \hat{\boldsymbol{x}}\|^2]$ subject to a constraint on the average rate R, for asymptotically large R and Gaussian $\boldsymbol{x}$.

II. Analysis

Without loss of generality, assume that $\boldsymbol{x}$ is distributed with zero mean and diagonal covariance matrix $\boldsymbol{R}_{\boldsymbol{xx}} = \mathrm{diag}(\sigma_0^2, ..., \sigma_{K-1}^2)$ (else can use KLT). Let $\boldsymbol{q} = \boldsymbol{y} - \hat{\boldsymbol{y}}$ be the quantization error and let $\boldsymbol{e} = \boldsymbol{x} - \hat{\boldsymbol{x}}$ be the reconstruction error. At high rate, assume $\boldsymbol{q}$ is distributed with zero mean and diagonal covariance matrix with $E[\|q_i\|^2] = c\sigma_{y_i}^2 2^{-2R_i}$, where $c = \pi e/6$ if entropy coded uniform scalar quantization is used. The distortion can be written as $D = \sum_s p_s D_s$, where $D_s = E[\|\boldsymbol{e}\|^2 | S = s]$, and p_s is the probability of the channel being in state s. Let $\boldsymbol{y}_{r,s}$ denote the $N_{r,s}$ dimensional vector of received coefficients. Let $\boldsymbol{F}_{r,s}$ be a $N_{r,s} \times K$ matrix consisting of rows of $\boldsymbol{F}$ corresponding to the received coefficients.

To obtain an expression for D_s, there are two cases to consider: $N_{r,s} \geq K$ and $N_{r,s} < K$. When $N_{r,s} \geq K$, the decoder has enough information to localize the input vector to a finite cell. Although the actual reconstruction will use a consistent reconstruction [1, 3], for analysis purposes, we use the optimal linear reconstruction as $\hat{\boldsymbol{x}} = \boldsymbol{F}_{r,s}^+ \hat{\boldsymbol{y}}_{r,s}$, where $\boldsymbol{F}^+$ is the pseudo-inverse of $\boldsymbol{F}$. Since $\boldsymbol{x} = \boldsymbol{F}_{r,s}^+ \boldsymbol{y}_{r,s}$, the conditional distortion can be written as $D_s = E[\|\boldsymbol{e}\|^2 | S = s] = E[\|\boldsymbol{F}_{r,s}^+ \boldsymbol{q}_{r,s}\|^2]$. When $N_{r,s} < K$, then there is not enough information to localize $\boldsymbol{x}$ to a finite cell. In particular $\boldsymbol{x}$ is bounded in $N_{r,s}$ dimensions and unbounded in $K - N_{r,s}$ dimensions. Thus, $\boldsymbol{x} = \boldsymbol{F}_{r,s}^+ \boldsymbol{y}_{r,s} + (\boldsymbol{F}_{r,s}^\perp)^T \boldsymbol{y}_{r,s}^\perp$, where the rows of $\boldsymbol{F}_{r,s}^\perp$ form an orthonormal basis for the subspace orthogonal to the span of the rows of $\boldsymbol{F}_{r,s}$ and $\boldsymbol{y}_{r,s}^\perp$ is a $K - N_{r,s}$ dimensional vector. Now the optimal linear reconstruction is

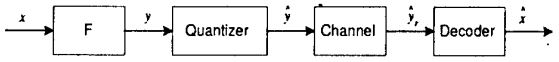


Fig. 1: System setup.

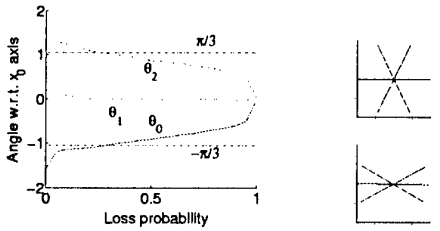


Fig. 2: Results for optimal 3×2 expansion: (a) θ_i (b) φ_i for loss probabilities of 0.2 (top) and 0.95 (bottom).

$\hat{\boldsymbol{x}} = \boldsymbol{F}_{r,s}^+ \hat{\boldsymbol{y}}_{r,s} + (\boldsymbol{F}_{r,s}^\perp)^T E[\boldsymbol{y}_{r,s}^\perp | \boldsymbol{y}_{r,s} = \hat{\boldsymbol{y}}_{r,s}]$ which gives a distortion of $D_s = E[\|\boldsymbol{F}_{r,s}^+ \boldsymbol{q}_{r,s}\|^2] + E[\|\boldsymbol{y}_{r,s}^\perp\|^2 | \boldsymbol{y}_{r,s} = \hat{\boldsymbol{y}}_{r,s}]$. Since the source is Gaussian, $E[\|\boldsymbol{y}_{r,s}^\perp\|^2 | \boldsymbol{y}_{r,s}]$ can be easily computed.

Using the equations for D_s and the fact that $E[\boldsymbol{q}\boldsymbol{q}^T]$ is diagonal, the portion of distortion that can be minimized by bit allocation can be written as $D_b = \sum_{i=0}^{N-1} \alpha_i \sigma_{y_i}^2 2^{-2R_i}$, where α_i is a function of the transform $\boldsymbol{F}$, the channel state probabilities p_s, and the quantization constant c. Let D_{nb} be the remaining portion of the distortion D. Minimizing D_b is a classic bit allocation problem with solution given by $R_i = R/N + \log_2(\alpha_i \sigma_{y_i}^2 / (\prod_{j=0}^{N-1} \alpha_j \sigma_{y_j}^2)^{1/N})/2$. This gives an optimal D_b of $D_b^* = N(\prod_{j=0}^{N-1} \alpha_j \sigma_{y_j}^2)^{1/N} 2^{-2R/N}$. To find the optimal transform, we have to minimize $D_b^* + D_{nb}$. Since it is hard theoretically, we use numerical gradient descent techniques by varying one coefficient at a time.

Results show that at high loss rates D_{nb} is the dominating term which is minimized by repeating the coefficient with highest variance. At low loss rates, D_b^* is the dominating term which is minimized by the optimal source coder. Results are shown for 3×2 expansion in Figure 2, where the values for $\theta_i = \tan^{-1}(F_{i1}/F_{i0})$, $i = 0, 1, 2$ are plotted with rate constraint $R = 6$ bits and variances $\sigma_0^2 = 4$ and $\sigma_1^2 = 1$. Also shown is φ_i, which is the ith row of matrix $\boldsymbol{F}$.

References

[1] V. K. Goyal, M. Vetterli, and N. T. Thao. Quantized overcomplete expansions in $\mathbb{R}^n$: Analysis, synthesis, and algorithms. *IEEE Trans. Information Theory*, 44(1):16–31, January 1998.

[2] V. K. Goyal, J. Kovačević, and M. Vetterli. Quantized frame expansions as source-channel codes for erasure channels. In *Proc. Data Compression Conference*, pages 326–335, Snowbird, UT, March 1999. IEEE Computer Society.

[3] P.A. Chou, S. Mehrotra, and A. Wang. Multiple description decoding of overcomplete expansions using projection onto convex sets. In *Proc. Data Compression Conference*, pages 72–81, Snowbird, UT, March 1999. IEEE Computer Society.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Multiple Description Quantization by Deterministic Annealing

Prashant Koulgi, Shankar L. Regunathan, Kenneth Rose[1]
Dept. of ECE, University of California, Santa Barbara, CA 93106, rose@ece.ucsb.edu

We consider the design of vector quantizers for diversity-based communication over two channels of capacities R_1 and R_2 with possibly differing failure probabilities. A Multiple Description Vector Quantizer (MDVQ) maps an n-dimensional source vector x to n-dimensional code vectors $\hat{x}_{ij}^0$, $\hat{x}_i^1$ and $\hat{x}_j^2$ from the code books $\hat{\mathcal{X}}^0$, $\hat{\mathcal{X}}^1$ and $\hat{\mathcal{X}}^2$ respectively. We use the notation of [1]. Let $d(x,y)$ be a single-letter distortion measure, and random vectors X and $\hat{X}^m, m = 0,1,2$ represent the source and decoder outputs respectively. For given values of R_1, R_2, λ_1 and λ_2 we then wish to find an MDVQ which minimizes the average distortion cost

$$D = E\{d(X,\hat{X}^0)\} + \lambda_1 E\{d(X,\hat{X}^1)\} + \lambda_2 E\{d(X,\hat{X}^2)\}.$$

We shall assume $d(x,y) = ||x-y||^2$. Note that λ_1 and λ_2 may be interpreted as the channel failure probabilities.

The problem of finding the rates asymptotically achievable by MDVQs of very large dimensions is only partially solved. For references to the extensive literature on this problem, see [2]. In [1], Vaishampayan derived an iterative algorithm for the design of multiple description scalar quantizers (MDSQs), which is closely related to Lloyd's algorithm for quantizer design. While the algorithm monotonically decreases the average distortion cost, it is likely to be trapped in poor local minima, unless "good" initial code books and initial index assignment are used. Vaishampayan recognized this shortcoming, and proposed heuristic initializations for the special case where the two channels have identical capacities and failure probabilities (i.e., $\lambda_1 = \lambda_2$ and $R_1 = R_2$) [1]. But these do not generalize well to vectors, or to asymmetric channels.

We propose a Deterministic Annealing (DA) approach to the design of unstructured MDVQs for two-channel diversity systems, where the channels may have possibly differing capacities and failure probabilities. Our approach is independent of initialization, does not assume any prior knowledge of the source density and avoids many poor local minima of the cost surface. It consists of iterative optimization of a random encoder at gradually decreasing levels of randomness, as measured by the Shannon entropy. At the limit of zero entropy, a hard multiple description quantizer is obtained. Our approach is inspired by, and builds on, the DA approach for vector quantizer design [3].

Let us begin by assuming that the three code-books, $\hat{\mathcal{X}}^0 = \{\hat{x}_{ij}^0\}$, $\hat{\mathcal{X}}^1 = \{\hat{x}_i^1\}$ and $\hat{\mathcal{X}}^2 = \{\hat{x}_j^2\}$ are given. We use a random encoding rule, and assign input source vector x to the index pair (i,j) with probability $q(ij|x)$. These encoding probabilities are chosen to minimize D subject to a specified level of randomness, measured by the Shannon entropy. Correspondingly, we minimize the Lagrangian $F = D - TH$. Here H is the entropy, and the Lagrangian multiplier, T, is called the "temperature" of the system in reference to the statistical physics analogy. Minimizing F with respect to $q(ij|x)$ gives

$$q(ij|x) = \frac{\exp[-(\frac{1}{T})\{||x-\hat{x}_{ij}^0||^2 + \lambda_1||x-\hat{x}_i^1||^2 + \lambda_2||x-\hat{x}_j^2||^2\}]}{Z_x},$$

where the normalizing factor Z_x ensures that $\sum_{ij} q(ij|x) = 1$. Further, the corresponding minimum of F is easily seen to be $F^* = \min_{q(ij|x)} F = -T\sum_x p(x)\log Z_x$. We now find the optimal sets of reproduction vectors which minimize F^* for this random encoder:

$$\hat{x}_{ij}^0 = \sum_x p(x|ij)x, \quad \hat{x}_i^1 = \sum_x p(x|i)x, \quad \hat{x}_j^2 = \sum_x p(x|j)x.$$

Our algorithm consists of minimizing F^* with respect to the code vectors starting at a high temperature and tracking the minimum while decreasing the temperature.

Scalar (for asymmetric channels) and vector quantizers designed by DA provided substantial gains over those designed by the iterative algorithm of [1] even for small codebook sizes. For a 2-d Gauss-Markov source with $\rho = 0.9$, the average distortion cost of the DA-designed MDVQ (with $R_1 = R_2 = 1.5$bpss, $\lambda_1 = \lambda_2 = 0.01$) was 0.7dB lower than the best of twenty different MDVQs designed by the Lloyd approach with random initializations. Note that the initializations suggested in [1] do not extend to vectors. These initializations can be used in the design of scalar quantizers. While the heuristic initializations are better than random initializations, the DA-designed quantizers outperformed both. For scalar quantizers of a Gaussian source, the average distortion cost for DA-designed MDSQs of $R_1 = R_2 = 3$bpss, $\lambda_1 = 0.006$, $\lambda_2 = 0.012$ and $R_1 = 3$bpss, $R_2 = 2$bpss, $\lambda_1 = \lambda_2 = 0.01$ were respectively 0.5dB and 1.0dB lower than the best of the MDSQs designed by the algorithm of [1], with both random and heuristic initializations.

In [2], El Gamal and Cover are credited with this weak characterization of a multiple description achievable region: rate-distortion quintuples $(R_1, R_2, D_0, D_1, D_2)$ are achievable if there exist random variables I_1 and I_2 jointly distributed with the source X such that $R_m \geq I(X;I_m)$, $m = 1,2$, and $R_1 + R_2 \geq I(X;I_1,I_2) + I(I_1;I_2)$ and side and central reproductions of the forms $\hat{X}^m = g_m(I_m)$, $m = 1,2$, and $\hat{X}^0 = g_0(I_1,I_2)$ such that $E\{d(X,\hat{X}^t)\} \leq D_t$, $t = 0,1,2$. The DA algorithm for MDVQ design can be shown to imitate parametric determination of the convex hull of this achievable region.

References

[1] V. A. Vaishampayan, "Design of multiple description scalar quantizers," *IEEE Trans. Inform. Theory*, vol. 39, pp. 821-834, May 1993.

[2] Z. Zhang and T. Berger, "New results in binary multiple descriptions," *IEEE Trans. Inform. Theory*, vol. IT-33, pp. 502-521, July 1987.

[3] K. Rose, E. Gurewitz and G. C. Fox, "Vector Quantization by Deterministic Annealing," *IEEE Trans. Inform. Theory*, vol. 38, pp. 1249-1257, July 1992.

[1]This work was supported in part by the NSF under grant no. MIP-9707764, the UC MICRO program, Conexant Systems, Inc., Fujitsu Laboratories of America, Inc., Lernout & Hauspie Speech Products, Lucent Technologies, Inc. and Qualcomm, Inc.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

A constructive approach to distributed source coding with symmetric rates

S. Sandeep Pradhan and Kannan Ramchandran [1]
Department of EECS, University of California
Berkeley, CA-94720,USA
pradhan5,kannanr@eecs.berkeley.edu

Ralf Koetter
Dept. of ECE, University of Illinois
Urbana, IL-61801, USA
koetter@pizza.csl.uiuc.edu

Abstract — **We propose encoding and decoding methods based on linear codes, to achieve all the integral points in the rate region of Slepian-Wolf [1] problem. The extension of these concepts to the construction of Euclidean-space codes is also studied and analyzed for the case of trellis codes.**

I. Introduction

Distributed source coding deals with the efficient encoding of correlated sources that do not communicate with one another. This was first introduced in [1] where it was shown that two correlated memoryless sources, X and Y can be separately compressed at a total rate approaching the joint entropy. In this paper we focus on the sensor network system considered by Flynn and Gray [2] as shown in Fig. 1. Here we have a source X which is observed in a corrupted form by a number of sensors. Let Y_i denote the signals captured by the i^{th} sensor. Each sensor encodes its message into bits to be transmitted to a receiver to get the optimal reconstruction of the signal X. Here we consider symmetric encoding of correlated sources in a bandwidth-restricted system.

II. Symmetric Encoding of Binary Sources

We consider an example for illustration of the basic concepts. Consider a pair[2] of correlated discrete memoryless sources X and Y such that $X, Y \in \{0,1\}^n$ and $d_H(X,Y) \leq t$ where $d_H(.,.)$ is the Hamming distance. According to [1], X and Y can be separately compressed at rate pairs R_1, R_2 given by

$$R_1, R_2 \geq n-k, R_1 + R_2 \geq 2n-k, \qquad (1)$$

where k meets the sphere packing bound. Let us consider a system based on $(n, k, 2t+1)$ linear binary code, $\mathcal{C}$, to achieve these points on the rate region.

Theorem: $\mathcal{C}$ achieves all the integral points on (1)

Proof: Let $\mathbf{G}$ be the generator matrix of $\mathcal{C}$. Let $\mathbf{G1}$ and $\mathbf{G2}$ be $n-R_1 \times n$ and $n-R_2 \times n$ matrices respectively, obtained by a partition of k rows of $\mathbf{G}$. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be the linear codes associated with $\mathbf{G1}$ and $\mathbf{G2}$ respectively. The encoders associated with X and Y send the index of the coset of these subcodes containing their outcome. Decoding involves finding a pair of codewords from the given cosets of $\mathcal{C}_1$ and $\mathcal{C}_2$ which are closest in distance. Q.E.D.

III. Lossy encoding using trellis codes:

Let the random processes Y_1, Y_2 received by the sensors are given by $Y_i = X + N_i$ for $i = 1, 2$, where N_i are independent of X. We need to encode Y_1 and Y_2 separately to be transmitted to the receiver to get an optimal reconstruction of X. First we quantize them separately using the quantizers designed for their marginal distributions. We then exploit the correlation between Y_1 and Y_2 (using algebraic codes) to reduce the rate of transmission. We encode the observations in blocks while minimizing the mean squared error.

Let us consider a scalar quantizer with 8 levels. Suppose $R_1 = R_2 = 2$ bits/source sample. Let ∇ be the set of reconstruction levels of the scalar quantizer. We partition ∇^n into 2^{2n} cosets each containing 2^n code vectors. The encoder-1 and encoder-2 (of Y_1 and Y_2 respectively) partition ∇^n in two different ways. Consider the 4-state Ungerboeck trellis built on ∇ with a 2/3 convolutional encoder with the generator matrix polynomial $\mathbf{G(t)}$. We form $\mathbf{G1(t)}$ and $\mathbf{G2(t)}$ by partitioning the rows of $\mathbf{G(t)}$. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be the codes associated with $\mathbf{G1(t)}$ and $\mathbf{G2(t)}$ respectively. Each of the encoders, sends the index of the coset of these subcodes containing the observed quantized output, thus spending 2 bits/source sample. We obtain the most probable sequence-pair using the Viterbi algorithm in the tensor product trellis. It can be shown that the decoding complexity is the same as that of decoding a codeword in the underlying trellis code.

Distance Properties: Let us denote the i^{th} coset of $\mathcal{C}_j$ as $\mathcal{C}_j(i)$ for $i \in \{1, 2, \ldots, 2^{2n}\}$ and $j = 1, 2$. For any coset pairs (i, j), define: $\alpha(i,j)$= minimum of distances $d_e(\mathbf{c1}, \mathbf{c2})$ between any two codewords $(\mathbf{c1}, \mathbf{c2}) \in (\mathcal{C}_1(i), \mathcal{C}_2(j))$ such that $\exists$ at least one pair $(\mathbf{c3}, \mathbf{c4}) \neq (\mathbf{c1}, \mathbf{c2})$ with $d_e(\mathbf{c1}, \mathbf{c2}) \geq d_e(\mathbf{c3}, \mathbf{c4})$, $(\mathbf{c3}, \mathbf{c4}) \in \mathcal{C}_1(i), \mathcal{C}_2(j))$. We define the correlation distance, d_c as follows:

$$d_c = \underset{i,j \in \{1,2,\ldots,2^{2n}\}}{\text{minimum}} \{\alpha(i,j)\} \qquad (2)$$

Theorem: For all the trellis codes $d_c \geq \frac{d_{min}}{2}$.

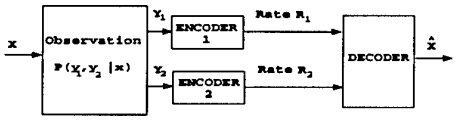


Figure 1: Sensor network communication system: Encoders observe corrupted version of the source X, and transmit their information to the decoder to get the best reconstruction of X. The encoders do not communicate with each other.

[1] This work was supported in part by DARPA Grant F29601-99-1-0169 and NSF (CAREER) Grant MIP 97-03181.

[2] extension to more than 2 sources is straightforward

References

[1] D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. IT*, pp. 471–480, Jul 1973.

[2] T. J. Flynn and R. M. Gray, "Encoding of correlated observations," *IEEE Trans. IT*, pp. 773–787, Nov 1987.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Shannon Capacity of Large Odd Cycles

Tom Bohman, Miklós Ruszinkó, Luboš Thoma
Dept. Mathematical Sciences
Carnegie Mellon University
Pittsburgh, PA 15213-3890, USA
email: tbohman,ruszinko,thoma@andrew.cmu.edu

Abstract — **It is known that** $\liminf_{n\to\infty}((2n+1)/2 - \Theta(C_{2n+1})) = 0$ **and that the** lim sup **of this difference is at most** $1/4$**, where** $\Theta(G)$ **is the Shannon capacity of the graph** G**. In this paper we prove that the above** lim sup **is at most** $1/6$ **and conjecture that the limit itself exists and equals** 0**. We show that the** lim sup **is small by constructing large independent sets in the third power of** C_{2n+1}**.**

I. Shannon Capacity

The *zero error capacity* of a discrete noisy channel C was invented by Shannon [5]. A channel consists of a finite set X of possible input letters and for each $x \in X$ a subset Y_x of a (not necessarily finite) output set Y. Here Y_x is the set of possible outputs of the channel on input x. Clearly, if the decoder receives an output $y \in Y_{x_1} \cap Y_{x_2}$ where $x_1 \neq x_2 \in X$ then the decoder cannot be certain of the input letter, i.e., it will make an error in decoding with a certain probability. On the other hand, if for $x \neq x' \in X$ we have $Y_x \cap Y_{x'} = \emptyset$, the decoder will be able to determine the exact input letter: it is the unique $x \in X$ for which the output y is contained in Y_x.

In order to determine the maximum number of letters that can be transmitted through the channel without the possibility of an error, Shannon associated a (characteristic) graph $G = G(C)$ to the channel C as follows. The vertices $V(G)$ of the graph G are labeled by the possible input letters ($|V(G)| = |X|$), and two vertices x_1, x_2 are adjacent iff $Y_{x_1} \cap Y_{x_2} \neq \emptyset$. Clearly, the labels of an independent set can be transmitted without an error. Therefore, the number of letters that can be transmitted by C without an error is exactly the *independence number* $\alpha(G)$.

If the sender transmitted k letters, say, $x_1, \ldots, x_k$, i.e., the channel has been used k times, then the output of the channel will also contain k symbols $y_1, \ldots, y_k$, $y_i \in Y_{x_i}$. This situation can be considered as a single use of the channel C^k, which has input set X^k, output set Y^k and the set of possible outputs $Y_{x_1} \times \cdots \times Y_{x_k}$ on input $x_1, \ldots, x_k$. The k^{th} power G^k of a graph G is defined as follows. The vertex set of G^k is $V(G^k) = V(G)^k$, and two vertices $(x_1, x_2, \ldots, x_k)$ and $(x'_1, x'_2, \ldots, x'_k)$ are adjacent iff for all $1 \leq i \leq k$ either $x_i = x'_i$ or x_i and x'_i are adjacent in G. It is easy to see that the number of sequences of length k that can be transmitted without an error is the independence number of the k^{th} power of $G(C)$.

The Shannon capacity of C is defined as

$$\Theta(C) = \sup_k \left(\alpha\left(G(C)^k\right)\right)^{1/k} = \lim_{k\to\infty} \left(\alpha\left(G(C)^k\right)\right)^{1/k}.$$

Note that the capacity gives a measure of the optimal perfomance of the channel when transmitting long sequences. This limit, by super-multiplicativity exists and – since $(\alpha(G))^k \leq \alpha(G^k)$ for an arbitrary graph G – it is always at least $\alpha(G)$. It is worth of mentioning, that Shannon originally [5] defined the capacity as $\log \Theta$ (we use the definition and notation of Lovász [4]). Also notice, that Θ depends on the graph $G(C)$ only, and every graph is the characteristic graph of some channel. Therefore, we consider the Shannon capacity of graphs:

$$\Theta(G) = \sup_k \left(\alpha(G^k)\right)^{1/k} = \lim_{k\to\infty} \left(\alpha(G^k)\right)^{1/k}.$$

Since Shannon's invention of the capacity [5] in 1956, it has been one of the central topics in both information theory and extremal graph theory. For a more detailed overview of this fascinating topic we refer the reader to the excellent surveys of Alon [1] and Gargano, Körner, Vaccaro [2].

The aim of this paper is to investigate the Shannon capacity of large odd cycles C_{2n+1}. It follows from a result of Hales [3] that for an infinite subsequence n_k, $k = 1, 2, \ldots$, of positive integers the difference $n_k + 1/2 - \Theta(C_{2n_k+1})$ tends to zero as k tends to infinity (note $\alpha(C_{2n+1}) = n$), i.e.,

Theorem I.1 (Hales)

$$\liminf_{n\to\infty}(n + 1/2 - \Theta(C_{2n+1})) = 0.$$

Hales also showed that the lim sup of this difference is at most $1/4$. Modifying Hales linear algebraic construction, we show the difference cannot be larger then $1/6$ as n tends to infinity

Theorem I.2

$$\limsup_{n\to\infty}(n + 1/2 - \Theta(C_{2n+1})) \leq 1/6.$$

We strongly believe that the limit as n tends to infinity of the difference $n + 1/2 - \Theta(C_{2n+1})$ exists and is equal to 0.

References

[1] N. Alon, "Graph powers", *Combinatorics, Probability & Computing*, to appear.

[2] L. Gargano, J. Körner, U. Vaccaro, "Capacities: From information theory to extremal set theory", *Journal of Combinatorial Theory – A*, 68 (1994), 296-316.

[3] R.S. Hales, "Numerical invariants and the strong product of graphs", *Journal of Combinatorial Theory – B*, 15 (1973), 146-155.

[4] L. Lovász, "On the Shannon capacity of a graph", *IEEE Transactions on Information Theory* 25(1) (1979), 1-7.

[5] C. E. Shannon, "The zero-error capacity of a noisy channel", *IRE Transactions on Information Theory*, 2(3) (1956), 8–19.

[1]The second author was partially supported by OTKA Grants T 030059 and T 29074, FKFP 0607/1999.

[2]The third author was partially supported by NSF grant DMS-9970622.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Asymptotic Capacity of the Two-Dimensional Square Constraint*

Zsigmond Nagy
Department of Electrical and Computer Engineering, University of California, San Diego, CA 92093-0407
nagy@code.ucsd.edu

Kenneth Zeger
Department of Electrical and Computer Engineering University of California, San Diego, CA 92093-0407
zeger@ucsd.edu

Abstract — **Two-dimensional run length limited codes satisfying the square constraint are considered. Let S denote a square of area $A(S)$ and let α_n be a positive sequence satisfying $\lim_{n\to\infty}\alpha_n = \infty$. It is shown that the capacity C_n corresponding to the set $\mathcal{S}_n = \alpha_n S \cap \mathbf{Z}^2$ asymptotically satisfies**

$$\lim_{n\to\infty} C_n \cdot \frac{\alpha_n^2}{\log_2 \alpha_n^2} = \frac{4}{A(S)} \ .$$

I. Introduction

One-dimensional run length constraints are important in magnetic recording applications and two-dimensional run length constraints have recently gained interest due to optical recording applications [1, 2, 3]. A two-dimensional run length constraint requires that a binary labeling of the integer lattice $\mathbf{Z}^2$ have a specified minimum and maximum number of zeros between consecutive ones both horizontally and vertically. Additional constraints, such as run length constraints along diagonals can also be imposed in order to more accurately model optical recording devices. In this paper we examine the asymptotic behavior of the "square" constraint. The square constraint imposes the condition that for every "one" stored in the plane, it must be surrounded by a square of zeros of some given side length. As the side length of the square grows to infinity the amount of information that can be stored per unit area shrinks to zero. In other words the capacity of the constraint falls to zero. In this paper we determined the exact rate that the capacity of the square constraint falls to zero as a function of the area of the constraint.

II. Definitions and Results

Let $\mathbf{R}^2$ denote the two-dimensional plane, and $\mathbf{Z}^2$ the two-dimensional integer lattice (i.e. $\mathbf{Z}^2 = \{(x_1, x_2) : x_1, x_2 \in \mathbf{Z}\}$).

Suppose that $\mathcal{V} \subset \mathbf{Z}^2$, such that $(0,0) \in \mathcal{V}$. The code $f : \mathbf{Z}^2 \to \{0,1\}$ *satisfies the constraint* $\mathcal{V}$ (or, f defines a *valid labeling* of $\mathbf{Z}^2$ with respect to $\mathcal{V}$), if for every $\mathbf{x} \in \mathbf{Z}^2$

$$f(\mathbf{x}) = 1 \Rightarrow f(\mathbf{y}) = 0 \qquad \text{for } \forall \mathbf{y} \in \mathcal{V} + \mathbf{x}, \ \ \mathbf{y} \neq \mathbf{x} \ . \quad (1)$$

A subset of $\mathbf{Z}^2$ of the form $\mathcal{R}_{(a,b)}^{(c,d)} = \{(\mathbf{x},\mathbf{y}) \in \mathbf{Z}^2 : a \leq x \leq c, b \leq y \leq d\}$ for some integers a, b, c, d, will be called a rectangle. A binary labeling of the rectangle $\mathcal{R}_{(a,b)}^{(c,d)}$is *valid* with respect to a given constraint $\mathcal{V}$, if the labeling can be extended to a labeling of $\mathbf{Z}^2$ satisfying the constraint $\mathcal{V}$. Let $N_{\mathcal{V}}(m,n)$ denote the number of valid labelings of the rectangle $\mathcal{R}_{(0,0)}^{(n,m)}$ with respect to $\mathcal{V}$. The capacity $C_{\mathcal{V}}$ corresponding to a set $\mathcal{V} \subset \mathbf{Z}^2$ including the origin is defined as

$$C_{\mathcal{V}} = \lim_{m,n\to\infty} \frac{\log_2 N_{\mathcal{V}}(m-1, n-1)}{mn} \ .$$

*This work was supported in part by the National Science Foundation.

The proof in [1] can be generalized to show that the above limit exists.

III. The asymptotic capacity of the square constraint

In this section $S \subset \mathbf{R}^2$ will denote a square centered at the origin, whose sides are parallel to the coordinate axes. Let $\mathcal{S} = S \cap \mathbf{Z}^2$, and let α_n be a sequence of positive real numbers, such that $\lim_{n\to\infty}\alpha_n = \infty$. Consider the sequence of capacities C_n corresponding to the constraints $\mathcal{S}_n = \alpha_n S \cap \mathbf{Z}^2$, as $n \to \infty$. In the main theorem of this section we determine the asymptotic rate that C_n goes to zero as $n \to \infty$.

Lemma 1 *Let C_n denote the capacity corresponding to the constraint $\mathcal{S}_n$. Write $\mathcal{S}_n = \mathcal{R}_{(-d,-d)}^{(d,d)}$ for some integer d, and consider the set $\hat{\mathcal{S}}_n = \mathcal{R}_{(0,0)}^{(d,d)}$. For every positive integer n, C_n satisfies the inequality*

$$C_n \leq \frac{\log_2(A(\hat{\mathcal{S}}_n) + 1)}{A(\hat{\mathcal{S}}_n)} \ ,$$

where $A(\hat{\mathcal{S}}_n)$ denotes the number of lattice points in $\hat{\mathcal{S}}_n$.

Lemma 2 *Let C_n denote the capacity corresponding to the constraint $\mathcal{S}_n$. Write $\mathcal{S}_n = \mathcal{R}_{(-d,-d)}^{(d,d)}$ for some integer d, and consider the set $\hat{\mathcal{S}}_n = \mathcal{R}_{(0,0)}^{(d,d)}$. For $\forall \epsilon > 0, \forall \gamma \in \mathbf{Z}^+$ there exists N, such that for $\forall n > N$,*

$$C_n \geq \left(\frac{\gamma}{\gamma+1}\right)^2 \frac{\log_2 A(\hat{\mathcal{S}}_n))}{A(\hat{\mathcal{S}}_n)} - \epsilon. \quad (2)$$

Theorem 1 *Let C_n denote the capacity corresponding to the constraint $\mathcal{S}_n = \alpha_n S \cap \mathbf{Z}^2$. Then,*

$$\lim_{n\to\infty} C_n \cdot \frac{\alpha_n^2}{\log_2 \alpha_n^2} = \frac{4}{A(S)} \ .$$

References

[1] A. Kato and K. Zeger, "On the Capacity of Two-Dimensional Run Length Constrained Channels," *IEEE Trans. Inform. Theory.* vol. 45, July 1999, pp.1527–1540.

[2] W. Weeks and R. E. Blahut "The Capacity and Coding Gain of Certain Checkerboard Codes," *IEEE Trans. Inform. Theory.* vol. 44, May 1998, pp. 1193-1203

[3] P. H. Siegel and J. K. Wolf, "Bit Stuffing Bounds on the Capacity of 2-Dimensional Constrained Arrays," *Proceedings of 1998 IEEE International Symposium on Information Theory,* Boston, MA, August 1998, p. 323.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Capacity of retro-information channels

Philippe Jacquet
INRIA
78153 Le Chesnay cedex
France
philippe.jacquet@inria.fr

Véronique Joly
ONERA
92322 Chatillon cedex
France
joly@onera.fr

Abstract — **Retro-information is possible in non-unitary universe. We give an estimate of the capacity of retro-information channels in parallel. The result is significantly different from classical channel capacity.**

I. Introduction

The word *retro-information* denotes the hypothetical possibility to transfer information backward in time. How retro-information could be made possible is discussed in [2, 3] and is the extension of quantum information theory [1] over unitarity singularities. In this case the measure operators are not unitary. In short, physical evidence of non-unitarity could come from the following observations:

1. The unification of Quantum Theory with General Relativity poses problems to physicists and cosmologists.
2. A non-unifiable universe necessarily carries symmetry violations which imply unitarity exceptions.

In this paper we assume that retro-information is possible and we want to establish quantitative results on the capacity of several retro-information channels in parallel when they are submitted to a *forward coupling*: *i.e.* when the result of the transmission is made available to the transmitter via a reliable forward channel *before* the transmission occurs. To our knowledge this kind of configuration in communication theory is completely new and innovative.

II. Computation of channel capacities

We consider a $V \times M$ retro-information channel and denote by ψ the wave function associated to this channel. When i denotes a V-ary output symbol and j a M-ary setting symbol, we denote A_j^i the subset of quantum measurements A_i^j which provide output symbol j under setting i. We model the channel via its transfer operator $\mathbf{T}$, *i.e* the $V \times M$ matrix whose (i,j) coefficient is $\rho(A_j^i) = \int_{A_j^i} |\psi|^2$.

In unitary universes, for all j: the $\rho(A_j^i)$'s sum to one, and we have a classical information transfer probability operator. In the following we do not assume that the matrix $\mathbf{T}$ is unitary, *i.e.* $(1,\ldots,1)$ *may not* be a left eigenvector.

We now consider n i.i.d retro-information channels in parallel. The transfer operator associated to the n channels is $\mathbf{T}^{\otimes n}$. Let $Z_n = z_1 \ldots z_n$ be the M-ary codeword of the setting symbols of the channels and $Y_n = y_1 \ldots y_n$ the V-ary codeword of their output symbols. Denoting $A(Y_n, Z_n) = A_{z_1}^{y_1} \times \cdots \times A_{z_n}^{y_n}$ we have $\rho(A(Y_n, Z_n)) = \rho(A_{z_1}^{y_1}) \times \cdots \times \rho(A_{z_n}^{y_n})$.

Let $X_n = x_1 \ldots x_n$ be a V-ary codeword to be send via the channels. In absence of forward coupling, the setting Z_n is only a function of X_n: $Z_n = Z_n(X_n)$ and

$$P(Y_n|X_n) = \frac{\rho(A(Y_n, Z_n(X_n)))}{\sum_{Y_n'} \rho(A(Y_n', Z_n(X_n)))} \qquad (1)$$

In presence of Forward Coupling Function (FCF), Z_n is a function of both X_n and Y_n: $Z_n = Z_n(X_n, Y_n)$ and

$$P^F(Y_n|X_n) = \frac{\rho(A(Y_n, Z_n(X_n, Y_n)))}{\sum_{Y_n'} \rho(A(Y_n', Z_n(X_n, Y_n')))} \qquad (2)$$

Theorem 1 *There exists a set of FCF which rises the capacity of the n V-ary channels in parallel to nC^F where*

$$C^F = \min\{1, \log_V(\frac{\sum_i \max_j \rho(A_j^i)}{\sum_i \min_j \rho(A_j^i)}\} \qquad (3)$$

Remark: This new capacity is much greater than the classical capacity nC without FCF. Figure 1 shows both C and C^F in the binary symetric case where $\mathbf{T} = \begin{bmatrix} p & 1-p \\ 1-p & p \end{bmatrix}$ with $p > \frac{1}{2}$. In this case we have $C = 1 + p\log_2 p + (1-p)\log_2(1-p)$, while $C^F = \min\{1, \log_2 \frac{p}{1-p}\}$.

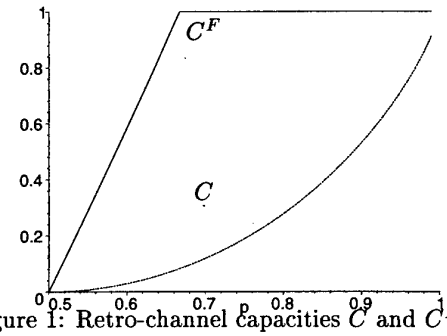


Figure 1: Retro-channel capacities C and C^F versus p.

III. Conclusion

We have presented a new information transfer configuration in information theory based on extrapolated physical assumptions. Retro-information *a priori* is a logical challenge (even when restricted to short space-time lap), however it can be framed in a consistent axiomatic which can take into account paradoxical effects due to forward coupling. The unexpected results about channel capacities contributes to make retro-information a very promising area of investigation.

References

[1] B. Schumacher, M.D. Westmoreland, "Sending classical information via noisy quantum channel," *Phys. Rev. A*, vol. 56, pp. 131-138, 1997.

[2] P. Jacquet and V. Joly, "Retro-information in Wheeler-Feynman universe model: application over an hypothetical concept in quantum mechanics," INRIA RR-3530, 1998.

[3] —, "Capacity of retro-information channels," INRIA RR-3836, 2000.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On the evaluation of the capacity of channels with memory

Jean Conan[1]
Department of ECE
Ecole Polytechnique de Montreal
P.O. Box 6079 station CENTRE
VILLE
Montreal,P.Q., Canada
e-mail: conan@comm.polymtl.ca

Abstract — **The determination of the capacity of a binary Finite State Channel with memory is in general a very difficult task. In this paper we present a new systematic method which amounts to computing the entropy of the channel error sequence represented as the output of a stochastic finite state automaton with state cardinality at most twice the one of the original channel. Each state of the original channel yields a maximum of two states in the automaton state transition diagram according to whether the preceeding error symbol was a one or a zero. The error class E is defined as the class of all states terminating on an error while the remaining class $\overline{E}$ contains states with transitions corresponding to no error. Consequently any path along states in E represents a solid burst of errors and reciprocally all the solid bursts of errors can only result from transitions between states in E and the same property applies to errorless events which can only result from transitions between states in $\overline{E}$. If the channel has K states, the final result is obtained by computing at most $2K$ series whose elements are the coefficients of the generating functions of the runs of $0's$ after an error terminating in any of the states of E and of the runs of $1's$ after an errorless event terminating in any of the states of $\overline{E}$.**

I. Summary

In this paper we address the problem of computing the capacity of a class of finite state binary transmisssion channels. Our basic model considers a finite state binary channel with inputs $\{x_n\}$ and outputs $\{y_n\}$ taking values on $\{0,1\}$ and such that

$$y_n = x_n \oplus z_n \cdot \tag{1}$$

where z_n is the error with values on $\{0,1\}$ assumed to be independent of the input. The generation of the error process $\{z_n\}$ depends on the current state $s_n \in \{0,1,...,K-1\}$ according to the law $\Pr\{\ z_n = 1|\ s_n = k\} = 1 - p_k$ and the state process is Markov according to a given transition probabilities matrix $Q = [\Pr\{\ s_n = j|\ s_{n-1} = i\}]\ i,j \in \{0,1,...,K-1\}$. Such a channel model might be adequate to represent a fading channel for which the error rate increases as the transmitted signal fades out. It constitutes a generalization of the classical Gilbert-Elliott channel which has $K = 2$ states. Results due to Gilbert [1] are known for this channel in the case where $p_0 = 1, p_1 \neq 1$ and more generally by using a different approach with non zero probability of error in both states [2]. In contrast, our proposed method of computation of the capacity is valid for any $K \geq 2$ and extends in a systematic way the original approach of Gilbert based on the analysis of bursts of consecutive zeros occuring after an error. It turns out however that in general statistics relating to the bursts of ones are also required. If the channel has K states, the final result is obtained by computing at most $2K$ series whose elements are the coefficients of the generating functions of the runs of $0's$ after an error terminating in any of the states of E and of the runs of $1's$ after an errorless event terminating in any of the states of $\overline{E}$. Similarly to the case of the well known Gilbert channel, an alternate more elegant sum of series which in general converge slower can be used based on the coefficients of other generating functions representing the probabilities of the runs of consecutive errors between errorless events starting in any state of $\overline{E}$ and the error free runs between errors starting from any state in E.

[1]This work was supported by NSERC Grant OGP0001701.

References

[1] E. N. Gilbert,"Capacity of a Burst-Noise Channel," The Bell System Technical Journal, pp. 1253-1265, Sept. 1960.

[2] M. Mushkin and I. Bar-David,"Capacity and Coding for the Gilbert-Elliott Channels," IEEE Trans. Inform. Theory, vol. 35, no. 6, pp. 1277-1290, Nov. 1989.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Fourier spectrum of optimal Boolean functions via Kasami's identities

Anne CANTEAUT* *INRIA, Domaine de Voluceau, ***LIFL,Université des Sciences
Claude CARLET** Rocquencourt, BP 105, 78153 et Technologies de Lille,
Pascale CHARPIN* Le Chesnay Cedex, FRANCE 59655 Villeneuve d'Ascq
Caroline FONTAINE*** **GREYC, Université de Caen, Cedex, FRANCE
14032 Caen Cedex, FRANCE

Abstract — **We introduce a new approach for the study of weight distributions of cosets of the Reed-Muller code of order 1. We next examine the impact of our results when some cryptographic criteria of Boolean functions are considered.**

Our main purpose is to study the nonlinearity, and other cryptographic criteria of Boolean functions throughout the properties of weight distributions of cosets of the Reed-Muller code of order 1 – denoted by $R(1,m)$. Indeed, it appears in recent papers that the knowledge of the whole Fourier-spectrum of a given function, and not only its maximal value, is of great interest from a theoretical point of view as well as for applications [1, 4]. We begin by giving a general result, based on the method introduced by Kasami in [5] by using Pless identities.

Theorem 1 *Let m be a positive integer, $m \geq 3$. Consider any binary linear code C of length $n = 2^m$, dimension $k = m+2$ and minimum distance δ. Let us denote by a_w (resp. b_w) the number of codewords of weight w in C (resp. $C^\perp$) and by $\mathcal{I}(\lambda)$ the number*

$$\mathcal{I}(\lambda) = \sum_{w=1}^{2^{m-1}-1} (w-2^{m-1})^2 \left((w-2^{m-1})^2 - \lambda^2\right) a_w.$$

Assume that C contains the all-one vector $\mathbf{1}$ and that $C^\perp$ is such that $b_1 = b_2 = b_3 = 0$. Then for any positive integer $\lambda \leq 2^{m-1}$, we have

$$\mathcal{I}(\lambda) = 2^m \left(3b_4 - 2^{m-2}\left((2^{m-1}-1)^2 + (\lambda^2 - 2^{m-1})\right)\right)$$

If $\delta \geq 2^{m-1} - \lambda$ then $\mathcal{I}(\lambda) \leq 0$ which can be expressed as

$$b_4 \leq \frac{1}{3}\, 2^{m-2}\left((2^{m-1}-1)^2 - 2^{m-1} + \lambda^2\right). \qquad (1)$$

Equality holds in (1) if and only if $\delta = 2^{m-1} - \lambda$ and if the weight distribution of C is: $a_0 = a_{2^m} = 1$ and

w	δ	2^{m-1}	$2^m - \delta$
a_w	$\frac{2^{2m-2}}{(\delta - 2^{m-1})^2}$	$2^{m+2} - \frac{2^{2m-1}}{(\delta-2^{m-1})^2} - 2$	$\frac{2^{2m-2}}{(\delta-2^{m-1})^2}$

Since $b_4 \neq 0$, the minimum distance of $C^\perp$ is exactly 4.

The codes $(x + R(1,m)) \cup R(1,m)$, where $x \notin R(1,m)$, satisfy the hypothesis of Theorem 1. A coset $x + R(1,m)$ is said to be *almost optimal* if its minimum weight is greater than or equal to w_0, where $w_0 = 2^{m-1} - 2^{(m-1)/2}$ for odd m, and $w_0 = 2^{m-1} - 2^{m/2}$ for even m. It is called *three-valued almost optimal* if it has three weights only, 2^{m-1} and $\pm w_0$ – its weight distribution is the one given in Theorem 1.

Corollary 1 *If $x + R(1,m)$ is almost optimal, then*
- *if m is odd, then $b_4 \leq \frac{1}{3}\, 2^{m-2}\,(2^{m-1}-1)^2$;*
- *if m is even, then $b_4 \leq \frac{1}{3}\left(2^{m-2}\,(2^{m-1}-1)^2 + 2^{2m-3}\right)$.*

In both cases, equality holds if and only if $x + R(1,m)$ is three-valued almost optimal.

Let f be any Boolean function with m variables. The *Fourier transform* of f is

$$\mathcal{F}(f) = \sum_{x \in \mathbf{F}_2^m} (-1)^{f(x)} = 2^m - 2wt(\Omega_f)\,.$$

The set $\{\pm\mathcal{F}(f+\varphi_\alpha) \mid \alpha \in \mathbb{F}_2^m\}$ is called the Fourier-spectrum of f, where φ_α denotes any linear function.

The *nonlinearity* of f is equal to $2^{m-1} - (\mathcal{L}(f)/2)$, where

$$\mathcal{L}(f) = \max_{\alpha \in \mathbf{F}_2^m} \mid \mathcal{F}(f+\varphi_\alpha) \mid.$$

Denote by Ω_f the codeword composed of the values $f(x)$, $x \in \mathbb{F}_2^m$. We will say that f is almost optimal (or three-valued almost optimal) when the coset $\Omega_f + R(1,m)$ satisfies this property. Let $D_a f$ be the derivative of f with direction a: $D_a f(x) = f(x) + f(a+x)$. The main indicator related to the *global avalanche criterion* is

$$\mathcal{V}(f) = \sum_{a \in \mathbf{F}_2^m} \mathcal{F}^2(D_a f).$$

We will examine the connections between the nonlinearity and the global avalanche criterion. We first show that if f is almost optimal then $\mathcal{V}(f) \leq 2^{2m+1}$ for odd m and $\mathcal{V}(f) \leq 2^{2m+2}$ for even m – with equality if and only if f is three-valued almost optimal.

We next study the restrictions of a Boolean function f to each coset of any linear subspace of $\mathbf{F}_2^m$. We notably establish a relation between the Fourier spectrum of f and the Fourier spectra of its restrictions. This leads us to obtain some characterizations of bent functions, of three-valued almost optimal functions and of almost optimal functions which have a linear structure. We give a full explanation of links between bent functions and three-valued almost optimal functions.

REFERENCES

[1] A. Canteaut, P. Charpin, H. Dobbertin, " Divisibility of cyclic codes and highly nonlinear functions on $\mathbf{F}_{2^m}$", *SIAM Journal of Discrete Mathematics*, 13(1):105–138, 2000..

[2] C. Carlet, "On cryptographic propagation criteria for Boolean functions", *Information and Computation*, (151):32–56, 1999.

[3] H. Dobbertin, "Construction of bent functions and balanced Boolean functions with high nonlinearity", *FSE'94*, LNCS 1008, Springer Verlag, pp. 61-74.

[4] E. Filiol, C. Fontaine, "Highly nonlinear balanced Boolean functions with a good correlation-immunity", *EUROCRYPT'98*, LNCS 1403. pp. 475–488. Springer-Verlag, 1998.

[5] T. Kasami, "Weight distributions of Bose-Chaudhuri-Hocquenghem Codes", in: R.C. Bose and T.A. Dowlings, eds, Combinatorial Math. and Applications, (Univ. of North Carolina Press, Chapel Hill, NC, 1969) Ch. 20.

[6] X. Zhang, Y. Zheng, "GAC – the criterion for Global Avalanche Characteristics of cryptographic functions", *Journal of Universal Computer Science*, vol.1, n. 5 (1995), 320-337.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

A Construction of Resilient Functions with High Nonlinearity

Thomas Johansson, Enes Pasalic
Dept. of Information Technology
Lund University
Box 118, S-22100 Lund, Sweden
e-mail: thomas,enes@it.lth.se

Abstract — **We propose a construction of resilient functions with n binary input variables and m binary output variables. In certain cases, the nonlinearity of these functions is the highest nonlinearity known.**

I. Introduction

An n-input m-output function, $F(x_1,\ldots,x_n)=(f_1,\ldots,f_m)$, is a set of m Boolean functions, $f_1,\ldots,f_m$, where each $f_i:\mathbb{F}_2^n\mapsto\mathbb{F}_2$. One of the many applications of these functions may be the realization of S-boxes in DES-like block ciphers. Different properties and criteria for such functions have been studied, see e.g. [3]. Here, we consider two criteria, namely nonlinearity and resiliency.

The previous work on nonlinear resilient functions is mostly based on the two constructions presented in [2] and [4]. As proved in [2], there is a tradeoff between the nonlinearity and resiliency when the two constructions are compared. The construction in [2] gives higher nonlinearity, while in [4] a larger resiliency could be obtained for the same n and m.

II. New Construction

The construction presented here is an extension of the design of nonlinear Boolean functions presented in [1]. It yields highly nonlinear resilient functions for any given input triple (n,m,t), where t is the order of resiliency. A well-known result states that a function $F(x_1,\ldots,x_n)=(f_1,\ldots,f_m)$ is an (n,m,t)-resilient function if and only if all nonzero linear combinations of $f_1,\ldots,f_m$ are $(n,1,t)$-resilient functions. Furthermore, the nonlinearity of $F(x)=(f_1(x),\ldots,f_m(x))$, denoted by N_F, is defined as the minimum nonlinearity of all nonzero linear combinations of the component functions of F.

Theorem 1 *Let n,m,t and d be four positive integers with $n\geq 4, 1\leq t\leq n-3, 1\leq d\leq n-t, m\leq n-d$ and $S_{n,m,t,d}=\{A_y^{(i)}\in\mathbb{F}_2^{n-d}, i=1,\ldots,m \mid wt(A_y^{(i)})\geq t+1, y\in\mathbb{F}_2^d\}$. For any $a\in S_{n,m,t,d}$, let $s_{a,c}^*=|\{y\in\mathbb{F}_2^d \mid \sum_{i=1}^m c_i A_y^{(i)}=a\}|$ and $s^*=\max_{c\in\mathbb{F}_2^m}\max_a s_{a,c}^*$. We now define a function $F:\mathbb{F}_2^n\mapsto\mathbb{F}_2^m$ by*

$$F(y,x)=(A_y^{(1)}x, A_y^{(2)}x,\ldots,A_y^{(m)}x),$$

where $y=(y_1,\ldots,y_d)\in\mathbb{F}_2^d, x=(x_1,\ldots,x_{n-d})\in\mathbb{F}_2^{n-d}$. Then the following holds:

1. *F is uniformly distributed if $\sum_{i=1}^m c_i A_y^{(i)}\neq 0$, for any $c\in\mathbb{F}_2^m, c\neq 0$.*
2. *F is t-resilient if for any $a\in\mathbb{F}_2^{n-d}\mid 0\leq wt(a)\leq t$ and $c\in\mathbb{F}_2^m$, $c\neq 0$, it holds that $\sum_{i=1}^m c_i A_y^{(i)}\neq a$.*
3. *$N_F=2^{n-1}-s^*2^{n-d-1}$.*

Note, that each component function $A_y^{(i)}x$ is a concatenation of 2^d distinct t-resilient linear functions on $\mathbb{F}_2^{n-d}$. Hence, it is convenient to introduce a $2^d\times m$ matrix A_y, having as each entry an $(n-d,1,t)$-resilient Boolean function defined uniquely by a vector $A_y^{(i,j)}\in\mathbb{F}_2^{n-d}$ s.t. $wt(A_y^{(i,j)})\geq t+1$. Due to the first two parts of Theorem 1 each row of A_y must span an $[n-d,m,t+1]$ linear code.

The parameter s^* is the number of repetitions of any vector $A_y^{(i,j)}$ in any nonzero linear combination of A_y's columns. It can be proved that the nonlinearity is maximized is $s^*=1$, which means that each vector may only appear once in any nonzero linear combination of A_y's columns.

According to the third part of Theorem 1 the nonlinearity is maximized when d is maximized, where d must satisfy a trivial upper bound $\binom{n-d}{t+1}+\binom{n-d}{t+2}+\cdots+\binom{n-d}{n-d}\geq 2^d$. We can show that given an $[n-d,m,t+1]$ linear code, we are able to fill 2^m-1 out of 2^d rows of A_y without violating the restrictions given by Theorem 1. Thus, given $\lceil 2^d/(2^m-1)\rceil$ nonintersecting $[n-d,m,t+1]$ linear codes the matrix A_y can be constructed.

The results presented here are obtained using computer search for nonintersecting linear codes. A comparison with the construction described in [2] is presented in Table 1 in the case of 2-resilient functions. Such a favorable comparison can be extended to any order of resiliency if the number of input variables n is not too large, say for $n<25$.

N_F	$n=9$		$n=10$		$n=11$		$n=12$	
m	Our	[2]	Our	[2]	Our	[2]	Our	[2]
2	240	192	480	384	992	896	1984	1792
3	192	-	448	-	960	-	1984	1792
4	128	-	384	-	896	-	1920	-
5	0	-	256	-	768	-	1792	-
6	0	-	0	-	512	-	1536	-

Table 1: Comparison on N_F of 2-resilient functions

[1]This work was supported in part by Swedish Research Council for Engineering Sciences under Grant 97-130

References

[1] S. Chee, S. Lee, D. Lee, S. H. Sung, "On the correlation immune functions and their nonlinearity", *Advances in Cryptology - ASIACRYPT '96, Lecture Notes in Computer Science*, 1163, pp. 232–243, Springer-Verlag, 1996.

[2] K. Kurosawa, T. Satoh and K. Yamamoto "Highly Nonlinear t-Resilient Functions". *Journal of Universal Computer Science*, vol. 3, no. 6, pp. 721–729, Springer Pub. Co., 1997.

[3] K. Nyberg, "On the construction of highly nonlinear permutations", *Advances in Cryptology - EUROCRYPT'92, Lecture Notes in Computer Science*, 658, pp. 92–98, Springer-Verlag, 1993.

[4] X. M. Zhang and Y. Zheng, "On nonlinear resilient functions", *Advances in Cryptology - EUROCRYPT'95, Lecture Notes in Computer Science*, 921, pp. 274–288, Springer-Verlag, 1995.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On the Structure and Numbers of Higher Order Correlation-Immune Functions

Yuriy Tarannikov
Mech. & Math. Department
Moscow State University
119899 Moscow, Russia
e-mails: yutaran@nw.math.msu.su,
taran@vertex.inria.msu.ru

Abstract — **It is proved by means of Ramsey-like technique that for each positive integer k there exists a minimal nonnegative integer $p'(k)$ that any $n-k$ th order correlation-immune function of n binary input variables, $f \not\equiv$ const , depends nonlinearly on at most $p'(k)$ inputs. It is proved that the number of $n-k$ th order correlation-immune functions of n binary input variables, $k =$ const , $n \to \infty$, is polynomial. For $k = 1, 2, 3$ the exact formulas for the numbers of such functions are obtained.**

We consider memoryless Boolean functions f: $GF(2)^n \to GF(2)$, $\widetilde{x} \to f(\widetilde{x})$. The number of '1's in the table of the Boolean function f is given by its Hamming weight W_f. A memoryless function f is said to be correlation-immune of order m, with $1 \le m \le n$, if the output of f and any m input variables are statistically independent. This concept was introduced by Siegenthaler [3]. In an equivalent non-probabilistic formulation (see [4]) the Boolean function f is called correlation-immune of order m if $W_{f_1} = W_{f_2}$ for any two its $(n-m)$-inputs subfunctions f_1 and f_2.

In [1] it was pointed out that correlation-immune function is a particular case of an orthogonal array (OA), namely, mth order correlation-immune function of n inputs with weigth W_f corresponds to simple $(W_f, n, 2, m)$-OA. Note that for maximal m such that a function is correlation-immune of order m the value $m+1$ was called a dual distance of a code (a code is a characteristic set of the function) by Delsarte [2] and declared as one of "four fundamental parameters of a code". Of course, Delsarte did not use the words "correlation-immune".

In this work we consider $(n-k)$th order correlation-immune functions of n inputs in the case $k =$ const , $n \to \infty$, i. e. higher order correlation-immune functions. Further, $(n-k)$th order correlation-immune functions of n inputs are called k-functions. Also we assume that if $n \le k$ then any Boolean function of n inputs is k-function.

The polynomial representation of f is called an algebraic normal form (ANF) of the function. The degree of f, denoted by $\deg(f)$, is defined as the number of variables in the longest term in ANF of f. The terms of length 1 are called linear terms. We say that the Boolean function $f(x_1, x_2, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_n)$ depends on the input x_i linearly if the variable x_i presents in the ANF of function f only as a linear term x_i. In all another cases we say that the function $f(x_1, x_2, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_n)$ depends on the input x_i nonlinearly (including the case then the input x_i is fictitious for the function $f(x_1, x_2, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_n)$).

Theorem 1. *For each positive integer k there exists a minimal nonnegative integer $p'(k)$ that any k-function f, $f \not\equiv$ const , depends nonlinearly on at most $p'(k)$ inputs.*

A Boolean function f is called balanced if $W_f = W_{\overline{f}}$.

We say that k-function $f(x_1, x_2, \ldots, x_m)$ is a reproductive k-function if the function $g(x_1, x_2, \ldots, x_m, y) = f(x_1, x_2, \ldots, x_m) \oplus y$ is k-function.

Remark. *k-function $f(x_1, x_2, \ldots, x_m)$ is a reproductive k-function iff it is true at least one of two following conditions: a) $m < k$; b) the function f is balanced.*

Corollary from Theorem 1. *For each positive integer k there exists a minimal nonnegative integer $p(k)$ that any reproductive k-function f depends nonlinearly on at most $p(k)$ inputs.*

It is obviously that $p(k) \le p'(k)$. Below we show that $p(k) \ne p'(k)$ at least for $k = 2, 3$.

Theorem 2. *For $n > p'(k)$ the number $N(n, n-k)$ of $(n-k)$th order correlation-immune functions of n inputs is expressed by the following formula.*

$$N(n, n-k) = \sum_{i=0}^{p(k)} A(k,i) \binom{n}{i} + 2,$$

where $A(k,i)$ is the number of i-inputs reproductive k-functions that depend on all inputs $x_1, x_2, \ldots, x_i$ nonlinearly.

Corollary from Theorem 2. *The asymptotics of the number $N(n, n-k)$ of $n-k$ th order correlation-immune functions of n inputs is expressed by the following formula, $k =$ const , $n \to \infty$.*

$$N(n, n-k) \sim \frac{A(k, p(k))}{p(k)!} n^{p(k)}.$$

Theorem 3. $p(1) = p'(1) = 0$, $p(2) = 1$, $p'(2) = 3$, $p(3) = 4$, $p'(3) = 6$;

$$\begin{aligned} &N(n, n-1) = 4 && \text{for } n > 0, \\ &N(n, n-2) = 2n + 4 && \text{for } n > 3, \\ &N(n, n-3) = n^4 - (2/3)n^3 + (5/3)n + 4 && \text{for } n > 6. \end{aligned}$$

Theorem 4. $p(k) \ge 3 \cdot 2^{k-2} - 2$.

References

[1] P. Camion, C. Carlet, P. Charpin, N. Sendrier, "On correlation-immune functions," *Advances in Cryptology: Crypto '91, Proceedings, Lecture Notes on Computer Science*, vol. 576, pp. 86–100, 1991.

[2] Ph. Delsarte, "Four fundamental parameters of a code and their combinatorial significance," *Information and Control*, vol. 23, no. 5, pp. 407–438, 1973.

[3] T. Siegenthaler, "Correlation-immunity of nonlinear combining functions for cryptographic applications," *IEEE Transactions on Information theory*, vol. IT-30, No 5, pp. 776–780, 1984.

[4] G. Z. Xiao, "Correlation-immunity of Boolean functions," *Electron. Lett.*, vol. 23, no. 25, pp. 1335–1336, 1987.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Large Weight Patterns Decoding in GOPPA codes and Application to Cryptography

Pierre Loidreau
Project CODES, INRIA
Rocquencourt
Domaine de Voluceau, B.P. 105
78 153 Le Chesnay CEDEX, France
e-mail: Pierre.Loidreau@inria.fr

Abstract — **By using the action of the FROBENIUS group it is possible to decode far beyond the error-correcting capability of GOPPA codes provided the error-vector has a definite structure. In particular cases the generation of these patterns can be easily described and gives a number of decodable patterns numerous enough to avoid enumeration. We show that it is possible to use this property to strengthen the MCELIECE-type cryptosystems against attacks based on random decoding.**

I. INTRODUCTION

We present a method to decode error-patterns of large weight in GOPPA codes by using a subgroup of the automorphism group of the GOPPA codes. Namely, we use the group generated by the FROBENIUS automorphism. By its action on the large weight error-patterns one obtains error-patterns of weight less than the error-correcting capability of the code.

The efficiency of this method and the number of decodable patterns depend on the nature of the FROBENIUS group. In a well chosen case we show that it is possible to decode a large number of patterns with weight one and a half larger than the error-correcting capability of the code. These patterns being easily generated, they can be used to improve the work factor of the random decoding attack on the MCELIECE public-key cryptosystem without increasing the size of the public-key.

II. AUTOMORPHISM GROUP OF GOPPA CODES

GOPPA codes are a subfamily of alternant codes generated by a polynomial g of degree t over a finite field $\mathrm{GF}(2^m)$. The set $L = (\alpha_1, \ldots, \alpha_n)$ of elements in L that are not roots of g is denoted generating vector. The GOPPA code $\Gamma(L, g)$ of length $n = |L|$ is the set of binary words $a = (a_{\alpha_1}, \ldots, a_{\alpha_n})$ such that

$$\mathrm{H}.{}^t a = 0$$

where $\mathrm{H} = \left(\alpha_j^i / g(\alpha_j)\right)_{i=0,j=1}^{t-1,n}$.

Generally, the automorphism group of a GOPPA code is trivial. However, we showed that when the generating polynomial g has coefficients over a subfield $\mathrm{GF}(2^s)$ of $\mathrm{GF}(2^m)$, the automorphism group contains the group generated by the FROBENIUS automorphism σ of $\mathrm{GF}(2^m)/\mathrm{GF}(2^s)$. [2]

III. TOWER DECODABLE PATTERNS

Suppose one receives the word

$$c = m + e$$

where m is a word in $\Gamma(L, g)$, g is taken over $\mathrm{GF}(2^s)$ and e is an error-vector. If the weight of e is less than the error-correcting capability t of the code then one recovers m easily. Since the automorphism group of the code contains the group generated by the FROBENIUS automorphism σ of $\mathrm{GF}(2^m)/\mathrm{GF}(2^s)$, any linear combination $\sum_{i=0}^{m/s-1} \epsilon_i^{(u)} \sigma^i(m)$ of the transformed of m through the FROBENIUS is in $\Gamma(L, g)$. The transform of the error pattern e becomes $\sum_{i=0}^{m/s-1} \epsilon_i^{(u)} \sigma^i(e)$ and we say that

Definition 1 *e is tower decodable in $\Gamma(L, g)$ if*

1. *There exists linear combinations indexed by u*

$$\mathcal{E}^{(u)} = \sum_{i=0}^{m/s-1} \epsilon_i^{(u)} \sigma^i(e)$$

of the $\sigma^i(e)$ such that the $\mathcal{E}^{(u)}$ can be decoded in the GOPPA code $\Gamma(L, g)$,

2. *the knowledge of some of the $\mathcal{E}^{(u)}$ enables the receiver to recover the error-pattern e with a certain probability.*

IV. APPLICATION TO MCELIECE CRYPTOSYSTEM

We take the MCELIECE parameters [3] that is, the private key is a generating matrix of a GOPPA code $\Gamma(L, g)$ where L is an indexation of $\mathrm{GF}(2^{10})$ and g is irreducible over $\mathrm{GF}(2^{10})$ of degree 50. The error-correcting capability of the code is 50. The public key is the scrambled private key. The best known work factor for the attack by random decoding is 2^{64} [1].

In our scheme we take g over $\mathrm{GF}(2^2) \subset \mathrm{GF}(2^{10})$. Hence, the Frobenius group has cardinality 5. The public-key is the scrambled private key reordered according to the orbits of the Frobenius group. By randomly chosing a number of 25 orbits out of 204 and placing randomly 3 bits on every chosen orbit we construct tower decodable patterns of weight 75. The number of such patterns is 2^{188}. For the decoding, we need to decode at most two words. The size of the public-key is the same as in the original scheme whereas the work factor of the attack by random decoding becomes 2^{90}.

REFERENCES

[1] A. CANTEAUT and F. CHABAUD. A new algorithm for finding minimum-weight words in a linear code: Application to McEliece's cryptosystem and to narrow-sense bch codes of length 511. *IEEE Transactions Information Theory*, 44(1):367–378, January 1998.

[2] P. LOIDREAU. Codes derived from binary GOPPA codes. *Sixth* International workshop on Algebraic and Combinatorial Coding Theory, sept. 1998, Pskov, Russia

[3] R. J. MCELIECE. A public-key cryptosystem based on algebraic coding theory. Technical report, Jet Propulsion Lab. DSN Progress Report, 1978.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

An Error Performance Analysis of Iterative Threshold Decoding

Christian Cardinal[1], David Haccoun[1] and François Gagnon[2]

[1]Department of electrical and computer engeneering
Ecole Polytechnique de Montréal
P.O. Box 6079 Station Centre Ville
Montreal, QC, Canada,
H3C 3A7

[2]Department of electrical engeneering
Ecole de Technologie Supérieure
1100, Notre-Dame W.
Montreal, QC, Canada,
H3C 1K3

Abstract- *A method for analyzing the error performance of the iterative threshold decoder using strict sense multi-orthogonal convolutional codes where the multiplicity order is larger or equal to the number of iterations is presented. This allows a tractable analysis, since all random variables are considered independent at each decoding step. The analysis provides a good prediction of the error probability convergence value of the iterative decoding process using strict sense doubly orthogonal convolutional codes.*

I. Introduction

A novel iterative threshold decoding procedure without interleaving has been introduced in [1]. This technique uses Convolutional Self Doubly Orthogonal Codes, CSO^{2}C. With these codes, the need for interleaving to obtain independent observables at each iteration is alleviated and hence the procedure does not require an interleaver, neither at the encoding nor at the decoding process. The double orthogonality property of the code may be defined either in the wide sense (CSO^{2}C-WS) or in the strict sense (CSO^{2}C-SS) [2]. The rate ½ codes CSO^{2}C-WS allow some repetitions of observables which produce correlated inputs at the second iteration. For the rate ½ code CSO^{2}C-SS, all repetitions of observables are avoided by using a parallel structure of the encoder. The definition of CSO^{2}C-SS may also be extended to multiple orthogonality of order M where no repetition is possible over M consecutive iterations. Such codes are called Strict-Sense Convolutional Self Multi-Orthogonal Codes, CSO^{M}C-SS.

In this paper, we present a method for analyzing the error performance of the iterative threshold decoder using CSO^{M}C-SS where M is larger than or equal to the number of iterations.

II. Bit Error Performance for Single Decoding Iteration

A threshold decoder produces at its output an approximated *Maximum A Posteriori* (MAP) value, $\lambda(i)$, for each information symbol u_i to be decoded at time i. This MAP value corresponds to a summation of J parity-check equations $\psi_j(i)$, at time i, over the currently received information symbol $y_u(i)$, that is :

$$\lambda(i) = y_u(i) + \sum_{j=1}^{J} \psi_j(i) \qquad (1)$$

The parity-check equations $\psi_j(i)$ are obtained using add-min operators as defined in [1]. This operator represents an approximation of the log-likelihood ratio (LLR) of the modulo-2 sum of binary random variables. Since CSOC is used, $\lambda(i)$ is a sum of independent random variables (RV) and the Probability Density Function (PDF) of $\lambda(i)$ is the convolution of the PDFs of each RV which belongs to the sum given by (1). Even though the RVs are not identically distributed, they are somewhat similar and hence their sum tends to be gaussian. The average value $\bar{\lambda}$ of $\lambda(i)$ is obtained as a sum of the means of all RVs. Similarly, its variance σ_λ^2 may also be expressed as a sum of the variances of all RVs $y_u(i)$ and $\psi_j(i)$. Therefore, the bit error probability, $P_b(E)$, may be approximated by :

$$P_b(E) \cong \frac{1}{\sqrt{2\pi\sigma_\lambda^2}} \int_{-\infty}^{0} \exp\left[-\left(\lambda-\bar{\lambda}\right)^2 / 2\sigma_\lambda^2\right] d\lambda = Q\left(\bar{\lambda}/\sigma_\lambda^2\right) \qquad (2)$$

In order to evaluate (2), we have determined the PDF of the RV $\psi_j(i)$ where all its N constituant RVs are gaussian distributed with mean m_l and variance σ_l^2, l= 1, 2, ..., N. Using (2) and considering a feedback threshold decoder, we have calculated $P_b(E)$ for different CSOC. Comparisons between theoretical and simulation results show only a small discrepancy, thus confirming the validity of the approach.

III. Extention to Iterative Threshold Decoding Without Interleaving

The above analysis is extended to obtain $P_b(E)$ for multiple iterations where the code used is CSO^{M}C-SS. Hence, all RVs are considered independent at each decoding step. The main idea behind this approach is to apply recursively the method developed in Section II. We consider, for the current iteration m, that inputs provided by the previous iteration (m-1) are gaussian distributed with mean $\bar{\lambda}^{(m-1)}$ and variance $\sigma_\lambda^2(m-1)$. Simulation results for rate ½ CSO^{2}C-SS codes having J parity-check equations coincide with those predicted using the theoretical analysis where rate ½ CSO^{M}C-SS codes with a value of J are used. In addition to validating the analyzing this also shows that only double orthogonality is in effect needed in order to obtain good error performance. The results also indicate that CSO^{M}C-SS codes converge more quickly than CSO^{2}C-SS codes.

IV. Conclusion

We have presented a method for evaluating the bit error probability of iterative threshold decoding using CSO^{M}C-SS. This method is based on the evaluation of the probability density function of the approximated MAP value obtained at the output of the threshold decoder. The multiple orthogonality is shown to be useful in the analysis of the performance of CSO^{2}C-SS codes. Furthermore, the results indicate that doubly orthogonal CSO^{2}C-SS codes may be sufficient to obtain a good error performance.

References

[1] Cardinal C., Haccoun D., Gagnon F., Batani N., (1999), "Turbo Decoding Using Convolutional Self Doubly Orthogonal Codes", ICC'99, Vancouver, BC, pp. 113-117.

[2] Gagnon, F., Haccoun, D., "Convolutional Codes with Extended Self-Orthogonality and New Low-Density Parity-Check Block Codes". Submitted to IEEE Transaction on Information Theory, june 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Bandwidth Efficient Hybrid ARQ Schemes Using Turbo Codes

Adrish Banerjee[1]
Department of EE,
University of Notre Dame,
Notre Dame, IN, U.S.A.
e-mail: Banerjee.5@nd.edu

Daniel J. Costello Jr.
Department of EE,
University of Notre Dame,
Notre Dame, IN, U.S.A.
e-mail: Costello.2@nd.edu

Thomas E. Fuja
Department of EE,
University of Notre Dame,
Notre Dame,IN, U.S.A.
e-mail: Fuja.1@nd.edu

Abstract — **New bandwidth efficient Type-I and Type-II hybrid-ARQ (HARQ) schemes using Turbo Trellis Coded Modulation (TTCM) are proposed. These schemes combine the power-efficiency of turbo codes with the bandwidth efficiency of Trellis Coded Modulation (TCM) to give efficient FEC/ARQ system designs.**

I. Introduction

When data is transmitted in the form of packets, it is common to use Automatic Repeat reQuest (ARQ) or retransmission techniques in addition to Forward Error Correction (FEC) to improve the performance of a communication system. Several schemes have been suggested in which code combining retransmission schemes using low rate turbo codes have been shown to yield good performance [1]. Separately, sequence combining TCM schemes have been proposed for systems requiring higher throughputs [2]. In this paper, we present several TTCM schemes for use in ARQ systems, thereby combining the advantages of TCM with those of Turbo codes in a retransmission environment.

II. System Description

We assume a selective repeat ARQ scheme with suitably large buffers at the transmitter and receiver. Furthermore, we assume an error free feedback channel over which positive (ACK) or negative (NACK) acknowledgements can be sent. The underlying TTCM scheme used here is the one proposed by Berrou et. al [3]. A coherent receiver model is assumed. The data sequence consists of information bits and a 16-bit CRC sequence. The sequence is fed into the Turbo encoder whose output is punctured to the desired rate and formatted into P-symbol data packets, $U = (u_1, \cdots u_P)$, where each symbol u_i consists of m bits (i.e., a signal constellation size of 2^m).

The following HARQ schemes using TTCM are considered. In *Scheme 1*, the same packet is retransmitted until the receiver accepts it as error free or until a preset maximum allowed number of retransmission attempts is reached. The error prone packets in the previous transmissions are discarded. In *Scheme 2*, also known as an average diversity combining scheme, copies of a retransmitted packet are combined into a single packet of the same blocksize by averaging the soft demodulated values of each packet and then decoding. *Scheme 3* is an incremental redundancy scheme where received packets are concatenated to form noise-corrupted codewords from increasingly longer and lower rate codes. During the first transmission only the information bits are sent. Subsequently, the check digits are incrementally transmitted to adaptively meet the error performance requirements of the system. Finally, we assume the blocksize is the same for all transmissions in order to keep network overhead to a minimum.

[1]This work was supported by Motorola Inc., NASA grant NAG 5-8355, NSF grant NCR95-22939, and NSF grant CCR-9996222.

III. Numerical Results

Scheme 1 and *Scheme 2* employing TTCM use a rate 2/3 Turbo code obtained by puncturing parity bits from a 4-state $(7,5)_{octal}$ constituent recursive convolutional encoder along with Gray mapping to a 8PSK signal constellation. The turbo decoder uses the APP algorithm. After every iteration, the CRC is checked. *Scheme 3* employing TTCM uses a mother turbo code of rate 1/3 mapped to an 8PSK constellation and higher rates are achieved by puncturing. *Scheme 1* employing TCM uses a rate 2/3 convolutional encoder obtained by puncturing a rate 1/2 16-state $(23,35)_{octal}$ convolutional encoder. The throughputs are plotted in Fig.1 for an information blocksize of 512 on an AWGN channel.

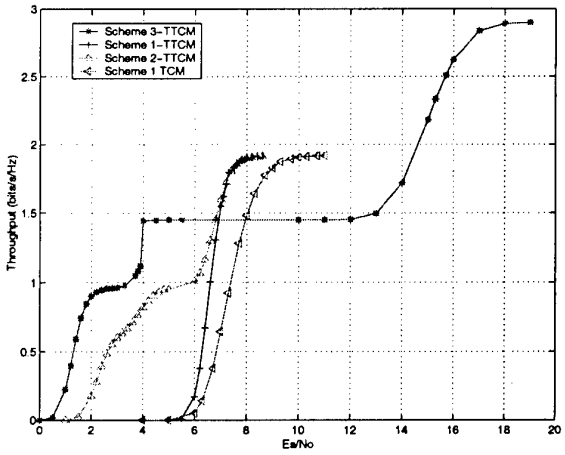


Fig. 1: Throughput comparison of various schemes

IV. Conclusions

In this paper, a new application of turbo codes to bandwidth efficient ARQ schemes is introduced. Since the combining schemes described here use a single decoder to decode any received packet or any combination of received packets, the implementation of these protocols requires only minor modifications to the transmitting and receiving systems of a standard turbo code.

References

[1] K. Narayanan and G. Stuber, "Turbo decoding for packet data systems," *Communication Theory Mini-Conference, GLOBECOMM 97*, pp 44-48, 1997.

[2] R. H. Deng, "Hybrid ARQ schemes employing coded modulation and sequence combining," *IEEE Transactions on Communications* , vol. 42, pp. 2239-2245, 1994.

[3] S.L. Goff, A. Glavieux, and C. Berrou, "Turbo-codes and high spectral efficiency modulation," *ICC 94* , pp. 645-649, 1994.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Convergence of Relative Frequency of Occurrence of Error Bursts on Channels with Memory

Mitsuru HAMADA[1]

Abstract — **The exponential convergence of the relative burst weight $W_b(Z_1 \dots Z_n)/n$, i.e., the relative frequency of occurrence of bursts is established for a broad class of functionals $\{Z_i\}$ of finite Markov chains.**

I. Introduction

Motivated by the intention to evaluate asymptotically multiple-burst-error-correcting codes on channels with memory, the exponential convergence of the relative burst weight $W_b(Z_1 \dots Z_n)/n$ is established for a broad class of functionals $\{Z_i\}$ of finite Markov chains (MCs). Here, b is a fixed but arbitrary positive integer, and $W_b(Z_1 \dots Z_n)$ denotes the number of error bursts of length $\le b$ that appear in $Z_1 \dots Z_n$, which is to be viewed as the additive noise sequence of a channel.

The standard notation we employ includes $\mathbb{N} = \{1, 2, \dots\}$, $\mathcal{A}^*$ which denotes the set of all finite-length sequences of symbols from $\mathcal{A}$, and $x_m^n = x_m \dots x_n$.

We treat a stochastic process $\{Z_i\}_{i\in\mathbb{N}}$ such that $Z_i = f(U_i)$, $i \in \mathbb{N}$, for some homogeneous MC $\{U_i\}_{i\in\mathbb{N}}$ and some function $f : \mathcal{U} \to \mathcal{Z} = f(\mathcal{U})$, where $\mathcal{U}$ is finite, $|\mathcal{Z}| > 1$, and $\mathcal{Z}$ contains the symbol 0. We adopt the definitions of primary notions (such as burst weight and swept coverings) in [1, Section 2].

II. Results and Derivation

We parse the observed sequence $Z_1 Z_2 \dots$ into phrases

$$Z_1^{\tau_1}, Z_{\tau_1+1}^{\tau_2}, \dots,$$

$\tau_1 < \tau_2 < \dots \in \mathbb{N}$, so that $Z_1^{\tau_1}, Z_{\tau_1+1}^{\tau_2}, \dots$ belong to

$$\mathcal{W} = \{0\} \cup (\mathcal{Z} \setminus \{0\})\mathcal{Z}^{b-1},$$

where $(\mathcal{Z} \setminus \{0\})\mathcal{Z}^{b-1} \subset \mathcal{Z}^*$ denotes the set of $(|\mathcal{Z}| - 1)|\mathcal{Z}|^{b-1}$ phrases of length b whose leading symbols are not zero. Then, by Corollary 1 of Hamada [1, Section 2], the number of appearances of phrases belonging to $(\mathcal{Z} \setminus \{0\})\mathcal{Z}^{b-1}$ in the parsed sequence up to time n is the burst weight $W_b(Z_1^n)$, where we ignore the possible existence of the incomplete phrase in the last position, which may cause a negligible disagreement with the true burst weight. The point is that the above parsing substitutes for Procedure 1 of Hamada [1, Section 2] for the purpose of obtaining the swept covering for $\{i \in \{1, \dots, n\} : Z_i \neq 0\}$ whose size is $W_b(Z_1^n)$.

Let $\boldsymbol{l}(n)$ denote the number of all phrases produced up to time n in the parsing of $Z_1 Z_2 \dots$; let $\mathsf{Q}_n(w)$ denote the number of occurrences of phrase w up to time n divided by $\boldsymbol{l}(n)$, $n \ge b$. Then, $W_b(Z_1^n) \simeq \boldsymbol{l}(n)\{1 - \mathsf{Q}_n(0)\}$ and $n \simeq \boldsymbol{l}(n)\{\mathsf{Q}_n(0) + b(1 - \mathsf{Q}_n(0))\}$. Therefore, approximately,

$$W_b(Z_1^n)/n \simeq \widehat{W}_n \stackrel{\text{def}}{=} \frac{1 - \mathsf{Q}_n(0)}{\mathsf{Q}_n(0) + b(1 - \mathsf{Q}_n(0))}. \qquad (1)$$

This indicates a one-to-one correspondence between (the approximation of) $W_b(Z_1^n)/n$ and $\mathsf{Q}_n(0)$, and hence, the behavior of $W_b(Z_1^n)/n$ hinges on that of $\mathsf{Q}_n(0)$.

Now consider the dissection or parsing of the underlying MC $U_1 U_2 \dots$ corresponding to that of $Z_1 Z_2 \dots$:

$$V_1 = U_1^{\tau_1}, V_2 = U_{\tau_1+1}^{\tau_2}, \dots,$$

where $\tau_1 < \tau_2 < \dots$ are the time instances at which the partitions of $Z_1 Z_2 \dots$ occur. Clearly, $V_1, V_2, \dots$ all belong to

$$\mathcal{V} \stackrel{\text{def}}{=} f^{-1}(0) \cup (\mathcal{U} \setminus f^{-1}(0))\mathcal{U}^{b-1},$$

where $(\mathcal{U} \setminus f^{-1}(0))\mathcal{U}^{b-1} \subset \mathcal{U}^*$ is the set of all phrases of length b whose leading symbols do not belong to $f^{-1}(0)$. Then,

$$\mathsf{Q}_n(0) = \sum_{v \in f^{-1}(0)} \mathsf{P}_n(v), \qquad (2)$$

where the relative frequencies $\mathsf{P}_n(v)$ of $v \in \mathcal{V}$ are defined similarly to $\mathsf{Q}_n(w)$, $w \in \mathcal{W}$. Note that $\{V_k\}_{k\in\mathbb{N}}$ is a MC whose transition probabilities are

$$P(v'|v) = P(v'|\underline{v}), \quad v, v' \in \mathcal{V}, \qquad (3)$$

where $\underline{v}$ denotes the last symbol of v, and $P(x_2 x_3 \dots x_n|x_1) = \prod_{i=1}^{n-1} P(x_{i+1}|x_i)$ is determined by transition probabilities $P(u'|u)$, $u, u' \in \mathcal{U}$, of the underlying MC $\{U_i\}_{i\in\mathbb{N}}$ for any $x_1^n \in \mathcal{U}^n$, $n \in \mathbb{N}$, $n \ge 2$. Thus, from (1), (2), and the strong law of large numbers for MCs, we have

Theorem 1 *If the phrase-to-phrase MC $\{V_k\}$ is irreducible, and Π is the stationary distribution of $\{V_k\}$, then*

$$\frac{W_b(Z_1^n)}{n} \to \xi(y) \stackrel{\text{def}}{=} \frac{1 - y}{y + b(1 - y)} \quad (n \to \infty) \quad \textit{almost surely,}$$

where $y = \sum_{v \in f^{-1}(0)} \Pi(v)$.

This result can be strengthened by the method of types:

Theorem 2 *Let $J \subset [0, 1/b]$ be an interval whose end points are distinct. If $\{V_k\}$ is irreducible, then*

$$\lim_{n\to\infty} n^{-1} \log \Pr\{W_b(Z_1^n)/n \in J\} = -\inf_{\Phi\in\Gamma} D(\Phi||P)/L(\Phi),$$

where $\Gamma = \left\{\Phi : \xi\left(\sum_{v\in f^{-1}(0)} \bar{\Phi}(v)\right) \in J, \bar{\Phi} = \bar{\bar{\Phi}}\right\}$, $\bar{\Phi}$ and $\bar{\bar{\Phi}}$ denote the two marginals of a probability distribution Φ on $\mathcal{V} \times \mathcal{V}$ as in [2, p. 790], the usage of D in [2, Eq. (12)] is also adopted, P is given in (3), and $L(\Phi) = \sum_{v\in\mathcal{V}} \bar{\Phi}(v) \times$ (length of v).

References

[1] M. Hamada, "Almost sure convergence of relative frequency of occurrence of burst errors on channels with memory," *IEICE Trans. Fundamentals*, vol. E82-A, no. 10, pp. 2022–2033, Oct. 1999. Available, for the time being, at `http://search.ieice.or.jp/1999/pdf/e82-a_10_2022.pdf`.

[2] I. Csiszár, T. M. Cover, and B.-S. Choi, "Conditional limit theorems under Markov conditioning," *IEEE Trans. Information Theory*, vol. IT-33, no. 6, pp. 788–801, Nov. 1987.

[1] Dept. of Information and Communication Engineering, University of Electro-Communications, Chofu-shi, Tokyo 182-8585, Japan. E-mail: `hamada@w-one.cas.uec.ac.jp`. This work was supported by a JSPS Research Fellowship for Young Scientists.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Some low constant weight code designs for the parallel asynchronous communication scheme*

Luca G. Tallini
Dipartimento Di. Tec., Politecnico di Milano,
20133 Milano, ITALY. E-mail: luca.tallini@polimi.it

Bella Bose
Department of Computer Science, Oregon State University,
Corvallis, OR 97331. E-mail: bose@cs.orst.edu

Abstract — **In a constant weight w code of length n, each code word has w 1's and $n-w$ 0's. If the ratio w/n is low, the code is referred to as a low constant weight (LCW) code. In this paper, some simple designs of LCW codes are presented. Further, the speed performance of these codes is derived and then it is shown that these codes have much better performance than the dual-rail codes, when used in asynchronous buses.**

Index terms: low weight codes, constant weight codes, unordered codes, proximity detecting codes, asynchronous communication systems, low power systems.

In [2], it has been shown that the lower the weight of the codes the faster is the implementation of an asynchronous bus. Hence, low weight codes find a direct application in the design of parallel asynchronous communication systems. Low weight codes also find application in the design of low power VLSI systems [3].

This paper presents some low constant weight codes which are very efficient in terms of speed if used in realizing an asynchronous communication system. They are also efficient in terms of complexity and redundancy. First their construction will be sketched and then their speed performance will be quantified. Let $\mathcal{S}_w^k$ indicate the set of all words of length k and weight w and DC(n,k,w) indicate a binary block code of length n, constant weight w and k information bits.

DC$(n=4,k=2,w=1)$ code design. This design is defined by the following encoding function, $\mathcal{E}:\mathbb{Z}_2^2 \rightarrow \mathcal{S}_1^4$, for the code: $\mathcal{E}(00)=0001$, $\mathcal{E}(01)=0010$, $\mathcal{E}(10)=0100$, $\mathcal{E}(11)=1000$. Note that both encoding and decoding functions can be realized with extremely simple logic. Note also that concatenating this code with itself it is possible to obtain very simple DC$(n=2k,k,w=0.5k)$ codes which require the same number of redundant bits as the usual dual-rail code, but the number of 1's in each code word is only half that of a dual-rail code word.

DC$(n=7,k=4,w=2)$ code design. This design is defined by the following encoding function $\mathcal{E}:\mathbb{Z}_2^4 \rightarrow \mathcal{S}_2^7$ for the code which is defined in terms of boolean logic (given $x,y \in \mathbb{Z}_2$, let $x{\cdot}y$ indicate the logical AND between x and y, $x \vee y$ the logical OR between x and y, and $\overline{x}$ the logical NOT of x): $\mathcal{E}(x_1x_2x_3x_4)=(x_1{\cdot}x_2, x_1{\cdot}\overline{x_2}, \overline{x_1}{\cdot}x_2, x_3{\cdot}x_4 \vee \overline{x_1}{\cdot}\overline{x_2}{\cdot}x_3, x_3{\cdot}\overline{x_4} \vee \overline{x_1}{\cdot}\overline{x_2}{\cdot}\overline{x_4}, \overline{x_3}{\cdot}x_4 \vee \overline{x_1}{\cdot}\overline{x_2}{\cdot}x_4, \overline{x_3}{\cdot}\overline{x_4} \vee \overline{x_1}{\cdot}\overline{x_2}{\cdot}\overline{x_3})$. Whereas, $\mathcal{E}^{-1}(y_1y_2y_3y_4y_5y_6y_7)=(y_1 \vee y_2, y_1 \vee y_3, y_4 \vee \overline{y_6}{\cdot}\overline{y_7}, y_6 \vee \overline{y_5}{\cdot}\overline{y_7})$. Also in this case both encoding and decoding functions can be realized with very simple logic. Further, note that concatenating this code with itself it is possible to obtain DC$(n=1.75k,k,w=0.5k)$ codes which have the same features as the codes given above but are less redundant.

DC$(n=13,k=8,w=3)$ code design. Note that any constant weight 3 coding method requires at least 5 extra check bits to encode 8 bit data. Further, using 5 check bits, 8 is the maximum length of information word that can be made constant weight 3. Thus, this code is optimal from the redundancy point of view. The code design is also simple because the whole coding system (encoder plus decoder) for this code can be implemented using less than 1070 transistors with a depth of less than 30 transistors. Because of the space limitation, the code design is not given here. Note that, concatenating this code with itself it is possible to obtain efficient DC$(n=1.625k,k,w=0.375k)$ codes.

Speed performance analysis of LCW codes in the asynchronous communication scheme. Parallel asynchronous communication in asynchronous busses is realized using unordered codes [1], [4], [2]. Researchers in [1], have modeled the asynchronous communication scheme as a situation in which the sender communicates with the receiver using n parallel tracks (the bus lines) by rolling marbles in the tracks. If the i-th component of the code word is a 1 then the sender rolls a marble in the i-th track of the bus. The amount of time a marble takes to travel from the source to the destination is unknown and may differ from track to track or even from roll to roll. But it is non-negative and finite. The only way the receiver has to realize the complete reception of the code word is to make a membership test of the current word in the unordered code at the receiver end of the bus. Once complete reception is detected, the receiver sends an acknowledgment signal to the sender indicating that it is ready to receive the next code word. In the usual implementation of the scheme, the receiver detects the complete reception of the word when the last marble of the word is received. This is a special case of t-proximity detection [4] in which certain t-proximity detecting (t-PD) codes are used to allow the receiver to send the acknowledgment signal to the sender when all but t of the transmitted 1/marbles of a code word have been received. Examples of t-PD codes are constant weight codes, for all $t \geq 0$ [4]. For $j=1,2,\ldots,w$ let X_j be the random variable which represents the transmission time for the j-th marble of the word. In [2], assuming that the X_j's are continuous, independent and all uniformly distributed over the time interval $[t_{min},t_{max}]$, it is shown that the average transmission time for a code word of a t-PD code is

$$\overline{T}_{t-PD}(w) = t_{min} + \frac{w-t}{w+1}(t_{max}-t_{min}).$$

In this paper, using the above formula we are able to quantify the speed performance of t-PD codes, $t \geq 0$, and make the transmission time comparisons given in Table 1. Analogous conclusion can be drawn for distributions which are different from the uniform distribution given above.

	0-PD	1-PD	2-PD	3-PD	4-PD	5-PD	6-PD	7-PD
DC$(w=1)$	25.9%	-	-	-	-	-	-	-
DC$(w=2)$	13.3%	41.7%	-	-	-	-	-	-
DC$(w=3)$	7.9%	25.9%	51.1%	-	-	-	-	-
DC$(w=4)$	4.9%	18.1%	34.9%	57.4%	-	-	-	-
DC$(w=5)$	3.0%	13.3%	25.9%	41.7%	61.9%	-	-	-
DC$(w=6)$	1.7%	10.2%	20.2%	32.2%	46.9%	65.3%	-	-
DC$(w=7)$	0.7%	7.9%	16.2%	25.9%	37.4%	51.1%	67.9%	-
DC$(w=8)$	0.0%	6.3%	13.3%	21.4%	30.8%	41.7%	54.5%	70.0%
BC$(w=5.36)$	2.5%	-	-	-	-	-	-	-
1-VP$(w=7.29)$	0.5%	7.4%	-	-	-	-	-	-
2-VP$(w=7.73)$	0.2%	6.7%	14.1%	-	-	-	-	-

Tab. 1: Minimum speed-up comparisons between some t-PD codes and the dual-rail code with $k=8$ information bits used as 0-PD code. The codes DC(w) are constant weight w codes. The code BC$(w=5.36)$ is a Berger like code designed to minimize the average weight per code word. The codes 1-VP$(w=7.29)$ and 2-VP$(w=7.73)$ are respectively, systematic 1 and 2-PD codes of [4].

References

[1] M. Blaum and J. Bruck, "Delay-insensitive pipelined communication on parallel busses", *IEEE Transactions on Computers*, vol. 44, pp. 660–668, May 1995.

[2] L. G. Tallini and B. Bose, "On parallel asynchronous communication codes", in *Proceedings 1999 IEEE Information Theory Workshop*, IEEE Press, p. 107, June 1999.

[3] M. R. Stan and W. P. Burleson, "Low-power encodings for global communication in CMOS VLSI", *IEEE Transaction on VLSI Systems*, vol. 5, pp. 444–455, Dec. 1997.

[4] N. H. Vaidya and S. Perisetty, "Systematic proximity-detecting codes", *IEEE Transactions on Information Theory*, vol. 43, pp. 1852–1863, Nov. 1997.

*This work was supported by the National Science Foundation under Grant MIP-9705738.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Algorithm for Joint Decoding of Turbo Codes and M-ary Orthogonal Modulation

Paul C. P. Liang[1]
EECS Dept., Univ. of Michigan
Ann Arbor, MI 48109, USA
e-mail: cpliang@eecs.umich.edu

Wayne E. Stark
EECS Dept., Univ. of Michigan
Ann Arbor, MI 48109, USA
e-mail: stark@eecs.umich.edu

Abstract — **In this paper, we consider the concatenation of turbo codes and M-ary orthogonal modulation. A modified decoding algorithm that utilizes the correlated nature of an orthogonal symbol drawn from a Hadamard matrix and the soft-input/soft-output module of turbo codes is introduced. This improved decoding algorithm can significantly lower the error shoulder and reduce the SNR required for a given error probability.**

I. Introduction

In our research, a concatenation of turbo codes (outer code) and orthogonal codes (inner code) is investigated for PCS applications. We propose a two-stage joint decoding of both turbo codes and orthogonal codes. The proposed algorithm iteratively evaluates the log-likelihood metrics for both systematic and turbo-encoded parity bits and feeds the a priori information back to the orthogonal decoder.

II. System Model and Joint Decoding

An information sequence, $d_k \in \{0,1\}$, is encoded with a rate 1/3 turbo code. The coded sequence is then multiplexed onto a single data stream, block interleaved to break up the correlation among the consecutive bits, and passed to an orthogonal modulator. The orthogonal modulation is a Hadamard matrix with rate $r = \log_2 M/M = K/N$. An additive white Gaussian noise (AWGN) channel with and without Rayleigh fading is considered in this paper and noncoherent reception is used at the receiver.

The proposed iterative decoding process is composed of two stages. The first stage is the maximum a posteriori (MAP) decoding of the Hadamard matrix. The second stage is the modified turbo decoding.

For the first stage decoding, the received complex signal is processed with the fast Hadamard transform and then square-law combined to form a decision vector $\mathbf{w}$, where $\mathbf{w} = \{w_1, ..., w_{N-1}\}$. If the i^{th} row of the Hadamard matrix $(\mathbf{H}_i)$ is sent, the conditional probability is given as follows

$$p(w_j|\mathbf{H}_i) = \begin{cases} p_s(w_j) = \frac{1}{2\sigma^2} e^{-\frac{w_j+z^2}{2\sigma^2}} I_0\left(\frac{\sqrt{w_j}z}{\sigma^2}\right) & \text{for } j = i \\ p_n(w_j) = \frac{1}{2\sigma^2} e^{-\frac{w_j}{2\sigma^2}} & \text{for } j \neq i \end{cases}$$

where σ^2 is the average noise variance, z^2 is the expected received signal energy and $I_0()$ is the zeroth-order modified Bessel function of the first kind.

By applying Bayes law, the a posteriori probability can be expressed as $P(\mathbf{H}_i|\mathbf{w}) = p(\mathbf{w}|\mathbf{H}_i)P(\mathbf{H}_i)/p(\mathbf{w})$, where $p(\mathbf{w}|\mathbf{H}_i) = p_n(w_0) \cdot ... \cdot p_s(w_i) \cdot ... \cdot p_n(w_{N-1})$ and $p(\mathbf{w})$ is a constant independent of i. With the assumption of large packet size and proper interleaving, the information bits fed into one orthogonal symbol $(x_0...x_{K-1})$ are assumed to be independent and therefore the a priori information $P(\mathbf{H}_i) = P(x_0)P(x_1)...P(x_{K-1})$. The next step is to evaluate the conditional probability of the K systematic bits of the Hadamard function. This can be done by summing the objective x_k, $P(x_k = 0|\mathbf{w}) = \sum_{i=0,x_k=0}^{N-1} P(\mathbf{H}_i|\mathbf{w})$. Finally, we can evaluate the density function $p(\mathbf{w}|x_k)$ by applying Bayes law. This information will be passed onto the turbo decoding.

The second stage is an iterative decoding process and the derivation of this algorithm is well described in previous papers. After several turbo iterations, the log-likelihood ratio (LLR) of the systematic bits will converge. The LLR of systematic bits are used as a prior information to decode the turbo-encoded parity bits [2]. The decoding process is similar to that of the systematic bits. Finally, all the LLR information is then fedback as a priori information to the inner orthogonal code. In this two stage sequential decoding, the quality of the turbo decoding output is very important.

III. Result and Conclusion

Figure 1 shows the bit error rate (BER) of the 64-ary system in both an AWGN and Rayleigh fading channels with a packet size of 1200 information bits. The system without feedback to the orthogonal codes (i.e., without joint decoding (JD)) but with 10 turbo decoding iterations is compared to the system with 5 initial turbo decoding iterations, one feedback to the orthogonal decoding, and 5 additional turbo decoding iterations. The proposed JD algorithm achieves a significant reduction in error probabilities. The error shoulder introduced by the turbo code is also shown to be lowered to the region beyond interest.

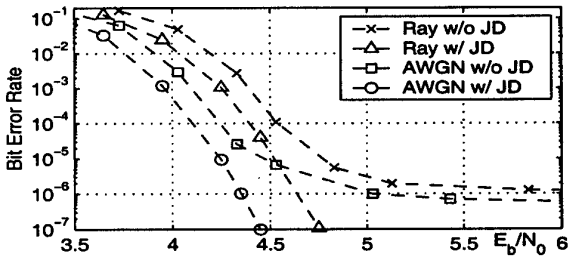


Fig. 1: BER for 64-ary noncoherent reception.

References

[1] R. Herzog, J. Hagenauer and A. Schmidbauer , "Soft-In/Soft-Out Hadamard Despreader for Iterative Decoding in the IS-95(A) System," *in Proc. ICC, 97.*, pp. 1219–1222.

[2] Paul C. P. Liang and Wayne E. Stark, "Iterative Multiuser Detection for Turbo-Coded FHMA Communications," to be appear *in Proc. of WCNC, 2000.*

[1]This work was supported by Army Research Office grant DAAH04-96-1-0377.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Turbo Nonlinear CPFSK with Iterative Decoding

Bon-Jin Ku, Woong-Gon Kim, Ha-Young Yang, Dae-Sik Hong and Chang-Eon Kang
Department of Electrical & Computer Eng., Yonsei University
134, Shinchon-dong, Seodaemoon-gu, Seoul, 120-749, Korea

Abstract — A Turbo nonlinear continuous phase frequency shift keying (CPFSK) with iterative maximum a posteriori probability (MAP) decoding is proposed. It uses the nonlinear CPFSK encoding components proposed by us. They have nonlinear characteristics and good performance of power and bandwidth with simple structures.

I. INTRODUCTION

Turbo codes, newly invented by Berrou et al [1], are good error-correcting codes that yield remarkable bit error rates (BER) close to Shannon limits with simple encoding structures. And they were proposed for BPSK modulation. But when more spectral efficiency is needed such as in satellite communications, other modulations with constant envelopes may be used.

In constant envelope digital modulation the information-carrying phase varies continuously, which reduces the side lobe of the spectrum of signal. Such a modulation scheme is called the continuous phase modulation (CPM) [2]. CPM can be decomposed into the continuous phase encoder (CPE) and the memoryless signal mapping (MM) modulation part in the same way as trellis-coded modulation (TCM). The nonlinear CPFSK introduces a nonlinear modulation index, which is a kind of multi-h CPM with the non-time-varying phase trellis. And we have proposed an *M*-ary nonlinear CPFSK scheme to achieve more spectrum efficiency [3]. Also, it achieves higher improved performance than ordinary CPFSK.

In this paper, we propose the Turbo nonlinear CPFSK systems with iterative MAP decoding. The overall structure is similar to Turbo codes or Turbo TCM [4] but uses the proposed nonlinear CPFSK encoding components that allow better performance than RSC components in Turbo code. The Turbo nonlinear CPFSK code has nonlinear characteristics and good performance of power and bandwidth with simple structures. The proposed schemes improve the performance relatively over Turbo code with modulations and overcome the nonlinear property, so they can provide reliable communications such as in satellite channels.

II. THE TURBO NONLINEAR CPFSK

The decomposition of the nonlinear CPFSK — the decomposition of the MM modulator and the nonlinear continuous phase encoder (NCPE).

A new representation of coded symbols considered as the sum of the product input and the past symbols of the convolutional encoder is expressed by

$$s(t,u_n)=\sqrt{\frac{2E}{T}}\cos(w_0 t+\psi(t,u_n)), \qquad (1)$$

where E is the bit energy, T is the symbol duration, and w_0 is the carrier frequency. To produce the present input symbol u_n and the present state V_n, it introduces the nonlinear symbol into the CPE and the nonlinear MM modulator. Then inputs of the nonlinear MM modulator can be represented as M-ary symbol u_n and V_n.

$$\Psi(t,u_n)=2\pi h\left(mod_N[u_n]\frac{(t-nT)}{T}+mod_N[V_n]\right), \qquad (2\text{-a})$$

$$u_n=x(a,f)=f_0+\sum_{i=1}^{c} f_i a_{n-i+1}+\cdots+f_{1\cdots c}a_n\cdots a_{n-c+1}, \qquad (2\text{-b})$$

$$V_n=a_{n-1}\cdot M^{c-1}+\ldots+a_{n-c+1}\cdot M^0, \qquad (2\text{-c})$$

$$V_{n+1}=mod_N[V_n+u_n], \qquad (2\text{-d})$$

where u, V, and the nonlinear mapping coefficients f are defined in the modular N spaces, M presents M-ary symbol and c is the number of input symbols at the nonlinear MM.

The overall system — we apply the basic principles and modified structures of Turbo codes for the Turbo nonlinear CPFSK. A search for good component codes is performed from Eq. (4). In the presence of AWGN, the probability of the nonlinear CPFSK maximum likelihood (ML) receiver making an erroneous decision can be closely approximated by

$$P_e\approx Q\left(\sqrt{\frac{d_{\min}^2 E_b}{N_0}}\right). \qquad (3)$$

$$d_{\min}^2=\frac{1}{T}\min_{a,b}\lim_{N_r\to\infty}\int_0^{N_r T}\left[1-(\cos\phi(t,a)-\cos\phi(t,b))\right]dt \qquad (4)$$

where E_b is bit energy, $d_{\min}^2$ is the normalized squared Euclidean distance and N_r is the number of interval of remerge path.

The iterative decoder consists of two identical concatenated decoders of the component codes separated by the interleaver. The component decoders are based on MAP algorithms generating weighted soft estimates of the input sequences.

III. CONCLUSIONS

In this paper, we have presented Turbo nonlinear CPFSK systems that have iterative MAP decoders. The overall structure is similar to Turbo codes or Turbo TCM codes but exploits the non-linearity of the component codes. They have nonlinear characteristics and good performance of power and bandwidth with simple structures.

REFERENCES

1. C. Berrou, A. Glavieux and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo-codes," ICC '93, Geneva, May 1993.
2. J. P. Fonseka, "Nonlinear continuous phase frequency shift keying," *IEEE Trans. on Comm.*, COM-39, pp. 1473-1481, 1991.
3. P. Y. Jou, B. J. Ku, S. J. Lim, Y. W. Yun and C. E. Kang, "*M*-ary nonlinear CPFSK over satellite channel," IWTS '97, pp. 237-240, May 1997.
4. P. Robertson and T. Worz, "Bandwidth-Efficient Turbo Trellis-Coded Modulation Using Punctured Component Codes," *IEEE Journal on Selected Areas in Comm.*, vol. 16, no. 2, pp. 206-218, Feb. 1998.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

BER Bounds for Turbo Coded Modulation and their Application to Adaptive Modulation

Sriram Vishwanath and Andrea Goldsmith[0]
Packard Electrical Engg., Stanford, California 94305, U.S.A
email:sriram,andrea@systems.stanford.edu

Abstract — **We present upper bounds for bit error rates of Turbo Coded Modulation (TuCM) on AWGN channels. We then apply these bounds to calculate the spectral efficiency of adaptive TuCM on flat fading channels, which comes within 4dB of the fading channel capacity limit.**

I. Transfer Function bounds

Techniques that compute bounds on the bit error rate of coded systems based on the input-output transfer function of the state diagram describing the system are referred to as *transfer function bounds.* Previous work describes such bounds for trellis codes and turbo codes[1] with binary modulation [1]. We extend this idea and apply it to Turbo Coded Modulation(TuCM) with permuter size N, where the output bits are mapped to a higher level constellation. Let the sets S_1 and S_2 represent all possible states and the sets B_1 and B_2 represent all possible edges in the state diagram of the constituent encoders 1 and 2 of the turbo code under consideration. Let E_1 and E_2 denote the set of all possible error states and C_1 and C_2 the sets of all possible edges in the error state diagrams of the constituent encoders 1 and 2. Then we define a super-state for constituent encoder 1 as an element of the set $Z_1 = \{(s_1, e_1) : s_1 \in S_1, e_1 \in E_1\}$ and a super-edge as belonging to the set $W_1 = \{[b_1, c_1] : b_1 \in B_1, c_1 \in C_1\}$. Similarly super-state set Z_2 and super-edge set W_2 can be defined for constituent encoder 2. We now define a combined-state as one that belongs to the set $\{(z_1, z_2) : z_1 \in Z_1, z_2 \in Z_2\}$ and a combined-edge as belonging to the set $\{[w_1, w_2] : w_1 \in W_1, w_2 \in W_2\}$. The combined-states and combined-edges in a graphical representation form a *combined state diagram.* In this diagram, each combined-edge $[w_1, w_2]$ has a label of the form $\mathbf{I}^i\mathbf{J}^j\mathbf{X}^x\mathbf{Y}^y\mathbf{D}^{d^2}\mathbf{L}$, where $\mathbf{I}, \mathbf{J}, \mathbf{X}, \mathbf{Y}, \mathbf{D}, \mathbf{L}$ are dummy variables which carry useful information in their exponents. i, j equal the input weights of the constituent encoders 1 and 2, corresponding to the combined-edge $[w_1, w_2]$. Similarly, x, y represent weights of error patterns and d the Euclidean distance between correctly and incorrectly decoded codewords corresponding to $[w_1, w_2]$. The variable $\mathbf{L}$ is present on each combined-edge to denote a transition. This combined-state diagram can be treated as a signal flow graph with the labels on the edges being treated as gains, and its transfer function from the all-zero state back to the all-zero state can be obtained. The coefficient of $\mathbf{L}^N$ in a series expansion of this transfer function can be written as $\mathbf{T}(\mathbf{I}, \mathbf{J}, \mathbf{X}, \mathbf{Y}, \mathbf{D}) = \sum_{1\le i,j,x,y\le N} \sum_d a_{i,j,x,y,d}\mathbf{I}^i\mathbf{J}^j\mathbf{X}^x\mathbf{Y}^y\mathbf{D}^{d^2}$ and the BER can be bounded as $P_{bit} \le \sum_{1\le i,x\le N} \sum_d \frac{x}{N} \frac{a_{i,i,x,x,d} e^{-d^2/4N_0}}{\binom{N}{i}\binom{N}{x}}$, where $N_0/2$ is the power spectral density of the noise. This expression can be simplified if the outputs of the two constituent encoders of the TuCM are modulated independently. If the coefficient of $\mathbf{L}^N$ in the transfer function of super-state diagram of the jth constituent encoder[2] is $\mathbf{T}_j(\mathbf{X}, \mathbf{I}, \mathbf{D}) = \sum_{1\le i,x\le N} \sum_d n_{j,x,i,d}\mathbf{X}^x\mathbf{I}^i\mathbf{D}^{d^2}$, then the BER of the net TuCM scheme can be bounded as $P_{bit} \le \sum_{1\le i,x\le N} \frac{x}{N}\left(\binom{N}{x}\binom{N}{i}\right)^{-1} \sum_d n_{1,x,i,d} n_{2,x,i,d} e^{-d^2/4N_0}$. An example code from [2] with 16-state constituent encoders, $N = 4096$ and 8PSK per encoder was chosen, with feedback polynomial $h_0 = 23$ and $h_1 = 14, h_2 = 16, h_3 = 21, h_4 = 31$ as feedforward polynomials and reordered mapping. The bound matched simulation results within 1.5 dB at high SNR.

II. Average bounds and Adaptive Modulation

Next, we propose an average bound for Self Concatenated Coded Modulation(SCCM), realizing that TuCM are special cases of these. We use the transfer function technique described in Section I, but this time average over all possible rate b/n recursive constituent encoders of memory k to get the Error-path Length Generating function(ELGF) as $\mathbf{A}(\mathbf{M}, \mathbf{L}) = \sum_{i,j} a_{i,j}\mathbf{M}^i\mathbf{L}^j$, where $\mathbf{M}$ and $\mathbf{L}$ are dummy variables representing error weight and error length respectively. Using the definition for R_0 in [3] and averaging over all scramblers[3], we obtain $P_{bit} \le 1/N2^{-(N-kb)}\partial\mathbf{A}(\mathbf{M}, \mathbf{L})/\partial\mathbf{M}$ after substituting $\mathbf{M} = 1$ and $\mathbf{L} = 2^{2nR_0}$. Considering an adaptive coded modulation system with model and constraints as in [4], we use the average bound to calculate spectral efficiency with 16-state constituent codes and $N = 1024$. The results obtained show a 2dB gain in SNR compared to trellis coded modulation systems, with a spectral efficiency that comes within 4dB of channel capacity.

Acknowledgments

The authors would like to thank Dr.Dariush Divsalar at JPL, Caltech, for his careful reading of the manuscript.

References

[1] D. Divsalar, S. Dolinar and F. Pollara, "Transfer Function Bounds on the Performance of Turbo Codes", *TDA Progress Report 42-122*, August 15, 1995.

[2] S. Benedetto, D.Divsalar, G.Montorsi and F. Pollara, "Parallel Concatenated Trellis Coded Modulation", *Proc. of ICC'96*, June 1996.

[3] Andrew J.Viterbi, "Convolutional Codes and their Performance in Communication Systems", *IEEE Trans. on Commun. Technology*, Vol.Comm-19, No.5, pp 751–772, October 1971

[4] A. J. Goldsmith and S. Chua, "Adaptive Coded Modulation for Fading Channels", *IEEE Trans. on Commun.*, Vol. 46, pp. 595–602, May. 1998.

[0]This work was supported by ONR Young Investigation Award N00014-99-1-0578

[1]which typically consist of two constituent encoders in parallel.

[2]This super-state diagram is labelled with $\mathbf{I}^i\mathbf{X}^x\mathbf{D}^{d^2}\mathbf{L}$, with i, x, d being input weight, error weight and Euclidean distance of error.

[3]Scramblers map any sequence of length N to any other sequence of length N.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Serial Turbo Trellis Coded Modulation with Rate-1 Inner Code*

Dariush Divsalar, Sam Dolinar, and Fabrizio Pollara
Jet Propulsion Laboratory, California Institute of Technology. 4800 Oak Grove Drive, Pasadena, CA
e-mail: {dariush,sam,fabrizio}@shannon.jpl.nasa.gov

Abstract — **We develop new, low-complexity turbo codes suitable for bandwidth and power limited systems. These codes are constructed as an extension of Repeat-Accumulate codes to high-level modulations. Two design criteria are proposed, based on maximum-likelihood decoding and on Gaussian density evolution in iterative decoding.**

I. Structure of SCTCM with Rate-1 Inner Code

Our recent results on concatenation of an outer code with a simple accumulator as inner code for binary modulation [2] led us to develop a new method for serial concatenated TCM (SCTCM). For MPSK, or a two dimensional constellation with M points, let's define $m = \log_2 M$. We propose a novel method to design low-complexity serial concatenated TCM, which achieves $bm/(b+1)$ bits per modulation symbol, using an outer rate $b/(b+1)$ binary convolutional code (or a short block code) with maximum free Hamming distance. An interleaver π permutes the output of the outer code. The interleaved data enters a rate $m/m = 1$ recursive convolutional inner encoder. The m output bits are then mapped to one symbol belonging to a 2^m-level modulation.

The inner code and the mapping are jointly optimized. For short blocks we use the ML criterion based on maximizing the effective free Euclidean distance of the inner TCM (see [1] for more detail on ML design criteria). For large block sizes we use a new minimum-threshold criterion for iterative decoding to be discussed shortly. Considering 8PSK ($m = 3$) modulation as an example, then the throughput $r = 3b/(b+1)$ is as follows: for $b = 2$, $r = 2$; for $b = 3$, $r = 2.25$; and for $b = 4$, $r = 2.4$. This suggest that we can use a rate 1/2 convolutional code with puncturing to obtain various throughputs without changing the inner code or modulation.

For rectangular M^2-QAM, where $m = \log_2 M$, the structure becomes even simpler. In this case, to achieve throughput of $2mb/(b+1)$ bits/symbol we need a rate $b/(b+1)$ outer code and a rate m/m inner code, where the m output bits are alternatively assigned to in-phase and quadrature components of the M^2-QAM modulation. For example consider 16-QAM modulation, where $m = 2$, then the throughput $r = 4b/(b+1)$ is: for $b = 1$, $r = 2$; for $b = 2$, $r = 2.67$; for $b = 3$, $r = 3$; and for $b = 4$, $r = 3.2$.

Here we only discuss the example of 16QAM modulation, and $r = 3$ which implies $b = 3$. The encoder structure of SCTCM for 4-state inner TCM and 4-state outer is shown in Fig. 1 as an example.

II. Iterative Decoding Design Criteria

The design criterion is based on the method of density evolution proposed by Richardson and Urbanke [3]. It has been observed by many researchers that the extrinsic information in iterative decoding can be approximated by a Gaussian density function. El Gamal [4] considered the soft-input soft-output APP module in turbo decoders as a signal-to-noise ratio (SNR) transformer. Using these ideas, and the method for analyzing turbo codes suggested by El Gamal [4], we extended the results to analyze concatenated TCM by approximating the density functions for extrinsics as Gaussian densities, and then computing the mean and variance in the Gaussian density evolution. Since the probability of incorrect decoding is given by $Q(\sqrt{\text{SNR}})$, where SNR = mean^2/variance, we only need to track the SNR. This will result in a slightly pessimistic threshold since the Gaussian density has the highest entropy for a given variance. Slightly optimistic threshold results are obtained if we impose density consistency as proposed by Richardson et al, which suggests that we only need to compute the mean (SNR=mean/2). At each iteration, we computed SNRs (averaged over all transmitted patterns), and collected them for the outer and the inner codes. We used the example of 4-state outer with puncturing pattern 100100... and 4-state rate-1 inner as shown in Fig. 1. The output-input SNR for the inner code and the input-output SNR for the outer code are shown in Fig. 1. Iterations for E_b/N_o=5.5 dB are also shown in the Fig. 1. If the two curves do not cross, then the iterative decoder converges. Note that we used all assumptions made by Richardson and Urbanke for very large block sizes and the concentration theorem. In Fig. 1 we see that if E_b/N_o is greater than 4.8 dB, the iterative decoder converges, where the capacity limit is 4.54 dB. This method was used to select the 2-state and the 4-state inner TCM codes. The performance of iterative decoding of this serial TCM with 16QAM for input block size of 12288 bits and 8 iterations required E_b/N_o = 6 dB at BER=4 × 10^{-8}.

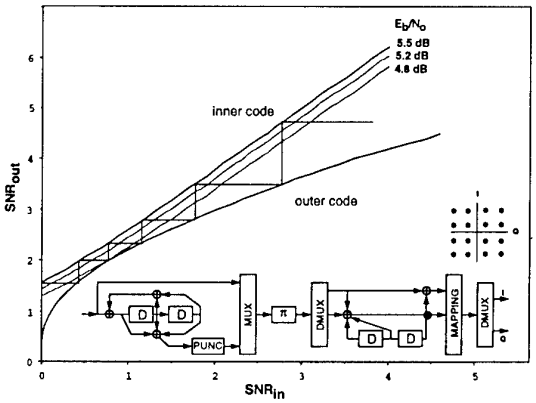


Figure 1: Graphical analysis of iterative decoding threshold (16QAM, puncturing pattern 100, r=3).

References

[1] S. Benedetto, D. Divsalar, G. Montorsi, F. Pollara, "Serial Concatenated Trellis Coded Modulation with Iterative Decoding: Design and Performance", IEEE Global Telecommunications Conference, (CTMC), November 1997.

[2] D. Divsalar, H. Jin, R.J. McEliece, "Coding Theorems for "Turbo-Like" Codes", 1998 Allerton Conference, Sept. 23-25, 1998.

[3] T. Richardson and R. Urbanke, "The capacity of low density parity check codes under message passing decoding, submitted to IEEE trans. on Information Theory.

[4] H. El Gamal, "On the theory and application of space-time and graph based codes," Ph.D. dissertation, 1999, University of Maryland at College Park.

*The work described was funded by the TMOD Technology Program and performed at the Jet Propulsion Laboratory, California Institute of Technology under contract with the National Aeronautics and Space Administration.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Quasi-cyclic Goppa codes.

Thierry P. Berger [1]
Université de Limoges,
Département de Mathématiques
123 av. A. Thomas,
87060F Limoges cedex, FRANCE
e-mail: thierry.berger@unilim.fr

Abstract — **In this paper, we construct quasi-cyclic Goppa (or related) codes. Some of these codes reach the parameters of best known codes. Generally, there is no known quasi-cyclic code for these lengths and dimensions.**

I. Introduction

Alternant codes are subfield subcodes of Generalized Reed-Solomon codes (GRS code). Goppa codes are particular case of Alternant codes. In [2], we proved that parity-check subcodes of Goppa codes and extensions of Goppa codes are also Alternant codes. In [3], A. Dür characterized of GRS codes. Some semi-monomial automorphisms of GRS codes that are not permutations of the support induce a permutation of the subfield-subcodes [1, 2]. We use this method for constructing Goppa codes invariant under some prescribed permutations.

II. Classical Goppa codes

Let K be the finite field $GF(p^m)$ and $\overline{K} = K \cup \{\infty\}$. Let $\mathcal{L} = (\alpha_0, \ldots, \alpha_{n-1})$ be an n-tuple of distinct elements of K. It will be the *support* of the codes. Let $\mathbf{v} = (v_0, \ldots, v_{n-1})$ be an n-tuple of non-zero elements of K. For $s = 0, \ldots, n$, let $\theta_{s,\mathbf{v},\mathcal{L}}$ be the n-tuple $\theta_{s,\mathbf{v},\mathcal{L}} = (v_0\alpha_0^s, \ldots, v_{n-1}\alpha_{n-1}^s) \in K^n$.

Definition 1 *Let k be an integer less than n. The Alternant code $\mathcal{A}_k(\mathbf{v}, \mathcal{L})$ is the code of length n over $GF(p)$ with parity-check matrix $M_k(\mathbf{v}, \mathcal{L})$ whose rows are $\theta_{s,\mathbf{v},\mathcal{L}}$ for $s = 0, \ldots, k-1$.*
Let $g(x) \in K[x]$ be a polynomial of degree $r \leq n$ such that $g(\alpha_i) \neq 0$ for $i = 0, \ldots, n-1$. The Goppa code $\mathcal{G}(g, \mathcal{L})$ with Goppa polynomial $g(x)$ and support $\mathcal{L}$ is the Alternant code $\mathcal{A}_r(\mathbf{v}_{g,\mathcal{L}}, \mathcal{L})$ with $\mathbf{v}_{g,\mathcal{L}} = (g(\alpha_0)^{-1}, g(\alpha_1)^{-1}, \ldots, g(\alpha_{n-1})^{-1})$.

Definition 2 *The parity-check subcode $\tilde{C}$ of C is the subset of elements $\mathbf{x} = (x_0, \ldots, x_{n-1}) \in C$ satisfying the parity-check control $x_0 + x_1 + \ldots + x_{n-1} = 0$.*
The extension $\overline{C}$ of C is obtained by adding a parity-check control symbol $x_n = -(x_0 + x_1 + \ldots + x_{n-1})$ to the codewords of C.

III. Main results

We use ∞ for the support of parity-check control symbol of the extension of a Goppa code.

Let f be an element of the projective semi-linear group $P\Gamma L(2, K)$. f can be considered as a permutation of $\overline{K}$: $f(\zeta) = (a\zeta^q + b)/(c\zeta^q + d)$, $ad - bc \neq 0$, $q = p^i$.

Let $\mathcal{L}_f$ be a union of orbits of elements of $\overline{K}$ under f. Clearly, f induces a permutation of the support $\mathcal{L}_f$.

Theorem 1 *Let $g(x) = \sum_{i=0}^{r} g_i x^i$ be a Goppa polynomial of degree $r < n$.*

1) Let f be an element of $A\Gamma L(1, K)$ (i.e. $f(\zeta) = a\zeta^q + b$). If g satisfies $g(ax^q + b) = a^r g_r^{1-q} g(x)^q$, the Goppa code $C = \mathcal{G}(g, \mathcal{L}_f)$ is invariant under f.

2) Let f be an element of $P\Gamma L(2, K)$, $\infty \notin \mathcal{L}_f$. If g satisfies $g(a) \neq 0$ and $\sum_{i=0}^{r} g_i (ax^q + b)^i (cx^q + d)^{r-i} = g(a) g_r^{-q} g(x)^q$, then the parity-check subcode $\tilde{C}$ of the Goppa code $C = \mathcal{G}(g, \mathcal{L}_f)$ is invariant under f.

3) Suppose that $\mathcal{L}_f$ contains ∞ and $\mathcal{L}$ is $\mathcal{L}_f$ without ∞. Let f be an element of $P\Gamma L(2, K)$. If g satisfies $g(a) \neq 0$ and $\sum_{i=0}^{r} g_i (ax^q + b)^i (cx^q + d)^{r-i} = g(a) g_r^{-q} g(x)^q$, then the extension $\overline{C}$ of the Goppa code $C = \mathcal{G}(g, \mathcal{L})$ is invariant under f.

IV. Application to the construction of quasi-cyclic Goppa codes

In [2], we gave an algorithm for computing the polynomials g described in Theorem 1.

Choosing for support $\mathcal{L}$ some union of orbits of same length, this gives us quasi-cyclic codes.

We give now some non-exhaustive examples of parameters. All these codes meet the bound of best known codes. The order of quasi-cyclicity (i.e. the order of the quasi-cyclic permutation) is given in index.

Goppa codes:

$[84, 70, 5]_{14}$, $[63, 51, 5]_9$, $[63, 39, 9]_9$, $[60, 48, 5]_{12}$, $[60, 36, 9]_{12}$, $[52, 40, 5]_{13}$, $[45, 27, 8]_9$, $[36, 18, 8]_9$.

Parity-check subcodes of Goppa codes

$[98, 83, 6]_{14}$, $[84, 55, 10]_{14}$, $[84, 69, 6]_{14}$, $[70, 41, 10]_{14}$, $[56, 41, 6]_{14}$, $[36, 18, 8]_{18}$.

Extended Goppa codes:

$[84, 55, 10]_{14}$, $[84, 3, 48]_{14}$, $[70, 41, 10]_{14}$, $[63, 38, 10]_9$, $[54, 41, 6]_{18}$, $[54, 35, 8]_{18}$.

These codes are obtained for $K = GF(128)$ or $K = GF(64)$ using MAGMA.

References

[1] T.P. Berger, "Cyclic Alternant codes induced by an automorphism of a GRS code," *Finite fields: Theory, Applications and Algorithms,* (R. Mullin & G. Mullen Eds). AMS, Contemporary Mathematics vol. 225, pp. 143-154, 1999.

[2] T.P. Berger, "On the cyclicity of Goppa codes, parity-check subcodes of Goppa codes and extended Goppa codes," to appear in *Finite Fields and their Applications.*

[3] A. Dür, "The Automorphism Group of Reed Solomon Codes," *J. of Combinatorial Theory,* series A, vol. 4, 1, pp. 69-82, 1987.

[1] Associated Searcher, projet CODES, INRIA-Rocquencourt, 78153F LE CHESNAY, FRANCE

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Algebraic Structure of Quasicyclic Codes

Kristine Lally
Department of Mathematics
National University of Ireland
Cork, Ireland
e-mail: k.lally@ucc.ie

Patrick Fitzpatrick
Department of Mathematics
National University of Ireland
Cork, Ireland
e-mail: fitzpat@ucc.ie

Abstract —

We use Gröbner bases of modules to construct and classify quasiscyclic codes. Whereas previous studies have been mainly concerned with the 1-generator case, our results elucidate the structure of arbitrary quasicyclic codes and their duals. We include a complete characterisation of selfdual quasicyclic codes of index 2.

I. Introduction

The theory of Gröbner bases of modules has been applied [F95, F96, F97] to decoding Reed-Solomon codes, to scalar rational interpolation, and to various other problems, such as Padé approximation, that can be represented as solving systems of polynomial congruences. The structure of quasicyclic codes was explored by Séguin and others [CS, SD, SH]. We adopt a new approach based on the construction of a canonical Gröbner basis generating set for a quasicyclic code regarded as a submodule of R^ℓ where $R = F[x]/\langle x^m - 1\rangle$.

NB: *Throughout the paper the word "code" means "quasicyclic code".*

II. Basic structure

Let $\mathcal{C}$ be a code of length ℓm and index ℓ over F, where ℓ the smallest power of the cyclic shift operator under which $\mathcal{C}$ is invariant. By a coordinate permutation we obtain the polynomial representation of $\mathcal{C}$ as an R–submodule of R^ℓ. The code $\mathcal{C}$ is the image of an $F[x]$-submodule $\tilde{\mathcal{C}}$ of $F[x]^\ell$ containing $\tilde{\mathcal{K}} = \langle (x^m - 1)e_i, i = 1, \ldots, \ell\rangle$ (where e_i is the standard basis vector) under the natural homomorphism $\varphi : (a_1, \ldots, a_\ell) \mapsto (a_1 + \langle x^m - 1\rangle, \ldots, a_\ell + \langle x^m - 1\rangle)$. We use position-over-term (POT) order in $F[x]^\ell$, with $e_i > e_j$ for $i < j$.

Theorem 1 *The reduced Gröbner basis of $\tilde{\mathcal{C}}$ is*

$$\tilde{\mathcal{G}} = \{g_i = (0, \ldots, g_{ii}, \ldots, g_{i\ell}), i = 1, \ldots, \ell\}$$

where

i. *g_{ii} is monic and $\partial g_{ki} < \partial g_{ii}$ for $k < i$*

ii. *g_{ii} divides $x^m - 1$*

iii. *if $g_{ii} = x^m - 1$ then $g_i = (x^m - 1)e_i$.*

The F–dimension of $F[x]^\ell/\tilde{\mathcal{C}}$ is $\sum_{i=1}^{\ell} \partial g_{ii}$. If G is the polynomial matrix with rows g_i then there is a matrix A satisfying $AG = GA = (x^m - 1)I$.

Thus $\mathcal{C}$ has an R–generating set $\mathcal{G}$ comprising the elements of a Gröbner basis $\tilde{\mathcal{G}}$ not mapped to zero under φ. We refer to this set of generators as a *GB generating set* of $\mathcal{C}$ (or *RGB generating set* as appropriate).

Corollary 2 *The dimension of the code $\mathcal{C}$ with GB generating set $\{\varphi(g_i), i = 1, \ldots, \ell\}$ is $\ell m - \sum_{i=1}^{\ell} \partial g_{ii} = \sum_{i=1}^{\ell} (m - \partial g_{ii})$.*

This makes it straightforward to enumerate the possible dimensions of codes, and thus, in principle, construct all possible codes of a given index.

The set of vectors in $F^{\ell m}$ defined by $\{x^{s_i} g_i : i = 1, \ldots, \ell, s_i = 0, \ldots, m - \partial g_{ii} - 1\}$ is a basis of $\mathcal{C}$. These form the rows of a block upper triangular generator matrix of $\mathcal{C}$. Using the matrix A introduced in Theorem 1 we can derive a Gröbner basis representation and generator matrix of $\mathcal{C}^\perp$.

III. Self-dual codes of index 2

We write $x^m - 1 = \prod_{n \in N} f_n^\varepsilon$ over F, where $\varepsilon = m/\mathrm{char}\, F$, and divide the irreducible factors $f_n, n \in N$ into two types according to whether or not $f_n^\star \sim f_n$ (where $u^\star$ denotes the reciprocal of u, and $\sim$ means "is a constant multiple of"). Let $I \subseteq N$ be the set of indices of factors having this property. The others then fall into reciprocal pairs. Let $J \subseteq N$ be a set of indices comprising one element of each of these pairs and define $\pi : J \to N \backslash (I \cup J)$ by $f_j{}^\star = f_{\pi(j)}$. Then $x^m - 1 \sim \prod f_i^\varepsilon \prod f_j^\varepsilon \prod f_{\pi(j)}^\varepsilon$, where $f_i{}^\star \sim f_i$, $f_j{}^\star \sim f_{\pi(j)}, f_{\pi(j)}{}^\star \sim f_j$ and we note that $\partial f_{\pi(n)} = \partial f_n$. Denote the monic factor $c \prod f_i^{\alpha_i} \prod f_j^{\alpha_j} \prod f_{\pi(j)}^{\alpha_{\pi(j)}}$, where c is an appropriate constant, by $[\alpha_i, \alpha_j, \alpha_{\pi(j)}]$.

Theorem 3 *The code $\mathcal{C}$ of index 2 is selfdual if and only if each minimal Gröbner basis of $\tilde{\mathcal{C}}$ has a generator matrix*

$$\begin{pmatrix} [\alpha_i, \alpha_j, \alpha_{\pi(j)}] & v[\beta_i, \beta_j\, \beta_{\pi(j)}] \\ 0 & [\gamma_i, \gamma_j, \gamma_{\pi(j)}] \end{pmatrix}$$

where

i. $2\alpha_i \le \varepsilon, \alpha_j + \alpha_{\pi(j)} \le \varepsilon$

ii. $2\alpha_i \le \varepsilon + \beta_i - \gamma_i, \alpha_j + \alpha_{\pi(j)} \le \varepsilon + \beta_j - \gamma_j, \alpha_j + \alpha_{\pi(j)} \le \varepsilon + \beta_{\pi(j)} - \gamma_{\pi(j)}$

iii. $\alpha_i + \gamma_i = \varepsilon, \alpha_j + \alpha_{\pi(j)} + \gamma_j + \gamma_{\pi(j)} = 2\varepsilon$

iv. $vv'[2\beta_i - 2\alpha_i, \beta_j + \beta_{\pi(j)} - \alpha_j - \alpha_{\pi(j)}, \beta_j + \beta_{\pi(j)} - \alpha_j - \alpha_{\pi(j)}] \equiv 1 \bmod [2\gamma_i - \varepsilon, \gamma_j + \gamma_{\pi(j)} - \varepsilon, \gamma_j + \gamma_{\pi(j)} - \varepsilon]$, *where* $v' = -x^r \hat{v}, r = \sum_i \partial f_i(\alpha_i - \beta_i) + \sum_j \partial f_j(\alpha_j + \alpha_{\pi(j)} - \beta_j - \beta_{\pi(j)})$.

In the special case $[\gamma_i, \gamma_j, \gamma_{\pi(j)}] = x^m - 1$ the RGB generating set of $\mathcal{C}$ is $(1 \quad v)$ where $v\hat{v} \equiv -1 \bmod x^m - 1$ and $\partial v < m$.

References

[CS] J. Conan, G. Séguin, Structural properties and enumeration of quasicyclic codes, *Appl. Alg. in Eng., Comm., and Comp.* 4 (1993) 25–39.

[F95] P. Fitzpatrick, On the key equation, *IEEE Trans. IT* 41 (1995) 1290-1302.

[F96] ———, On the scalar rational interpolation problem, *Math. Contr. Sig., Syst.* 9, (1996) 352-369.

[F97] ———, Solving multivariable congruences by change of term order, *J. Symb. Comp.*, 24 (1997) 505–510.

[SD] G.E. Séguin, G. Drolet, The theory of 1-generator quasi-cyclic codes, RMCC, Kingston, Ontario, 1990.

[SH] G.E. Séguin, H.T. Huynh, Quasi-cyclic codes - A study, RMCC, Kingston, Ontario, 1985.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

New Results on Binary Quasi-Cyclic Codes

Zhi Chen
School of Engineering
Kristianstad University
291 88 Kristianstad
Sweden
Email: Zhi.Chen@tec.hkr.se

Abstract— **Twelve new binary quasi-cyclic(QC) codes, which improve the lower bounds on minimum distances for binary linear codes, are presented, and a web database on best-known binary QC codes is constructed for public access.**

I. INTRODUCTION

Quasi-cyclic (QC) codes are a generalization of cyclic codes whereby a cyclic shift of a codeword by p positions is still a codeword. Cyclic codes are a special case of QC codes with p = 1. It has been known that QC codes contain many of the best-known linear codes[2,3].

Circulant matrices are building blocks in the generator matrix of a QC codes. A circulant matrix can be specified by a polynomial with the first row as the coefficients. If m be the dimension of the matrix, then the block length for the QC code is n = mp, where p is the number of circulants for the code.

Let $g_0(x)$, $g_1(x)$, ..., $g_{p-1}(x)$ be p generator polynomials for the QC [mp, k] code. Then its generator matrix can be defined by

$$G = (g_0(x), g_1(x), \ldots, g_{p-1}(x)) \quad (1)$$

Let

$$h(x) = (x^m - 1) / \gcd\{ x^m - 1, g_0(x), g_1(x), \ldots, g_{p-1}(x) \} \quad (2)$$

Then k, the dimension of the QC code, is equal to the degree of h(x). In this paper, only binary codes are discussed.

II. NEW BINARY QUASI-CYCLIC CODES

Computer search for good QC codes have been proved to be a good method and lots of QC codes improving lower bounds on minimum distance have been found[3].

The technique used in the this paper was presented first in [1]. Some refinements to reduce the complexities are introduced, and special search interests are paid to the case with m > 32.

With this approach, twelve new good QC codes which improve the lower bounds on the minimum distance [2] have been constructed and many other QC codes which are better than previously known QC codes or as better as the best-known codes are obtained[3]. Table 1 shows the parameters of twelve new QC codes. The column lb – ub gives the previously known lower and upper bounds on the minimum distance of the binary linear codes from the database maintained by Professor Brouwer[2]. The author [3] maintains a web database of binary QC codes (including weight distributions). This database is searchable by block length n, code dimension k, circulant matrix size m, parameter p, and contributor, or any combination of them. For the sake of space, the generator polynomials are omitted in the paper and they can be found in the database.

TABLE 1 NEW QC CODES THAT IMPROVE THE LOWER BOUNDS ON MINIMUM DISTANCE OF A BINARY LINEAR CODE

QC Code	p	m	d	lb-ub
[112, 13]	4	28	48	46-50
[99, 20]	3	33	34	33-39
[102, 17]	3	34	38	37-42
[164, 20]	4	41	62	61-72
[225, 19]	5	45	90	89-102
[153, 16]	3	51	64	62-68
[153, 18]	3	51	62	59-66
[204, 18]	4	51	82	80-92
[165, 20]	3	55	64	62-72
[165, 21]	3	55	62	61-72
[220, 20]	4	55	88	86-97
[220, 21]	4	55	86	85-96

In [4], a binary QC [102, 17] code with d = 37, m = 17 and p = 6 was found. As shown in the Table 1, a binary QC [102, 17] code with d = 38, m = 34, p = 3 and generator polynomials 607703, 11774425325, 4411577731 existed.

REFERENCES

[1] Zhi Chen, "Six new binary quasi-cyclic codes", IEEE Trans. Inform. Theory, vol.IT-40, no.5, pp.1666-1667, Sept. 1994

[2] Bounds on the minimum distance http://www.win.tue.nl/~aeb/voorlincod.html

[3] Web database of binary QC codes http://www.tec.hkr.se/~chen/research/codes/

[4] Petra Heijnen, Henk van Tilborg, Tom Verhoeff, and Sander Weijs, " Some new binary quasi-cyclic codes", IEEE Trans. Inform. Theory, vol. 44, 1994-1996, Sept. 1998

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On a Sequence of Cyclic Codes with Minimum Distance Six

Danyo Danev and Jonas Olsson[1]
Dept. of Electrical Engineering
Linköpings universitet
SE-581 83 Linköping, Sweden
e-mail: {danyo,jonoh}@isy.liu.se

Abstract — **A sequence of q-ary cyclic codes is considered. For each finite field $GF(q)$, $q \geq 4$, there is a code with parameters $[n,k,d;q] = [q(q-1)+1, q(q-1)-6, 6; q]$. We show that all these codes are n-, k- and d-optimal, with only one exception. Also the dual codes are considered. Their true minimum distances are calculated in the range $4 \leq q \leq 29$.**

I. Introduction

Standard terminology from coding theory is used. Cyclic codes are identified with ideals in the ring $GF(q)[x]/(x^n-1)$. The set I consisting of all roots of the generator polynomial $g(x)$ of a given code is referred to as a *defining set*. The minimal polynomial of α^i, where α is a primitive n-th root of unity in an extension field of $GF(q)$, will be denoted $m_i(x)$. Detailed proofs of the given statements can be found in [6].

II. The codes

Let q be a power of a prime. Denote by $\mathcal{C}_q$ the cyclic code of length $n = q(q-1)+1$ over $GF(q)$ with generator polynomial $g(x) = m_0(x)m_1(x)$. The codes $\mathcal{C}_2$ and $\mathcal{C}_3$ are trivial, consisting of the all-zero codeword only. Since $n|(q^6-1)$, then $\alpha \in GF(q^6)$ and the defining set I of $\mathcal{C}_q$ equals $\{\alpha^0, \alpha^1, \alpha^{-1}, \alpha^{(q-1)}, \alpha^{-(q-1)}, \alpha^q, \alpha^{-q}\}$. Thus for $q \geq 4$ the codes $\mathcal{C}_q$ are q-ary BCH codes [1, 2] of dimension $k = q(q-1)-6$ and designed minimum distance 4. But the true minimum distance is actually 6 for all prime powers $q \geq 4$.

Theorem 1 *For every prime power $q \geq 4$ the code $\mathcal{C}_q$ has minimum distance six, i.e. $\mathcal{C}_q$ has parameters $[q(q-1)+1, q(q-1)-6, 6; q]$.*

In the proof results of Roos [3], Van Lint and Wilson [4, p.28] and sphere packing arguments are used.

Define $D_q(n,k)$ and $K_q(n,d)$ to be the *maximal* value of d and k, respectively, for which an $[n,k,d;q]$ code exists. Furthermore, let $N_q(k,d)$ denote the *minimal* value of n for which an $[n,k,d;q]$ code exists. A code is said to be d-, k- or n-optimal if, respectively, $d = D_q(n,k)$, $k = K_q(n,d)$ or $n = N_q(k,d)$. The following statement shows that the codes $\mathcal{C}_q$, $q \geq 4$, are d-, k- and n-optimal with only one exception.

Theorem 2 *The following equalities hold.*

(i) $D_q(q(q-1)+1, q(q-1)-6) = 6$ *for* $q \geq 4$;

(ii) $K_q(q(q-1)+1, 6) = q(q-1)-6$ *for* $q \geq 4$;

(iii) $N_q(q(q-1)-6, 6) = q(q-1)+1$ *for* $q \geq 5$.

[1]This work was partially supported by the Swedish Research Counsil for Engineering Sciences under grant 271-97-554

Nevertheless, for fixed minimum distance d and *redundancy* $r = n-k$, $\mathcal{C}_q$ do not have *maximal information rate* $R = k/n = 1-\frac{r}{n}$ for all $q \geq 4$. It is known that there exist $[20, 13, 6; 4]$ and $[28, 21, 6; 5]$ codes providing two (the only known) examples (see [5, p. 420,435]) of this fact.

III. The dual codes

Let $\mathcal{C}_q^\perp$ denote the $[q(q-1)+1, 7, d^\perp; q]$ dual code of $\mathcal{C}_q$. Then $\mathcal{C}_q^\perp$ has defining set $\{\alpha^2, \alpha^3, \ldots, \alpha^{q-2}, \alpha^{q+1}, \alpha^{q+2}, \ldots, \alpha^{q^2-2q}, \alpha^{q^2-2q+3}, \alpha^{q^2-2q+4}, \ldots, \alpha^{q^2-q-1}\}$. Thus they are BCH codes with designed minimum distance $d_{BCH}^\perp := q^2 - 3q + 1$. Using the computer software MAGMA the true minimum distance $d^\perp$ of $\mathcal{C}_q^\perp$ has been calculated for $q \leq 32$. The result is presented in Table 1 together with $d_{BCH}^\perp$.

Table 1: True minimum distance of $\mathcal{C}_q^\perp$

q	$d^\perp$	$d_{BCH}^\perp$	q	$d^\perp$	$d_{BCH}^\perp$
4	5	5	16	216	209
5	11	11	17	247	239
7	30	29	19	315	305
8	43	41	23	474	461
9	57	55	25	565	551
11	93	89	27	665	649
13	136	131	29	773	755

We note that for $q = 7, 8$ and 9 the entries in our table improve the corresponding lower bounds given in [5, pp. 441-447].

Acknowledgments

The authors would like to thank S.M. Dodunekov for valuable discussions.

References

[1] R. C. Bose and D. K. Ray-Chaudhuri, "On a class of error correcting binary group codes", *Inform. and Control*, vol. 3, pp. 68–79, 1960.

[2] A. Hocquenghem, "Codes correcteurs d'erreurs", *Chiffres (Paris)*, vol. 2, pp. 147–156, 1959.

[3] C. Roos, "A generalization of the BCH bound for cyclic codes, including the Hartmann-Tzeng bound", *J. Combin. Theory Ser. A*, vol. 33, pp. 229–232, 1982.

[4] J. H. van Lint and R. M. Wilson, "On the minimum distance of cyclic codes", *IEEE Trans. Inform. Theory*, vol. IT-32, pp. 23-40, 1986.

[5] V. S. Pless and W. C. Huffman, Editors, *Handbook of Coding Theory*, North-Holland, 1998.

[6] D. Danev and J. Olsson, "On a Sequence of Cyclic Codes with Minimum Distance Six", *IEEE Trans. Inform. Theory*, vol. IT-46, no. 2, 2000.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Design of Provably Good Low-Density Parity Check Codes

Thomas Richardson
Lucent Technologies,
Murray Hill, NJ
tjr@lucent.com

Amin Shokrollahi
Lucent Technologies,
Murray Hill, NJ
amin@research.bell-labs.com

Rüdiger Urbanke
Communications Theory Lab,
EPFL, Lausanne, Switzerland
Rudiger.Urbanke@epfl.ch

Abstract — **We design sequences of low-density parity check codes that provably perform at rates extremely close to the Shannon capacity. These codes are built from highly irregular bipartite graphs with carefully chosen degree patterns on both sides. We further show that under suitable conditions the message densities fulfill a certain symmetry condition which we call the *consistency condition* and we present a *stability condition* which is the most powerful tool to date to bound/determine the threshold of a given family of low-density parity check codes.**

I. Introduction

In this paper we present *irregular* low-density parity check (LDPC) [1,4] codes which exhibit performance extremely close to the best possible as determined by the Shannon capacity formula. These codes are characterized by their *degree sequence pair* $(\lambda(x), \rho(x))$ [2] and a random choice of the connections. For the additive white Gaussian noise channel (AWGNC) the best code of rate one-half presented in this paper has a threshold within 0.06dB from capacity, and simulation results show that our best LDPC code of length 10^6 achieves a bit error probability of 10^{-6} less than 0.13dB away from capacity, beating even the best (turbo) codes known so far.

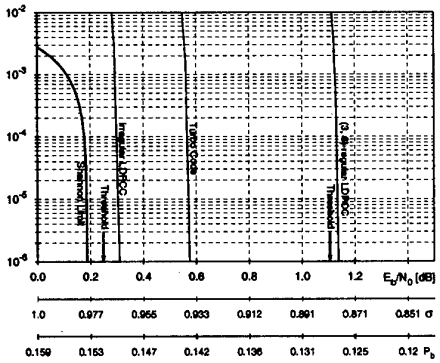


Figure 1: Comparison of (3,6)-regular LDPC code, turbo code, and optimized irregular LDPC code. All codes are of length 10^6 and of rate one-half. The bit error rate for the AWGNC is shown as a function of E_b/N_0 (in dB), the standard deviation σ, as well as the raw input bit error probability P_b.

II. Analytic Properties of Density Evolution

Assume we employ a message passing decoder on an infinitely long LDPC code. Let P_ℓ denote the distribution of messages emitted from the variable nodes at the ℓ-th iteration assuming that the all-one codeword was transmitted. The sequence of distributions P_ℓ and their determination is collectively referred to as *density evolution* [2].

In the following, we call a distribution f on $\bar{\mathsf{R}}$ *consistent* if it satisfies $f(x) = f(-x)e^x$ for all $x \in \bar{\mathsf{R}}^+$. For example, a Gaussian density is consistent iff its mean μ and variance σ^2 are related by $\sigma^2 = 2\mu$. The following theorem can often be used to achieve significant speed-ups and improved accuracy in the determination of these message distributions.

Theorem 1 *Suppose that a binary-input channel has symmetry property $p(y \mid x = 1) = p(-y \mid x = -1)$. Under the all-one codeword assumption let P_ℓ denote the message distribution of a belief-propagation decoder at the ℓ-th iteration, where all messages are assumed to be in log-likelihood ratio form. Then P_ℓ is consistent.*

Assume that after some iterations the number of remaining errors is fairly small. Will the number of errors converge to zero if we proceed with further iteration rounds or will it stay bounded away from zero regardless of the number of iterations? This is answered in

Theorem 2 *Let $g(s)$ be the moment generating function corresponding to the initial message distribution $P_0(x)$, i.e., $g(s) = E_{P_0}[e^{sX}]$, and assume that $g(s) < \infty$ for all s in some neighborhood of zero. Define $r = -\log(\inf_{s<0} g(s))$ which for consistent initial message distributions P_0 simplifies to $r = -\log\left(2\int_0^\infty P_0(x)\, e^{-x/2}\, dx\right)$. If $\lambda'(0)\rho'(1) > e^r$, then the probability of error of density evolution is strictly bounded away from 0. Conversely, if $\lambda'(0)\rho'(1) < e^r$, then there exists $\epsilon > 0$ such that if density evolution is initialized with a consistent message distribution P satisfying $\Pr_{err}(P) < \epsilon$, then the probability of error will converge to zero under density evolution.*

For the binary erasure channel, the binary symmetric channel and the additive white Gaussian noise channel we have $e^r = \frac{1}{\delta}$, $e^r = \frac{1}{2\sqrt{\epsilon(1-\epsilon)}}$, and $e^r = e^{\frac{1}{2\sigma^2}}$, respectively.

III. Optimization

By optimizing the degree sequence pair $(\lambda(x), \rho(x))$ we have found ensembles of irregular LDPC codes with thresholds extremely close to capacity for a wide range of rates and channels [3].

References

[1] R. Gallager, "Low-Density Parity-Check Codes," Cambridge, Massachusetts: M.I.T. Press, 1963.

[2] T. Richardson and R. Urbanke, "The Capacity of Low-Density Parity-Check Codes under Message Passing Decoding," submitted IEEE IT, 1999.

[3] T. Richardson, A. Shokrollahi and R. Urbanke, "Design of Provably Good Low-Density Parity-Check Codes," submitted IEEE IT, 1999.

[4] M. Luby, M. Mitzenmacher, A. Shokrollahi, and D. Spielman, "Analysis of Low-Density Codes and Improved Designs Using Irregular Graphs," in Proceedings of the 30th Annual ACM Symposium on Theory of Computing, 1998, pp. 249–258.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Low Density Parity Check Codes Based on Finite Geometries: A Rediscovery

Yu Kou and Shu Lin[1]
Department of Electrical and Computer Engineering
University of California, Davis
Davis, CA 95616, U.S.A.
Email: shulin@ece.ucdavis.edu

Marc P.C. Fossorier
Department of Electrical Engineering
University of Hawaii at Manoa
Honolulu, HI 96822 U.S.A.
Email marc@spectra.eng.hawaii.edu

I. Introduction

LDPC codes [1] with iterative decoding based on belief-propagation (IDBP) have been shown to achieve astonishing error performance [2]. But no algebraic or geometric method has been found for constructing these codes. Codes that have been found are largely computer generated, especially long codes. In this paper, we present two classes of high rate LDPC codes whose constructions are based on the lines of two-dimensional finite Euclidean and projective geometries, respectively.

II. Codes Constructed Based on Two-dimensional Finite Geometries

Regard the Galois field GF(2^{2s}) as the two-dimensional Euclidean geometry EG(2,2^s) over GF(2^s) [3]. Let α be a primitive element of GF(2^{2s}). Then $\alpha^\infty=0, \alpha^0=1, \alpha^1, \alpha^2, ..., \alpha^{2^{2s}-2}$ form all the points of EG(2,2^s). The zero element 0 is called the origin of EG(2,2^s). Every line in EG(2,2^s) consists of 2^s points. For a given point α^i in EG(2,2^s), there are 2^s+1 lines intersect at α^i. Let $\mathbf{v} = (v_0, v_1, \ldots, v_{2^{2s}-2})$ be a $(2^{2s}-1)$-tuple over GF(2). Number the components of $\mathbf{v}$ with the nonzero elements of GF(2^{2s}) as follows: the component v_i is numbered α^i for $0 \leq i \leq 2^{2s}-2$. Hence, α^i is the location number of v_i. Let $\mathcal{L}$ be a line in EG(2,2^s) that does not pass through the origin α^∞. Based on $\mathcal{L}$, form a binary $(2^{2s}-1)$-tuple as follows: $\mathbf{v}_\mathcal{L} = (v_0, v_1, \ldots, v_{2^{2s}-2})$ whose i-th component v_i is 1 if and only if its location number α^i is a point on $\mathcal{L}$. This vector $\mathbf{v}_\mathcal{L}$ is called the incidence vector of line $\mathcal{L}$. Now form a $(2^{2s}-1) \times (2^{2s}-1)$ matrix $\mathbf{H}$ with $\mathbf{v}_\mathcal{L}$ and its $2^{2s}-2$ cyclic shifts as rows. The rows of $\mathbf{H}$ are the incidence vectors of the $2^{2s}-1$ distinct lines in EG(2,2^s) which do not pass the origin, and the columns of $\mathbf{H}$ correspond to the $2^{2s}-1$ non-origin points of EG(2, 2^s). The ratio of the total number of ones to the total number of entries in $\mathbf{H}$ matrix, called the density, is $r = 2^s/(2^{2s}-1)$. Let $\mathbf{C}$ be the null space of $\mathbf{H}$. Then $\mathbf{C}$ is a LDPC code of length $n = 2^{2s}-1$. It is cyclic and its generator polynomial is completely characterized by its roots in GF(2^{2s}). It has $n-k = 3^s-1$ parity check bits and a minimum distance $d_{min} = 2^s+1$.

Similarly LDPC codes can also be constructed based on the lines of the two-dimensional projective geometry PG(2,2^s). This construction results in a class of PG-LDPC codes which are also cyclic.

Since both EG- and PG-LDPC codes are cyclic, their encoding is extremely simple. This is a contrast to the complex encoding of long computer generated LDPC codes. For iterative decoding of these cyclic LDPC codes, error detection at the end of each decoding iteration can also be achieved easily with a simple shift register.

[1]This research was supported by NSF under Grants CCR 94-15374 and CCR 98-14054 and NASA under Grants NAG 5-931 and NAG 5-8414.

III. Extension and Puncturing

A 2-dimensional EG- or PG-LDPC code can be extended by splitting each column $\mathbf{h}$ of its parity-check matrix $\mathbf{H}$ into q columns, $\mathbf{h}_1, \mathbf{h}_2, ..., \mathbf{h}_q$, with the "ones" of $\mathbf{h}$ distributed among $\mathbf{h}_1, \mathbf{h}_2, \cdots, \mathbf{h}_q$ (evenly or not evenly). This results in a low-density matrix $\mathbf{H}_{ext}$ with $q(2^{2s}-1)$ columns and density $r = 2^s/(q(2^{2s}-1))$. The null space $\mathbf{C}_{ext}$ of $\mathbf{H}_{ext}$ is also a LDPC code and is quasi-cyclic. Finite geometry LDPC codes can also be punctured in various ways to obtain good LDPC codes. We can remove columns of the parity-check matrix $\mathbf{H}$ correspond to the points on a line or a set of lines. Puncturing can also be achieved with combination of removing columns and rows of $\mathbf{H}$.

IV. Error Performance

EG- and PG-LDPC codes and their extended codes with IDBP achieve very good performance. As an example, let $m = 2$ and $s = 6$. There exists a (4095,3367) EG-LDPC code. The error performance of this code with IDBP is shown in Figure 1-(a). Suppose we split each column of the parity check matrix of this code into 16 columns. This column splitting results in a (65520,61425) extended EG-LDPC code. Using IDBP, this code achieves an error performance only 0.3dB away from Shannon limit, shown in Figure 1-(b).

References

[1] R. G. Gallager,"Low Density Parity Check Codes," *IRE Transactions on Information Theory*, IT-8, pp. 21-28, January 1962.

[2] D. J. C. MacKay,"Good Error-Correcting Codes Based on Very Sparse Matrices," *IEEE Transactions on Information Theory*, IT-45, pp.399-432, March 1999.

[3] S. Lin and D. J. Costello, Jr., *Error Control Coding: Fundamentals and Applications*, Prentice Hall, Englewood Cliffs, New Jersey, 1983.

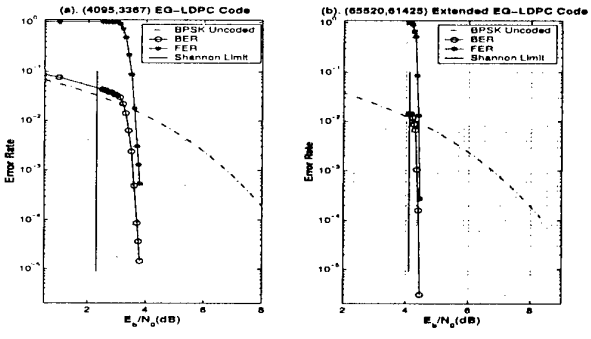


Figure 1: (a).Bit- and frame-error probabilities of the (4095,3367) EG-LDPC code. (b).Bit- and frame-error probabilities of the (65520,61425) Extended EG-LDPC code.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Analytical Approach to Low-Density Convolutional Codes[1]

K. Engdahl, M. Lentmaier, D. V. Truhachev, and K. Sh. Zigangirov
Department of Information Technology
Lund University, Box 118, SE-221 00 Lund, Sweden
e-mail: karin,michael,dimitri,kamil@it.lth.se

Abstract — **A statistical analysis of low-density convolutional (LDC) codes is performed. This analysis is based on the consideration of a special statistical ensemble of Markov scramblers and the solution to a system of recurrent equations describing this ensemble. The results of the analysis are lower bounds for the free distance of the codes and upper bounds for the maximum likelihood decoding error probability. For the case where the size of the scrambler tends to infinity some asymptotic bounds for the free distance and the error probability are derived. Simulation results for iterative decoding of LDC codes are also presented.**

Low-density convolutional (LDC) codes were introduced by Jimenez and Zigangirov [1] and the theory of these codes was further developed in the first part of the paper [3]. The LDC codes have some common features in comparison with low-density block codes, invented by Gallager [2], but at the same time there are differences, which arise from the recurrent nature of LDC codes. Particularly, the iterative decoding of LDC codes can be performed by a pipeline implementation.

The main goal of this paper is to demonstrate the possibility to get bounds on performances of LDC codes, similar to bounds for conventional convolutional codes, by the introduction of a special ensemble of Markov scramblers and application of Markov chain theory (see also [4]).

We have studied two classes of LDC codes, A and B. In class A, a rate $R_s = d/c$ convolutional scrambler is followed by a rate $R_b = (d-1)/d$ degenerated component convolutional encoder of memory zero. (It calculates one parity-check symbol to $d-1$ input symbols.) The resulting LDC code is a homogeneous $(d(1-R), d)$-code.

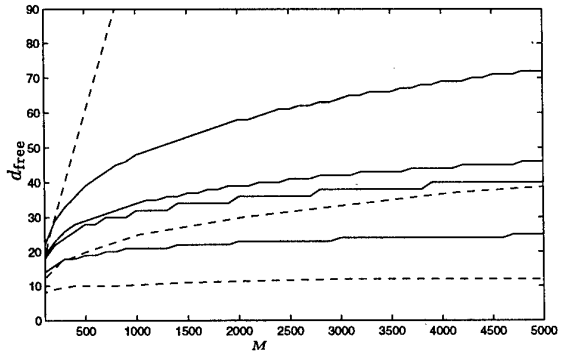


Fig. 1: Lower bounds on the free distance. The dashed lines correspond to (from bottom to top) (2,4), (2.5,5) and (3,6) codes of class A. The solid lines correspond to class B codes with component code memory 2,3,4 and 5.

[1]This work was supported in part by Swedish Research Council for Engineering Sciences under Grant 98-216.

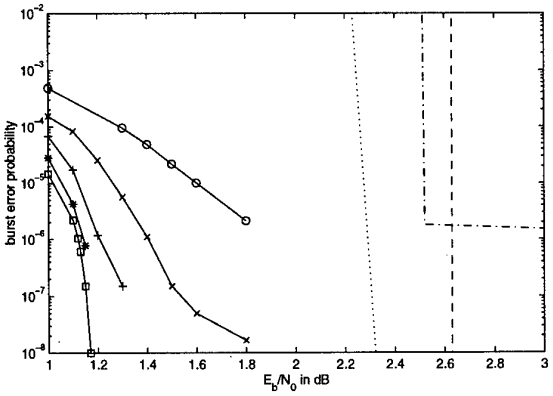


Fig. 2: Burst error probabilities for (3,6)-codes. The solid lines show (from top to bottom) simulation results for $m_s = 129, 257, 513, 1025, 2049, 4097$. The size of the scrambler is $M = 2.5(m_s - 1)$. The union bound (dashed-dotted) and the expurgated bound (dotted) are shown for $m_s = 129$. The vertical dashed line shows the cut-off rate limit.

In class B, a rate $R_s = d/c$ convolutional scrambler is followed by a rate $R_b = (d-c+b)/d$ component convolutional encoder. To simplify the description in this paper we consider only rate $R = 1/2$ LDC codes.

In Fig. 1 lower bounds on the free distance of some different codes are given as a function of the scrambler size M. It is worth to note that the bound grows linearly with M for the LDC (3,6)-codes of class A and only logarithmically for the other considered codes. Upper bounds on the burst error probability, together with simulation results of iterative decoding, are presented in Fig. 2. For the asymptotic case we proved, that there exists an LDC (3,6)-code (LDC (2,4)-code, respectively) of memory size M, for which the burst error probability decreases at least as $O(1/M^2)$ $(O(1/M))$, $M \to \infty$, for signal to noise ratios $E_b/N_0 \geq 2.63$ dB (3.58 dB). In analogy with conventional convolutional codes we can call the limit values of E_b/N_0 *cut-off rate limit.*

References

[1] A. Jimenez and K. Sh. Zigangirov, "Periodic Time-Varying Convolutional Codes with Low-Density Parity-Check Matrices", *IEEE Trans. on Inform. Theory*, vol. IT-45, no. 5, Sept. 1999.

[2] R. G. Gallager, *Low-Density Parity-Check Codes*, M.I.T. Press, Cambridge, Massachusetts, 1963.

[3] K. Engdahl and K. Sh. Zigangirov, "On the Theory of Low-Density Convolutional Codes I", *Probl. Peredach. Inform.*, vol. 35, no. 4, Oct-Nov-Dec 1999.
(see http://www.it.lth.se/~karin)

[4] K. Engdahl, M. Lentmaier and K. Sh. Zigangirov, "On the Theory of Low-Density Convolutional Codes", Proc. AAECC-13, *Lecture Notes in Computer Science*, vol. 1719, Springer, 1999, pp. 77-86.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On Gallager's Low-Density Parity-Check Codes

Gérard Battail[1]
E.N.S.T., 46 rue Barrault,
75634 Paris Cedex 13, France
gbattail@club-internet.fr

Abstract — **We show that low-density parity-check codes are random-like, and we comment this result.**

I. Introduction

Gallager's low-density parity-check (LDPC) codes [1] attract renewed interest. MacKay has recently shown that LDPC codes are indeed good in a precise meaning [2].

Why does the low-density of some parity-check matrix result in a good code, whereas most of its linearly equivalent matrices are not of low density? We show that such codes are actually random-like (RL) i.e., their weight distribution resembles that obtained in the average by random coding [3], an intrinsic property of the code, not of a peculiar matrix.

II. Density in a Systematic-Form Matrix

Let a binary matrix M have n m-bit columns of the same constant weight $j > 1$, but otherwise random and mutually independent. Assuming M of full rank, it can be transformed into an equivalent systematic matrix $M_{\rm sys} = [Q \;\; I_m]$ (I_m is the m-order unity matrix, the submatrix Q has $n-m$ columns and m rows) using the Gaussian elimination process.

Let ρ_i denote the average density of the $n-i$ columns not yet reduced to a single 1 after the i-th step of the elimination process. At its last step (the m-th), these columns make up submatrix Q so its density is ρ_m. Interpreting ρ_i as the probability of having a 1 at any given location, we obtain the recursion formula:

$$\rho_i = \rho_{i-1}[1 - 1/m + (1 + 2/m)\rho_{i-1} - 2\rho_{i-1}^2]. \qquad (1)$$

Assume first that i may increase indefinitely. According to (1), the asymptotic value ρ_∞ of the density is a root of the polynomial $(1/2 - \rho)(\rho - 1/m)$. The right hand side of (1) is an increasing function of i for $1/m < \rho_{i-1} < 1/2$ so $\rho_\infty = 1/2$ provided $\rho_0 > 1/m$, but the increase in ρ_i is limited by the maximum number of steps m. For m approaching infinity, ρ_m thus approaches $1/2$. For a finite value of m, ρ_m is an increasing function of $\rho_0 = j/m$. Even for the lowest possible value $j = 2$, numerical computation shows that densities close to $1/2$ are obtained even for moderate values of m (e.g., for $m = 50$ and $m = 100$, the computed density of Q with $j = 2$ is 0.49715 and 0.49999966, respectively). If $\rho_0 = 1/2$, then $\rho_i = 1/2, \forall i$. Anyhow, Q is random insofar as M itself is so.

Since the proof only involves average densities, it applies as well to non-constant column weight matrices provided no column weight is allowed to become less than 2.

III. Application to LDPC and Linear RL Codes

Let the parity-check matrix $H_{\rm ld}$ of an (n, k) linear code be a matrix M as in the previous section, resulting in an LDPC code. The systematic matrix equivalent to $H_{\rm ld}$ is:

$$H_{\rm sys} = [P^{\rm t} \;\; I_{n-k}], \qquad (2)$$

where the superscript t denotes transposition. Then, P is random with density close to $1/2$ if $n - k$ is large enough, as will be assumed throughout. The corresponding systematic generator matrix is $G_{\rm sys} = [I_k \;\; P]$, with P same as in (2).

The actual implementation of easily decodable LDPC codes leads to additional constraints which may weaken the randomness of P. Similarly, some constraints on the columns of $P^{\rm t}$ will be needed for obtaining a large minimum distance (e.g., $j = 2$ results in $d_{\min} = 3$, so larger j will be preferred).

For designing an (n, k) linear binary code *at random*, we may choose each entry of its generator matrix G independently of the others with probability $1/2$. With high probability, we thus obtain a matrix of rank k and effective length n (i.e., no column weight is 0) which generates a code with a distance distribution close to that obtained in the average by random coding. Assume furthermore that we demand that no column weight of G is less than 2. Then, applying the result of section II to G, submatrix P is random with density $1/2$. Instead of the full matrix G, it suffices to randomly generate the nonunity submatrix P with density $1/2$. But section II shows that we may as well restrict ourselves to generate at random a low-density parity-check matrix $H_{\rm ld}$ or generator $G_{\rm ld}$.

For designing a *random-like code*, we have to replace truly random binary variables by pseudo-random ones. They have the average properties of random variables, but are generated by deterministic means which enable to fulfil the above conditions. We may still generate either the submatrix P with density $1/2$, or one of the low-density matrices $H_{\rm ld}$ and $G_{\rm ld}$. Doing so, we only obtain a weight distribution close to that of random coding i.e., a *weakly RL* code [3]. Additional constraints may be needed to ensure a large minimum distance.

IV. Remark on the Weight Distribution

The normalized weight distribution of the codewords obtained by drawing G at random is Bernoulli of mean $n/2$. When P in the matrix $G_{\rm sys}$ is drawn at random, almost the same result is obtained. The unity submatrix and P both contribute Bernoulli distributions, of means $k/2$ and $(n-k)/2$ respectively, as if the information and parity vectors were independent. Of course, they are not, but their relation is as *complicated* as to make them behave as if they were so. Specifying a submatrix P involves $k(n-k)$ binary choices, so the information and parity vectors are associated according to a specific rule among as many as $2^{k(n-k)}$ possible ones.

References

[1] R.G. Gallager, "Low-density parity-check codes", *IRE Trans. Inform. Theory*, Vol. IT-8, No. 1, pp. 21–28, Jan. 1962.

[2] D.J.C. MacKay, "Good error-correcting codes based on very sparce matrices", *IEEE Trans. Inform. Theory*, Vol. 45, No. 2; pp. 399–431, March 1999.

[3] G. Battail, "On random-like codes," *Information Theory and Applications II*, Lecture Notes in Computer Science No. 1133, pp. 76–94, Springer, 1996.

[1] Retired

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Exact Thresholds and Optimal Codes for the Binary Symmetric Channel and Gallager's Decoding Algorithm A

L. Bazzi[1]
LIDS
MIT
e-mail: louay@mit.edu

T. Richardson
Lucent Technologies,
Murray Hill, NJ
e-mail: tjr@lucent.com

R. Urbanke
Communications Theory Lab,
EPFL, Lausanne, Switzerland
e-mail:Rudiger.Urbanke@epfl.ch

Abstract — **We show that for the case of a binary symmetric channel and Gallager's decoding algorithm A the threshold can, in many cases, be determined analytically. We further present optimal codes for a large range of rates.**

I. Introduction

Let x_0 be the expected number of initial errors, i.e., x_0 equals the cross-over probability of the binary symmetric channel. It was shown by Gallager [1] that the expected number of errors (under the independence assumption) in the l-th iteration is given by the recursion

$$x_l = x_0 - x_0 p^+(x_{l-1}) + (1 - x_0) p^-(x_{l-1}), \qquad (1)$$

where

$$p^+(x) := \lambda\left(\frac{1+\rho(1-2x)}{2}\right),$$

$$p^-(x) := \lambda\left(\frac{1-\rho(1-2x)}{2}\right),$$

and where $(\lambda(x), \rho(x))$ is the degree sequence pair.

The threshold x_0^* is the supremum of all x_0 in R^+ such that $x_l(x_0)$ as defined in (1) converges to zero as l tends to infinity.

II. Exact Thresholds

Lemma 1 Let τ denote the smallest positive real root of the polynomial $p(x) := xp^+(x) + (x-1)p^-(x)$ and assume that $\lambda_2\rho'(1) < 1$. Then $x_0^* \le X_0^* := \min\{\frac{1-\lambda_2\rho'(1)}{\lambda'(1)\rho'(1)-\lambda_2\rho'(1)}, \tau\}$.

We note that, although one can construct counterexamples, for most codes one has $x_0^* = X_0^*$. Table 1 summarizes thresholds of some standard regular codes for all of which one has $x_0^* = X_0^*$.

III. Optimal Codes

Given the ease with which thresholds can be determined, one might wonder whether optimal codes for the given decoder can be found. This is indeed the case. In a nutshell, one can show that for a wide range of rates the optimal codes for Gallager's decoding algorithm A are *left and right concentrated*, i.e., these codes have at most two non-zero (left or right) degrees and these non-zero degrees are consecutive. Fig. 1 shows the achievable thresholds as a function of the rate for the optimal concentrated degree sequences. The solid curve corresponds to the capacity formula $r = 1 - h(x_0^*)$. The dashed curve corresponds to the optimal concentrated degree sequence pairs. Note that over the whole range the optimal concentrated codes can achieve roughly half of capacity. Our main result now states that above a rate of roughly 2/5 these optimal *concentrated* codes are optimal. This implies that for these rates optimal codes and their thresholds can be found analytically.

[1]This work was performed while the first author was a summer intern at Bell Labs.

d_l	d_r	Rate	x_0^*
3	6	0.5	$\tau_{(3,6)} \sim 0.0394636562$
4	8	0.5	$\frac{1}{21}$
5	10	0.5	$\frac{1}{36}$
3	5	0.4	$\tau_{(3,5)} \sim 0.0611860546$
4	6	0.333	$\frac{1}{15}$
3	4	0.25	$\tau_{(3,4)} = \frac{2-\sqrt{2\left(-1+\sqrt{5}\right)}}{4}$

Table 1: Thresholds for the binary symmetric channel and Gallager's decoding algorithm A for some standard regular codes.

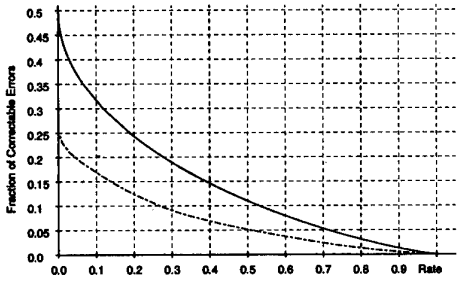


Figure 1: The solid curve corresponds to the capacity formula $r = 1 - h(x_0^*)$ whereas the dashed curve corresponds to the optimal concentrated codes.

References

[1] R. Gallager, "Low-Density Parity-Check Codes," Cambridge, Massachusetts: M.I.T. Press, 1963.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Solving Lattice Codebook Enumeration Problem for Generalized Gaussian Sources

P. Loyer (pierre.loyer@space.alcatel.fr) , J.M. Moureaux (moureaux@cran.u-nancy.fr), M. Antonini (am@i3s.unice.fr)

Abstract — **In the context of lattice quantization of a generalized gaussian source, with idependantly identically distributed signal values, a low complexity indexing algorithm, based on a geometrical approach, is proposed.**

I. Introduction

Signal vectors are distributed according to a probability density function (pdf) of the kind $\alpha \exp\left(-\beta\sum_{i=1}^{n}|x_i|^p\right)$. As a codebook, we take the intersection of surfaces of constant pdf with the cubic lattice.

Recently, Chen and al. [Chen97] proposed algorithms for quantizing to the Z^n lattice with a boundary well suited to this pdf. Unfortunately, when p is different from 1 or 2, enumerating or indexing lattice points reveals difficult [Chen97].

Our main contribution in this work is to propose a low complexity enumeration algorithm based on a geometrical interpretation and valid for values of p in the range $0 < p \le 2$. This point of view offers various advantages and particularly it enables one to reduce the algorithm to the calculation of a few convolutional products.

II. Mathematical Preliminaries

The L_p - norm of the vector $\vec{x}$ is $L_p(\vec{x})=\left(\sum_{i=1}^{n}|x_i|^p\right)^{1/p}$. In the subspace of the k first coordinates, we define the L_p - sphere of center c and radius R

$$S_k(c,R)=\left\{\vec{x}/L_p(c,\vec{x})\le R\right\} \qquad \textbf{Eq. 1}$$

and similarly the surface of the L_p - sphere $\overline{S}_k(c,R)$. We will use as well the word sphere for both $S_k(c,R)$ or $\overline{S}_k(c,R)$. The number p is omitted for the sake of simplicity of notations.

The (generalized) theta-function of the lattice $\mathbf{Z}^n$ is the generating function associated to the series $\left(\#\overline{S}_n(k^{\frac{1}{p}})\right)_{k=0\ldots\infty}$:

$$\theta_n(z)=\sum_{k=0}^{\infty}\#\overline{S}_n(k^{\frac{1}{p}})z^k. \qquad \textbf{Eq. 2}$$

We have

$$\theta_{n+1}(z)=\theta_n(z)\theta_1(z). \qquad \textbf{Eq. 3}$$

This recursive formula enables one to derive all theta-functions from $\theta_1(z)$. As a corollary, the term of index k of $\theta_{n+1}(z)$ is the convolutional product of the terms of $\vartheta_1(z)$ and $\theta_n(z)$ up to the index k.

The coefficient of the generic term of the theta-function counts the number of points with an energy $k = R^p$. It is easy to derive an enumeration algorithm from a counting algorithm. Assuming that points are ordered some way, we associate as a number to a given point the number of points which preceed it. Here, we order points from inside to outside of spheres and from the bottom to the top of the last axis.

III. Principle of Coding

We will focus on the index calculation at a given energy.

Any hyperplane $x_n = cte, |cte| \le R$, an integer, cuts $\overline{S}_n(R)$ in a n-1-dimensional sphere of radius $\left(R^p-|cte|^p\right)^{1/p}$. Thus, a sphere in dimension n can be seen as a stack of spheres in dimension n-1 along the last coordinate axis (say). This can be written as

$$\overline{S}_n(R)=\bigcup_{x_n=-\lfloor R\rfloor}^{\lfloor R\rfloor}\left(\overline{S}_{n-1}\left(\sqrt[p]{R^p-|x_n|^p}\right)+x_n\vec{e}_n\right). \qquad \textbf{Eq. 4}$$

Hence, the n-1-dimensional spheres being disjoined, we can deduce a recursive formula

$$\#\overline{S}_n(R)=\sum_{x_n=-\lfloor R\rfloor}^{\lfloor R\rfloor}\#\overline{S}_{n-1}\left(\sqrt[p]{R^p-|x_n|^p}\right). \qquad \textbf{Eq. 5}$$

IV. Algorithm

Given a point to be numbered $M(x_1,\ldots,x_n)$. Set $M_k(x_1,\ldots,x_k)$ and $R_k^p=\sum_{i=1}^{k}|x_i|^p$. We want to compute N the index associated to M. This index appears to be the sum of the number of points below M_k for every k. Thus we define a function named Number which counts the points below M_k in the space of the k first coordinates. It proceeds by adding up the cardinality of the layers under M_k. These cardinalities are computed by the means of theta-functions.

V. References

[Chen97] F. Chen, Z. Gao, J. Villasenor, "Lattice Vector Quantization of Generalized Gaussian Sources", *IEEE Transactions on Information Theory*, Vol.43, no.1, pp. 92-103, January 1997.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Successive Refinement of Information with Reliability Criterion

Evgueni A. Haroutunian[1]
Institute for Informatics and Automation Problems
of the Armenian National Academy
of Sciences and of the Yerevan State University
P. Sevak 1, 375044, Yerevan, Armenia
e-mail: evhar@ipia.sci.am

Ashot N. Harutyunyan[1]
Institute for Informatics and Automation Problems
of the Armenian National Academy
of Sciences and of the Yerevan State University
P. Sevak 1, 375044, Yerevan, Armenia
e-mail: ashar@ipia.sci.am

Abstract — **An generalized notion of source divisibility or in other words successive refinement of information with additional requirement of exponential decrease of error probability is considered. A condition necessary and sufficient for possibility of such successive refinement is established.**

I. Introduction

The idea of *source divisibility* or *successive refinement of information* developed in works of Koshelev [1]-[3], Equitz and Cover [4], Rimoldi [5] and other authors. We generalize the concept adding the requirement of reliability.

Let the probability distribution (PD) of messages of the discrete memoryless source $\{X\}$ is $P^* = \{P^*(x), x \in \mathcal{X}\}$, where a finite set $\mathcal{X}$ is the alphabet of the source. Reproduction alphabets of receivers are $\mathcal{X}^1$ and $\mathcal{X}^2$ and the corresponding single-letter distortion measures are $d_k : \mathcal{X} \times \mathcal{X}^k \to [0; \infty)$, $k = 1, 2$. Distortions $d_k(\mathbf{x}, \mathbf{x}^k)$ $(k = 1, 2)$ between source N-length message vector $\mathbf{x}$ and its reproducted versions $\mathbf{x}^k$ are considered as averages of per-letter distortions.

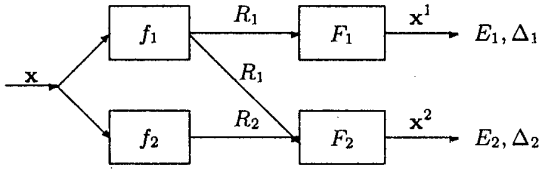


Fig. 1. Two-level communication system.

A code $(f, F) = (f_1, f_2, F_1, F_2)$ for the system consists of encoders: $f_k : \mathcal{X}^N \to \{1, 2, ..., L_k(N)\}$, $k = 1, 2$, and decoders: $F_1 : \{1, 2, ..., L_1(N)\} \to (\mathcal{X}^1)^N$,

$$F_2 : \{1, 2, ..., L_1(N)\} \times \{1, 2, ..., L_2(N)\} \to (\mathcal{X}^2)^N.$$

The probabilities of the sets of source vectors $\mathbf{x}$ which are reconstructed (using a code (f, F)) out of the permissible distortion levels Δ_1 and Δ_2 at each destination are denoted by $e_k(f, F, \Delta_k, N) = e_k$, $k = 1, 2$.

Let $\mathbf{E} = (E_1, E_2)$, $\mathbf{\Delta} = (\Delta_1, \Delta_2)$. A pair of rates (R_1, R_2) $(R_k \geq 0, k = 1, 2)$ is called $(\mathbf{E}, \mathbf{\Delta})$-achievable for reliabilities $E_k > 0$, distortion levels $\Delta_k \geq 0$, $k = 1, 2$, if for every $\epsilon > 0$ and sufficiently large N there exists a code (f, F), such that

$$N^{-1} \log L_k(N) \leq R_k + \epsilon, \; e_k \leq \exp\{-NE_k\} \; k = 1, 2.$$

II. Divisibility of source with reliability

Let P be a PD on $\mathcal{X}$, $Q = \{Q(x^1, x^2|x)\}$ be a conditional PD on $\mathcal{X}^1 \times \mathcal{X}^2$ and $Q(x^k|x)$ be the corresponding marginal PD. Denote by $D(P \parallel P^*)$ the divergence of PD P and P^* and $\alpha(E_k) = \{P : D(P \parallel P^*) \leq E_k\}$, $k = 1, 2$.

[1]This work was supported by INTAS Grant 94-469.

Consider a function $\Phi(P, \mathbf{E}, \mathbf{\Delta})$, values of which are such conditional PD Q corresponding to a PD P that for a given $\mathbf{\Delta}$ if $P \in \alpha(E_1)$ then $\mathbf{E}_{P,Q} d_k(X, X^k) = \sum_{x, x^k} P(x)Q(x^k|x)d(x, x^k) \leq \Delta_k$, $x \in \mathcal{X}$, $x^k \in \mathcal{X}^k$, $k = 1, 2$, and if $P \in \alpha(E_2) - \alpha(E_1)$ then the last inequality holds only for $k = 2$. Let $\mathcal{M}(P, \mathbf{E}, \mathbf{\Delta})$ is the collection of all such functions $\Phi(P, \mathbf{E}, \mathbf{\Delta})$ for given $\mathbf{E}, \mathbf{\Delta}$ and P.

The rate-reliability-distortion function $R(E_k, \Delta_k)$, $k = 1, 2$, which is the minimal achievable rate for one terminal source code ensuring reconstruction of messages with requirement of reliability E_k and distortion level Δ_k, is known [6]:

$$R(E_k, \Delta_k) = \max_{P \in \alpha(E_k)} \min_{Q : E_{P,Q} d_k(X, X^k) \leq \Delta_k} I_{P,Q}(X \wedge X^k).$$

Definition. Successive refinement from a level (E_1, Δ_1) to (E_2, Δ_2), for $\Delta_1 \geq \Delta_2$ and $E_1 \leq E_2$ is the $(\mathbf{E}, \mathbf{\Delta})$-achievability of the pair of rates $(R(E_1, \Delta_1), R(E_2, \Delta_2) - R(E_1, \Delta_1))$.

III. Necessary and sufficient condition

Theorem. For the considered multilevel system (Fig. 1) the successive refinement takes place iff there exist pairs of PD $P_1 \in \alpha(E_1), Q_1 \in \mathcal{M}(P_1, \mathbf{E}, \mathbf{\Delta})$ and $P_2 \in \alpha(E_1), Q_2 \in \mathcal{M}(P_2, \mathbf{E}, \mathbf{\Delta})$, such that

$$R(E_1, \Delta_1) = I_{P_1,Q_1}(X \wedge X^1), \; R(E_2, \Delta_2) = I_{P_2,Q_2}(X \wedge X^2),$$

and the random variables (RV) X, X^2, X^1 form a Markov chain $X_{P_2} \to X^2 \to X^1$, where X_{P_2} is the RV X with the distribution P_2.

Corollary. When the receivers requirements on reliability are absent, i. e. $E_1 = E_2 \to 0$, the result of Equitz and Cover from [4] follows.

References

[1] V. N. Koshelev, "Multilevel source coding and data-transmission theorem", in *Proc. VII All-Union Conf. on Theory of Coding and Data Transm.*, Vilnius, U.S.S.R., pt. 1, pp. 85–92, 1978.

[2] V. N. Koshelev, "Hierarchical coding of discrete sources", *Problemy peredachi informatsii*, vol. 16, no. 3, pp. 31–49, (in Russian), 1980.

[3] V. N. Koshelev, "On divisibility of discrete sources with the single-letter-additive measure of distortion", *Problemy peredachi informatsii*, vol. 30, no. 1, pp. 31–50, (in Russian), 1994.

[4] W. H. R. Equitz and T. M. Cover, "Successive Refinement of Information", *IEEE Trans. on Inform Theory*, vol. IT–37, no. 2, pp. 269–275, March 1991.

[5] B. Rimoldi, "Successive Refinement of Information: Characterization of the Achievable Rates", *IEEE Trans. on Inform Theory*, vol. IT–40, no. 1, pp. 253–259, January 1991.

[6] E. A. Haroutunian and B. Mekoush, "Estimates of optimal rates of codes with given error probability exponent for certain sources", (in Russian), Abstr. of Sixth Int. Symposium on Inform. Theory, Tashkent, vol. 1, pp. 22-23, 1984.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Approximation of the Resource Bounded Complexity Distortion Function

Daby Sow and Alexandros Eleftheriadis
Dept. of Electrical Engineering
Columbia University
500 West 120th Street, code 4712
New York, New York, 10027
e-mail:
{daby,eleft}@ee.columbia.edu

I. Introduction

This work addresses the coding of finite binary sequences with a finite amount of decoding computational resources. In this setting, we propose a general coding methodology and discuss its convergence properties.

II. Resource Bounded Complexity Distortion

Consider Shannon's traditional communication system where the source decoder is replaced by a universal Turing machine Ψ. Ψ also denotes a recursive function from $P = B^n = \prod_{i=1}^{n}\{0,1\}$ to B^n if programs are also represented by binary sequences. By $\cdot\Psi^{t,s}(p), p \in P$, we denote the execution of program p on Ψ using less than t execution steps and less than s memory cells. In this setting, it is natural to measure the performances of the encoder with the Resource Bounded Complexity Distortion Function [3] defined by: $C_D^{t,s}(x_1^n) = \frac{K^{t,s}(Q_D^{t,s}(x_1^n))}{n}$ where $x_1^n \in B^n$, $K^{t,s}(\cdot)$ is the Resource Bounded Kolmogorov Complexity [1] and $Q_D^{t,s}(x_1^n) = \arg\min_{y_1^n \in B^n; d_n(x_1^n, y_1^n) \leq D} K^{t,s}(y_1^n)$, D being a distortion constraint according to a distortion measure $d_n(\cdot,\cdot)$. There is an interesting equivalence between $C_D^{t,s}(x_1^n)$ and $R(D)$, the Rate Distortion Function. For a stationary ergodic source with recursive probability measure μ, $\lim_{t,s\to\infty}\lim_{n\to\infty} C_D^{t,s}(x_1^n) = R(D)$, μ-almost surely [3]. The two limits in this statement show that this equivalence holds only for infinite observations and that Shannon's theory does not bound the computational power of the decoder. As a consequence, the coding of finite objects with decoding computational bounds fits better in Kolmogorov's algorithmic framework and it becomes a recursive search for short descriptions.

III. Genetic Algorithms

We focus on time complexity and follow [4], to transform every program p into a new string of length $n+c$ by stuffing a new "no operation" symbol n_{op} to p. c is a constant such that $\forall x_1^n \in B^n, K^t(x_1^n) \leq n+c$, where $K^t(x_1^n) = \lim_{s\to\infty} K^{t,s}(x_1^n)$. Hence, the problem of encoding x_1^n can be reduced to a search problem in an exponentially large search space excluding the possibility of an exhaustive search. Genetic Programming (GP) [4] is a very attractive solution to this but to the best of our knowledge its convergence properties are not well understood. Instead, we propose to use Genetic Algorithm (GA) search techniques to identify good representations. The use of the n_{op} instruction allows us to modify the GP search into a well understood GA search where all programs have the same length. An evaluation metric, $f(p)$, commonly called the fitness measure, is used to assign to each program p of the search space a score associated with the ability of p to represent x_1^n. Let $I(\cdot)$ be the indicator function. $f(p) = I(D(p) > D)\frac{D_{max}+\beta-D(p)}{D_{max}+\beta} + I(D(p) \leq D)(n + c - l(p) + 1)$ where $l(p)$ is the length of p (before stuffing symbols n_{op}), $D(p) = d_n(x_n, \Psi^t(p))$ the distance between its output and x_1^n. $D_{max} = \sup_{x_1^n, y_1^n \in B^n}\{d(x_1^n, y_1^n)\}$, and $\beta > 0$. This fitness ranks programs based on distortion only, if the search operates outside $\mathcal{B}_{x_n}$, a ball of radius D centered at x_n. When it operates inside $\mathcal{B}_{x_n}$, it ranks programs based only on their length. Clearly, elements inside $\mathcal{B}_{x_n}$ have fitness greater than elements outside $\mathcal{B}_{x_n}$. With this measure, a typical GA process uses three genetic search operators (crossover, mutation and reproduction) to evolve generations of programs [4].

IV. Convergence Properties

The GA process can be modeled by a Markov Chain or more generally by a quadratic dynamical system. The probability to have an element with maximum fitness in the population converges [2] and it can be shown that this probability converges to 1 if the best individual in each generation is always reproduced in the next. In general, convergence to 1 can be guaranteed but this is not a sufficient property. Another important point is the speed of convergence to justify the superiority of this approach to the exhaustive search. It can be argued that the convergence is fast. To see this, denote by p_t the distribution at generation t. Let p_∞ be the stationary distribution. Define the mixing time [2] as $\tau(\epsilon) = \max_{p_0} \min\{t : \| p_{t'} - p_\infty \| \leq \epsilon, \forall t' \geq t$ where $\| \cdot \|$ denotes the variation distance and $\epsilon \in (0,1]$. It can be shown [2] that for a one-point crossover system, $\tau(\epsilon) \leq (n+c)\ln(n+c) + (n+c)\ln\epsilon^{-1}$.

References

[1] M. Li and P. Vitanyi, "An Introduction to Kolmogorov Complexity and its Applications", Springer Verlag, 2nd ed, 1997.

[2] Y. Rabani, Y. Rabinovich and A. Sinclair"A computational view of population genetics", Proc, 27th ACM Symp. Theo. Comp., pp 83–92, 1995.

[3] D. Sow and A. Eleftheriadis, "Representing information with computational resource bounds", Proc. 32nd Asilomar Conf. on Signals, Systems and Computer, Nov. 1998.

[4] M. Wineberg and F. Oppacher "A representation scheme to perform program induction in a Canonical Genetic Algorithm", Par. Prob. Solving from Nature III, Lec. Notes in Comp. Science, Vol 86, Springer-Verlag, 1994

0-7803-5857-0/00/$10.00 ©2000 IEEE.

High-Rate Transform Coding: How High is High, and Does it Matter?

Vivek K Goyal
Bell Labs, Lucent Technologies, Murray Hill, NJ 07974-0636
v.goyal@ieee.org, http://cm.bell-labs.com/who/vivek/

Abstract — **Karhunen–Loève transforms (KLT's) are the optimal orthogonal transforms for transform coding of Gaussian sources. This well-known fact is usually established with approximations from high-resolution quantization theory. How high does the rate have to be for these approximations to be accurate? The minimum rate allocated to any component should be at least about one bit. (The average rate per component may be much higher.) Does the rate actually have to be high for the KLT to be optimal? No, the KLT is optimal more generally. Two new, simple proofs of this fact are described. They rely on a scale invariance property, but not on high-resolution approximations or properties of optimal fixed-rate quantization.**

Let $\{x^{(n)}\}_{n\in\mathbb{Z}^+}$ be a sequence of independent, identically distributed (i.i.d.), zero-mean Gaussian random vectors of dimension N with covariance matrix $R_x = E[xx^T]$. In transform coding, an orthogonal linear transform T is applied to each source vector to get a vector of *transform coefficients* $y = Tx$. The transform coefficients undergo fixed- or variable-rate scalar quantization, yielding $\hat{y} = Q(y)$; a reproduction vector is obtained by inverting the transform: $\hat{x} = T^{-1}\hat{y}$. The fidelity of reproduction is measured by the mean-squared error per component between the source vector and the reproduction: $D = N^{-1}E\|x - \hat{x}\|^2$.

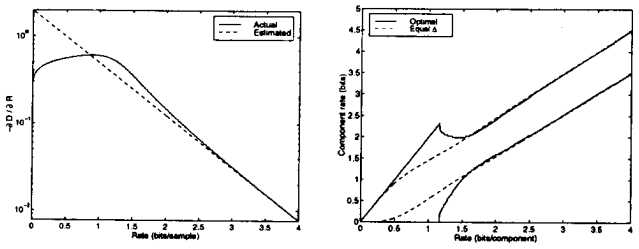
A transform that makes the transform coefficients uncorrelated is called a Karhunen–Loève transform (KLT). The optimality of the KLT was first shown by Huang and Schultheiss under assumptions of optimal fixed-rate quantization and a mild, commonsense condition on the bit allocation. (Earlier work by Kramer and Mathews did not involve quantization and was not in an operational rate–distortion framework.) Optimality of the KLT can also easily be established under the assumption that each component quantizer has distortion–rate performance described by

$$D_i = \frac{\pi e}{6}\sigma_i^2 2^{-2R_i}, \qquad (1)$$

where σ_i^2 is the variance of y_i. This result relies on optimal, arbitrary-real bit allocation, which is unrealistic.

At high rates, (1) is a good approximation of the performance of entropy-coded uniform quantization (ECUQ). The original intention of this work was to determine how high the rate has to be for the KLT to be optimal or nearly optimal when using ECUQ. Actually, there is no limitation on the rate for the KLT to be optimal. Also, through numerical calculations, bit allocations based on (1) are close to optimal when each coefficient has a rate of at least one bit per sample.

Limits of high-resolution analysis Lagrangian bit allocation using (1) is easy because of the simple form of $\partial D_i/\partial R_i$. Where (1) is accurate, the optimal allocation of bits results in equal quantization step sizes for each transform coefficient.



(a) (b)

The accuracy of the derivative of (1) is assessed in Fig. (a). With $\sigma_1^2 = 1$ and $\sigma_2^2 = 1/4$, optimal bit allocations are compared to those obtained with equal quantization step sizes in Fig. (b).

Optimality of the KLT The optimality of the KLT holds much more generally than previously published results indicated. The new result below does not rely on optimal fixed-rate quantization or high-resolution quantization theory.

Theorem [1] *Assume that the distortion–rate performance of a scalar quantizer applied to a component with variance σ^2 is $D = \sigma^2 f(R)$. Then a KLT is an optimal transform,* i.e., *for any given maximum rate, it minimizes the distortion.*

We may assume that $f(\cdot)$ is nonincreasing; if $R_1 > R_2$ but $f(R_1) > f(R_2)$, rate R_1 can be replaced in any purportedly optimal solution by rate R_2. $f(\cdot)$ need not be convex.

Proof 1: Let T be any orthogonal transform. Suppose that R_i bits are allocated to transform coefficient y_i. Assume $\sigma_i^2 > \sigma_j^2$ implies $R_i \geq R_j$; otherwise, the distortion can be reduced by the permutation of T that swaps y_i and y_j.

If the (i,j) component of $R_y = TR_xT^T$ is nonzero for some $i \neq j$, the Jacobi rotation that zeroes this value does not increase the distortion. Repeating the process until convergence (the classical Jacobi algorithm for computing eigendecompositions) yields a KLT at least as good as T. ■

Proof 2 (Telatar): This proof is based on elementary properties of majorization [2]. The problem is to minimize the function $D = N^{-1}\sum_{i=1}^N \sigma_i^2 f(R_i)$ by manipulating the σ_i^2's through the choice of T. Let $\sigma = (\sigma_1^2, \sigma_2^2, \ldots, \sigma_N^2) = \mathrm{diag}(TR_xT^T)$. For a Hermetian matrix, the diagonal elements are majorized by the eigenvalues, so σ is majorized by a vector λ of eigenvalues of R_x. Now the majorization of σ by λ is equivalent to σ being in the convex hull of the $N!$ permutations of λ. Thus, we are left with minimizing D over the convex polytope defined by the permutations of λ. In minimizing a linear function over a convex polytope, the optimum is always attained at a corner point. This establishes that the optimal transform is a KLT. ■

References

[1] V. K Goyal, J. Zhuang and M. Vetterli, "Transform coding with backward adaptive updates," *IEEE T. Inf. Th.*, July 2000.

[2] A. W. Marshall and I. Olkin, *Inequalities: Theory of Majorizations and Its Applications*, Academic Press, San Diego, 1979.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

The Rate Distortion Region for the Multiple Description Problem[1]

Michael Fleming
Dept. of Electrical Eng. (136-93)
California Institute of Technology
Pasadena, CA 91125, USA

Michelle Effros
Dept. of Electrical Eng. (136-93)
California Institute of Technology
Pasadena, CA 91125, USA

Abstract — **We derive the rate-distortion region for the two-channel multiple description problem on stationary discrete ergodic and nonergodic sources with alphabets admitting an ergodic decomposition. The results do not provide a single-letter representation for the rate-distortion region on i.i.d. sources.**

I. Introduction

In multiple description (MD) source coding with two channels, a source is described at two different rates, and each description is sent over a separate channel to the receiver. Each channel has some probability of breaking down, in which case all of the data sent on that channel is lost. If only channel i is working, the receiver makes reproduction $\hat{X}_i$ with average distortion D_i using the rate-R_i description sent on channel i. When both channels work, the receiver makes reproduction $\hat{X}_{12}$ with average distortion D_{12} using the description provided by combining the information on both channels with an additional rate-R_{12} description. The descriptions of both $\hat{X}_1$ and $\hat{X}_2$ are available when decoding $\hat{X}_{12}$; the additional rate R_{12} spent on $\hat{X}_{12}$ can be treated as refinement and split arbitrarily between the two channels.

Other authors have found upper and lower bounds on the achievable rate distortion region (the set of achievable vectors $(\mathbf{R},\mathbf{D}) = (R_1, R_2, R_{12}, D_1, D_2, D_{12})$) for the two-channel multiple description of an i.i.d. source. The bounds do not match for all sources. We present a new achievability theorem and matching converse giving the achievable rate-distortion region for both ergodic and nonergodic sources. On i.i.d. sources, our converse is similar to that of [1], and our achievability result uses an existing achievability result from [2]. We use a Lagrangian approach and closely parallel [3].

Both the converse and achievability proofs make use of distributions with a property that we call n-block conditional independence, defined in the following section. The use of distributions with this property arises from the observation that the bounds of [1] and [2] match when $\hat{X}_1$ and $\hat{X}_2$ are conditionally independent given X. While such conditional independence is not observed on a symbol-by-symbol basis, it arises naturally when using n-dimensional codes since $\hat{X}_1^n, \hat{X}_2^n$ and $\hat{X}_{12}^n$ are all uniquely determined by X^n.

II. N-Block Conditional Independence

Let the elements of a one-sided infinite sequence $\mathbf{Y}$ be denoted $Y_1, Y_2, \ldots$. We divide these elements into n-blocks as $\mathbf{Y}(i) = Y_{(i-1)n+1}^{in}$. We say that distribution $\mathbf{q}(\hat{\mathbf{x}}_{12}, \hat{\mathbf{x}}_1, \hat{\mathbf{x}}_2|\mathbf{x})$ has n-block conditional independence if $\mathbf{q}(\hat{\mathbf{x}}_{12}, \hat{\mathbf{x}}_1, \hat{\mathbf{x}}_2|\mathbf{x}) = \prod_{k=1}^{\infty} q_c^n(\hat{\mathbf{x}}_{12}(k), \hat{\mathbf{x}}_1(k), \hat{\mathbf{x}}_2(k)|\mathbf{x}(k))$, and $q_c^n(\hat{x}_1^n, \hat{x}_2^n|x^n) = q_c^n(\hat{x}_1^n|x^n) q_c^n(\hat{x}_2^n|x^n)$. Define $\Gamma(n)$ to be the set of all distributions $\mathbf{q}(\hat{\mathbf{x}}_{12}, \hat{\mathbf{x}}_1, \hat{\mathbf{x}}_2|\mathbf{x})$ with n-block conditional independence for a particular n, and let $\Gamma = \bigcup_{n=1}^{\infty} \Gamma(n)$.

III. Results

Let A be a discrete source alphabet, and define A^∞ to be the set of one-sided sequences from A. Let $\mathbf{p}$ be a stationary source with alphabet A^∞ and marginal p^n on A^n. Let $\hat{A}$ be a discrete reproduction alphabet, and let $\rho : A \times \hat{A} \to [0, \infty)$ be a nonnegative distortion measure. We assume that there exists a reference letter $y^* \in \hat{A}$ such that $E_p \rho(x, y) = d^* < \infty$. Define $\rho(x^n, y^n) = \sum_{i=1}^n \rho(x_i, y_i)$.

We denote an MD quantizer of blocklength n by $Q^n = (Q_1^n, Q_2^n, Q_{12}^n)$. For each S, Q_S^n maps A^n onto some finite or countable set of codewords $\mathcal{C}_S^n$ from $\hat{A}^n$. We assume that the description of $\hat{X}_{12}^n$ made by Q_{12}^n is a refinement of the descriptions $\hat{X}_1^n$ and $\hat{X}_2^n$ made by Q_1^n and Q_2^n respectively, since these individual descriptions are available to the decoder when decoding $\hat{X}_{12}^n$. The codeword descriptions are assumed to be uniquely decodable.

The set $\mathcal{R}(p)$ of asymptotically achievable rate-distortion vectors $(\mathbf{R},\mathbf{D})$ is, by a timesharing argument, a convex set, and can be entirely characterized by its support functional $j(\alpha,\beta,\mathbf{p}) = \inf_{(\mathbf{r},\mathbf{d}) \in \mathcal{R}(p)} \sum_{S \in \mathcal{M}} (\alpha_S d_S + \beta_S r_S)$, where $\mathcal{M} = \{\{1\},\{2\},\{12\}\}$.

The weighted rate-distortion function is defined as

$$J(\alpha,\beta,\mathbf{p}) = \inf_n J_n(\alpha,\beta,\mathbf{p}),$$

where

$$J_n(\alpha,\beta,\mathbf{p}) = \inf_{\mathbf{q} \in \Gamma(n)} \frac{1}{n} \Big[\sum_{S \in \mathcal{M}} \alpha_S E_{p^n q_c^n} \rho(X^n, \hat{X}_S^n) + \sum_{i=1}^{2} \beta_i I_{p^n q_c^n}(X^n; \hat{X}_i^n) + \beta_{12} I_{p^n q_c^n}(X^n; \hat{X}_{12}^n | \hat{X}_1^n, \hat{X}_2^n) \Big].$$

Stationary Ergodic Sources: When $\mathbf{p}$ is stationary and ergodic, the following result holds.

Theorem 1: $j(\alpha,\beta,\mathbf{p}) = J(\alpha,\beta,\mathbf{p})$.

Stationary Nonergodic Sources: When $\mathbf{p}$ is stationary and nonergodic, but an ergodic decomposition $\{\mathbf{p}_\mathbf{x} : \mathbf{x} \in A^\infty\}$ of $\mathbf{p}$ exists, then the following results hold.

Theorem 2: $J(\alpha,\beta,\mathbf{p}) = \int J(\alpha,\beta,\mathbf{p}_\mathbf{x}) dp(\mathbf{x})$.

Theorem 3: $j(\alpha,\beta,\mathbf{p}) = J(\alpha,\beta,\mathbf{p})$.

References

[1] S. Sher and M. Feder, "A converse theorem for the multiple description problem," *Eighteenth Convention of Electrical and Electronics Engineers in Israel*, pp. 1.1.4/1-4, Mar. 1995.

[2] A. El Gamal and T.M. Cover, "Achievable rates for multiple descriptions," *IEEE Trans. Info. Theory*, vol. 28, pp. 851-857, Nov. 1982.

[3] M. Effros, "Distortion-rate bounds for fixed- and variable-rate multi-resolution source codes," *IEEE Trans. Info. Theory*, vol. 45, pp. 1887-1910, Sep. 1999.

[1]This work was supported by a Pickering Fellowship, NSF grant CCR-9909026, Caltech's Lee Center for Advanced Networking, an F.W.W. Rhodes Memorial Scholarship, and a Redshaw Award.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On the Rate-Distortion Region for Multiple Descriptions *

Fang-Wei Fu† and Raymond W. Yeung‡

The problem of source coding with multiple descriptions (henceforth the multiple descriptions problem) was first posed by Gersho, Witsenhausen, Wolf, Wyner, Ziv and Ozarow at the 1979 IEEE Information Theory Workshop. Since then, this problem has been extensively studied. El Gamal and Cover [1] obtained an inner bound on the rate-distortion region for multiple descriptions, and showed that it is tight for the case of deterministic distortion measures (see [1], Theorem 2). Ozarow [2] showed that this inner bound is also tight for the Gaussian source with the square error distortion. Furthermore, Ahlswede [5], Zhang and Berger [4] showed that the El Gamal-Cover region is tight for the case of no excess rate for the joint description. In the excess rate case, Zhang and Berger [4] showed by a counterexample that the El Gamal-Cover region is not tight in general. How to establish the rate-distortion region for multiple descriptions is still open. It is one of the well known hard problems in multiuser information theory.

In this paper, we study the problem of source coding with multiple descriptions, which is described as follows. For a discrete memoryless source $\mathbf{X}$, there are two encoders $\mathbf{E}_1$ and $\mathbf{E}_2$, and three decoders $\mathbf{D}_1$, $\mathbf{D}_2$ and $\mathbf{D}_0$. The two encoders $\mathbf{E}_1$ and $\mathbf{E}_2$ describe the source $\mathbf{X}$ at respective rates R_1 and R_2. Decoder $\mathbf{D}_1$ receives the output of encoder $\mathbf{E}_1$ only, and it can recover $\mathbf{X}$ with distortion D_1. Decoder $\mathbf{D}_2$ receives the output of encoder $\mathbf{E}_2$ only, and it can recover $\mathbf{X}$ with distortion D_2. Decoder $\mathbf{D}_0$ receives the outputs of both encoders $\mathbf{E}_1$ and $\mathbf{E}_2$, and it can recover $\mathbf{X}$ with distortion D_0. We show that if decoder $\mathbf{D}_2$ (or $\mathbf{D}_1$) is required to recover a function of the source $\mathbf{X}$ perfectly in the usual Shannon sense, the El Gamal-Cover inner bound on the rate distortion region is tight. As a corollary, the Rimoldi [7] rate-distortion region for successive refinement of information, the Kaspi [8] rate-distortion function when side-information may be present at the decoder, and the El Gamal-Cover [1] achievable rate region for multiple descriptions with deterministic distortion measures can all be obtained. We have also obtained a new outer bound on the rate-distortion region which enhances the outer bound due to Witsenhausen and Wyner [3]. This new outer bound implies some interesting facts regarding the achievable rate-distortion vectors. Finally, inspired by the problem of multiple descriptions with deterministic distortion measures studied by El Gamal and Cover [1], and the problem of symmetrical multilevel diversity source coding studied by Roche, Yeung, Hau and Zhang (see [9] and [10]), we pose a multilevel diversity source coding problem for further studying.

*This research work is supported in part by the National Natural Science Foundation of China under the Grant 69802008 and the Research Grant Council of Hong Kong under Earmarked Grant CUHK 332/96E.

†Fang-Wei Fu is with the Department of Information Science, College of Mathematical Science, Nankai University, Tianjin 300071, China. E-mail: fwfu@sun.nankai.edu.cn

‡Raymond W. Yeung is with the Department of Information Engineering, The Chinese University of Hong Kong, Shatin, N.T., Hong Kong. E-mail: whyeung@ie.cuhk.edu.hk

References

[1] A. A. El Gamal and T. M. Cover, "Achievable rates for multiple descriptions," *IEEE Trans. Inform. Theory*, vol.28, pp.851-857, Nov. 1982.

[2] L. Ozarow, "On a source-coding problem with two channels and three receivers," *Bell Syst. Tech. J.*, vol.59, no.10, pp.1909-1921, Dec. 1980.

[3] H. S. Witsenhausen and A. D. Wyner, "Source coding for multiple descriptions, II: A binary source," *Bell Syst. Tech. J.*, vol.60, no.10, pp.2281-2292, Dec. 1981.

[4] Z. Zhang and T. Berger, "New results for multiple descriptions," *IEEE Trans. Inform. Theory*, vol.33, pp.502-521, July 1987.

[5] R. Ahlswede, "The rate-distortion region for multiple descriptions without excess rate," *IEEE Trans. Inform. Theory*, vol.31, pp.721-726, Nov. 1985.

[6] W. H. R. Equitz and T. M. Cover, "Successive refinement of information," *IEEE Trans. Inform. Theory*, vol.37, pp.269-274, Mar. 1991.

[7] B. Rimoldi, "Successive refinement of information: Characterization of the achievable rates," *IEEE Trans. Inform. Theory*, vol.40, pp.253-259, Jan. 1994.

[8] A. H. Kaspi, "Rate-distortion function when side-information may be present at the decoder," *IEEE Trans. Inform. Theory*, vol.40, pp.2031-2034, Nov. 1994.

[9] J. R. Roche, R. W. Yeung and K. P. Hau, "Symmetrical multilevel diversity coding," *IEEE Trans. Inform. Theory*, vol.43, pp.1059-1064, May 1997.

[10] R. W. Yeung and Z. Zhang, "On symmetrical multilevel diversity coding," *IEEE Trans. Inform. Theory*, vol.45, pp.609-621, Mar. 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

A Rate-Distortion Theorem Without Reference Letters

Takeshi Hashimoto
Dept. Electronic Engineering, University of Electro-Communications
Chofu, Tokyo 182-8585, Japan
e-mail: hasimoto@itl.ee.uec.ac.jp

Abstract — **We show the asymptotic attainability of $R(D)$ without assuming reference letters.**

I. Introduction

To show the attainability of $R(D)$ for a source X with a single letter fidelity criterion $d(a^N, b^N) \triangleq \sum_{i=1}^N d(a_i, b_i)$, we usually assume a *reference letter* y^* such that

$$E[\, d(X_t, y^*)\,] < \infty. \tag{1}$$

Its importance is readily understood by the fact that most of known source coding theorems, except[1] possibly for [3] and [4], rely on it or on a stronger assumption of bounded distortion.

We modify a scheme in [2] and prove a coding theorem for a stationary abstract-alphabet source only assuming an auxiliary source W^N such that $E[d(X^N, W^N)] < \infty$.

II. Rate-distortion function

The Nth-order rate-distortion function is the infimum

$$R_N(D) \triangleq \inf \frac{1}{N} I(X^N; W^N) \tag{2}$$

over all W^N such that $(1/N)E[d(X^N, W^N)] \le D$. It converges to $R(D)$ as $N \to \infty$ whenever X is stationary.

III. Variable-rate variable-distortion coding

We consider a reproduction code C_r^N consisting of infinitely many reproduction codewords $y_m^N \in B^N$, $m = 1, 2, \cdots$, and an addressing code C_a^N consisting of infinitely many binary b_m, $m = 1, 2, \cdots$. For each m, we let $\ell_m \triangleq |b_m|$ so that

$$\left(1+\frac{1}{N}\right)\log m+\frac{1}{N}+\log N \le \ell_m \le \left(1+\frac{1}{N}\right)\log m+\frac{1}{N}+\log N+1. \tag{3}$$

Then, ℓ_m satisfy Kraft's inequality and hence we can assume that C_a^N is uniquely decodable.

Our encoding scheme is as follows. For given $X^N = x^N$, we first observe the outcome $W^N = w^N$ and then search for the smallest $\tilde{m}$ satisfying $d(x^N, y_{\tilde{m}}^N) \le d(x^N, w^N)$. The transmitted codeword is then $b_{\tilde{m}}^N \in C_a^N$.

Let $D(x^N, w^N, C^N) \triangleq d(x^N, y_{\tilde{m}}^N)/N$ and $R(x^N, w^N, C^N) \triangleq \ell_{\tilde{m}}/N$ respectively.

IV. Coding theorem

For an auxiliary source W^N, let Y^N be an independent replica of W^N and construct a random ensemble of codes, $\mathcal{C}^N$, by selecting reproduction codewords randomly and independently of each other. Let $\mathcal{E}$ be the expectation with respect to $\mathcal{C}^N$.

Given $(X^N, W^N) = (x^N, w^N)$, let $\overline{R}(x^N, w^N) \triangleq \mathcal{E}[R(x^N, w^N, \mathcal{C}^N)]$. Then, from (3), we have

$$\overline{R}(x^N, w^N) \le k_N \log \mathcal{E}[\,\tilde{m}\,] + g_N + k_N, \tag{4}$$

where we let $k_N \triangleq (N+1)/N^2$ and $g_N \triangleq (\log N)/N$.

Let

$$F(\rho, \delta | a^N) \triangleq \Pr\left\{ \frac{1}{N} i_{XW}(a^N, W^N) \le \rho \text{ and } \frac{1}{N} d(a^N, W^N) \le \delta \,\middle|\, X^N = a^N \right\}. \tag{5}$$

Then, for $\rho = i_{XW}(x^N, w^N)/N + \Delta$, the right-hand side of (4) is bounded by

$$\le k_N \cdot (N\tilde{\rho} + N\Delta + 1) + g_N + k_N \log \frac{1}{F(\tilde{\rho} + \Delta, \tilde{\delta} | x^N)} \tag{6}$$

and we have

$$E\left[\overline{R}(X^N, W^N)\right] \le k_N \left[I(X^N; W^N) + N\Delta + 1 \right] + g_N + k_N E\left[\int \log \frac{1}{F(\rho + \Delta, \delta | X^N)} dF(\rho, \delta | X^N) \right]. \tag{7}$$

The last term is a two-dimensional Lebesgue-Stieltjes integral in $(\rho, \delta) \in (-\infty, \infty) \times [0, \infty)$ and, using a certain upper bound on it, we have

Theorem 1 *For $N \ge 3$, there exists C^N such that*

$$E[\, D(X^N, W^N, C^N)\,] \le D \quad \textit{and} \tag{8}$$

$$E[\, R(X^N, W^N, C^N)\,] \le R_N(D) + \frac{2\log N}{N} + \frac{3 + 2\log e + 3R_N(D)}{N} + \frac{13 + \log N}{N^2}. \tag{9}$$

V. A remark on time-continuous sources

Berger discussed the extension of coding theorems to time-continuous sources in [1]. He argued therein that we must extend our mathematical tools, which have been proved to be useful for time-discrete sources, to time-continuous sources. Up to now, however, there seems to be little progress in the attempt to extend those mathematical tools, such as AEP (asymptotic equi-partition) theorems, to time-continuous sources. Our coding scheme proposed in this paper can be extended to time-continuous sources since no facts in ergodic theory is used.

Acknowledgments

The author appreciates Prof. T.Kawabata in Univ. Elect.-Commun. and Prof. H.Yamamoto in Tokyo Univ.

References

[1] T. Berger, *Rate Distortion Theory.* Prentice-Hall, 1971.

[2] T. Hashimoto, *IEEE Trans. I.T.*, vol. IT-29, pp. 785-792, Nov. 1983 with an errata in vol. 38, pp. 1184-1185, May 1992.

[3] S. Miyake, "Universal coding with fidelity criterion on standard space", in Proc. *The 20th Symp. on Inform. Theory and Its Appl. (SITA97)* (Dec. 1997), pp. 813-816.

[4] J. Ziv, "Coding of sources with unknown statistics – Part II: Distortion relative to a fidelity criterion", *IEEE Trans. Information Theory*, vol. IT-18, pp. 389-394, May 1972.

[1] [3] is for fixed-distortion coding and [4] does not consider $R(D)$.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On the Rates-Reliability-Distortions and Partial Secrecy Region of a One-Stage Branching Communication System

Evgueni Haroutunian[1]
Institute for Informatics and Automation Problems of the Armenian National Academy of Sciences and of the YSU, Yerevan, Armenia
evhar@ipia.sci.am

Ashot Harutyunyan[1]
Institute for Informatics and Automation Problems of the Armenian National Academy of Sciences and of the YSU, Yerevan, Armenia
ashar@ipia.sci.am

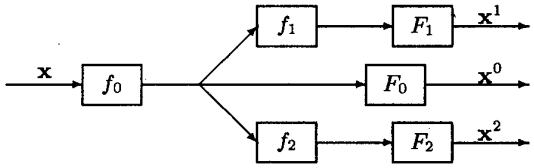
Anahit Ghazaryan[1]
Institute for Informatics and Automation Problems of the Armenian National Academy of Sciences and of the YSU, Yerevan, Armenia
evhar@ipia.sci.am

Edward van der Meulen[1]
Department of Mathematics Katholieke Universiteit Leuven, Belgium
ecvdm@gauss.wis.kuleuven.ac.be

Abstract — **A communication system is considered, where messages of K correlated sources $X_1, \cdots, X_K$ are encoded by a common encoder and two secondary encoders. At each receiver it is demanded: (i) to recover the messages of a part of the sources within given distortion levels, (ii) to keep secret the outputs of another part of the sources for receivers connected to the secondary encoders; and (iii) to disregard the information of the rest of the sources. It is required that for a given reliability $E > 0$ at all receivers the error probabilities of the blocklength N code do not exceed 2^{-NE}. Inner and outer bounds on the region of achievable rates are established, depending on the reliability E and permissible distortion and secrecy levels.**

I. Introduction

We study a problem of common encoding of K correlated sources for transmission to three destinations with respect to fidelity, security, and reliability criteria for the one-stage branching communication system shown in the figure. The problem is a generalization of the one studied by Yamamoto [1].



Let X_n, $n = \overline{1,N}$ be a sequence of N discrete, independent, identically distributed random vectors with K components, which represent messages of the k-th source at the n-th moment, $k = \overline{1,K}$, $n = \overline{1,N}$, with values in the finite set $\mathcal{X}_k$, $k = \overline{1,K}$, respectively. Let $\mathcal{X}_1 \times ... \times \mathcal{X}_K = \mathcal{X}$, $(\mathcal{X}_1)^N \times ... \times (\mathcal{X}_K)^N = (\mathcal{X})^N$. For each receiver $m = 0, 1, 2$ the set of indexes of sources $\{1, ..., K\}$ is divided into three groups: $\{1, ..., K\} = \mathcal{G}_1^m \bigcup \mathcal{G}_2^m \bigcup \mathcal{G}_3^m$, $\mathcal{G}_2^0 = \emptyset$. We denote by small letters the corresponding values of random vectors and random variables, such that $(x_{1,n}, ..., x_{K,n}) = x_n$, $(x_{k,1}, ..., x_{k,N}) = \mathbf{x}_k$, $k = \overline{1,K}$, $(\mathbf{x}_1, ..., \mathbf{x}_K) = \mathbf{x}$. Let $X_{k,n}^m$ be the reconstruction of the n-th message of the k-th source at the m-th receiver, with values in a finite set $\mathcal{X}_k^m$, respectively, $n = \overline{1,N}$, $k \in \mathcal{G}_1^m$, $m = 0, 1, 2$, $\mathcal{X}_1^m \times \cdots \times \mathcal{X}_K^m = \mathcal{X}^m$. For messages received at the outputs we use analogous notations, such as $(x_{1,n}^m, \ldots, x_{K,n}^m) = x_n^m$, $(x_{k,1}^m, \ldots, x_{k,N}^m) = \mathbf{x}_k^m$, $k = \overline{1,K}$, $(\mathbf{x}_1^m, \ldots, \mathbf{x}_K^m) = \mathbf{x}^m$, $m = 0, 1, 2$. The common probability distribution of the vector of messages of K sources is denoted by $P^* = \{P^*(x), x \in \mathcal{X}\}$. Let $d_k^m : \mathcal{X}_k \times \mathcal{X}_k^m \to [0, \infty)$, $k = \overline{1,K}$, $m = 0, 1, 2$ be the corresponding distortion measures. Distortion for N-vectors is defined by averaging. A code is a family of six mappings: (i) three encoding functions $f_0 : (\mathcal{X})^N \to \{1, \cdots, M_0(N)\}$, $f_1 : \{1, \cdots, M_0(N)\} \to \{1, \cdots, M_1(N)\}$, $f_2 : \{1, \cdots, M_0(N)\} \to \{1, \cdots, M_2(N)\}$, and (ii) three decoding functions $F_m : \{1, \cdots, M_m(N)\} \to (\mathcal{X}^m)^N$, $m = 0, 1, 2$. Let $\mathcal{A}_0 = \{\mathbf{x} : F_0(f_0(\mathbf{x})) = \mathbf{x}^0,\ d_k^0(\mathbf{x}_k, \mathbf{x}_k^0) \le \Delta_k^0,\ k \in \mathcal{G}_1^0\}$,

$$\mathcal{A}_m = \{\mathbf{x} : F_m(f_m(f_0(\mathbf{x}))) = \mathbf{x}^m,\ d_k^m(\mathbf{x}_k, \mathbf{x}_k^m) \le \Delta_k^m,\ k \in \mathcal{G}_1^m,$$
$$d_k^m(\mathbf{x}_k, \mathbf{x}_k^m) \ge \Delta_k^m,\ k \in \mathcal{G}_2^m\},\ m = 1, 2.$$

Security evaluation by distortion measures was first considered by Yamamoto in [2] and later in [3].

Error probabilities of the code (f, F) are: $e_m = 1 - P^{*N}(\mathcal{A}_m)$, $m = 0, 1, 2$. For brevity we denote $(\Delta_1^m, \cdots, \Delta_K^m) = \Delta^m$, $(\Delta^0, \Delta^1, \Delta^2) = \Delta$. A triplet of non-negative numbers (R_0, R_1, R_2) is called $(E, \boldsymbol{\Delta})$-achievable for $E > 0, \Delta_k^m \ge 0, k = \overline{1,K}, m = 0, 1, 2$, if for any $\epsilon > 0$ and N sufficiently large there exists a code (f, F) such that

$$N^{-1} \log M_m(N) \le R_m + \varepsilon,\ e_m \le \exp(-NE),\ m = 0, 1, 2.$$

The inner and the outer bounds for the rates-reliability-distortions-partial secrecy region $\mathcal{R}(E, \boldsymbol{\Delta})$ are constructed. When $E \to 0$, we obtain the inner and outer bounds for the corresponding rates-distortions-partial secrecy region $\mathcal{R}(\boldsymbol{\Delta})$.

In a special case we arrive at the results of Yamamoto [1] for a bidirectional branching communication system, but our inner bound is larger. The results are consistent with the corresponding results from [2], [4], [5].

Remark: Some cases of coincidence of the inner and the outer bounds are pointed out.

[1]This work was supported by INTAS Grant 94-469.

References

[1] H. Yamamoto, "Source coding theory for cascade and branching communication systems", *IEEE Trans. Inform. Theory*, vol. IT-27, no. 3, pp. 299-308, May 1981.

[2] H. Yamamoto, "A rate-distortion problem for a communication system with a secondary decoder to be hindered", *IEEE Trans. Inform. Theory*, vol. IT-34, No. 4, pp. 835-842, July 1988.

[3] H. Yamamoto, "Rate-distortion theory for the Shannon cipher system", *IEEE Trans. Inform. Theory*, vol. 43, no. 3, pp. 827-835, May1997.

[4] A. El Gamal and T. M. Cover, "Achievable rates for multiple descriptions", *IEEE Trans. Inform. Theory*, vol. IT-28, no. 6, pp. 851-857, Nov. 1982.

[5] E. A. Haroutunian, A. N. Harutyunyan and A. R. Ghazaryan, "On rate-reliabilities-distortions function of source with many receivers", *Proceedings of the 13-th Prague Conference on Information Theory, Statistical Decision Functions and Random Processes*, vol. 1, pp. 217-220, Prague, 1998.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Theoretical Analysis of a Correlation Attack based on Convolutional Codes

Fredrik Jönsson[1] and Thomas Johansson[1]
Department of Information Technology
Lund University, P.O. Box 118, 221 00 Lund, Sweden
e-mail: {fredrikj,thomas}@it.lth.se

Abstract — **This paper presents a theoretical analysis of a recent algorithm for fast correlation attacks, based on the use of convolutional codes [1].**

I. Introduction

Consider a binary synchronous stream cipher where a correlation has been identified between the keystream sequence and the output from one of the LFSRs. Then a correlation attack can be applied [2, 3].

Let the LFSR have length l and let the set of possible LFSR sequences be denoted by $\mathcal{L}$. Clearly, $|\mathcal{L}| = 2^l$ and for a fixed length N the truncated sequences from $\mathcal{L}$ is also a linear $[N, l]$ block code, referred to as $\mathcal{C}$. Furthermore, the keystream sequence $\mathbf{z} = z_1, z_2, \ldots, z_N$ is regarded as the received channel output and the LFSR sequence $\mathbf{u} = u_1, u_2, \ldots, u_N$ is regarded as a codeword from $\mathcal{C}$. Due to the correlation between u_i and z_i, we can describe each z_i as the output of the binary symmetric channel, BSC, when u_i was transmitted. The correlation probability $1-p$, defined by $1-p = P(u_i = z_i)$, gives p as the crossover probability (error probability) in the BSC.

The algorithm proposed in [1] transforms a part of the code $\mathcal{C}$ stemming from the LFSR sequences into a convolutional code. The encoder of this convolutional code is created by finding suitable parity check equations from $\mathcal{C}$. Here we can only give a brief sketch of the methods to create this convolutional code, for a complete description see [1].

Let us start with the linear code $\mathcal{C}$ stemming from the LFSR sequences. There is a corresponding $l \times N$ systematic generator matrix $G_{LFSR} = (I_l Z)$. Let $\mathbf{g}_i$ be the ith column of G_{LFSR}. Clearly, $u_i = \mathbf{u}_0 \mathbf{g}_i$, where $\mathbf{u}_0$ is the initial state of the LFSR. Fix the memory of the convolutional to B. We are now interested in finding parity check equations that involve a current symbol u_n, an arbitrary linear combination of the B previous symbols $u_{n-1}, \ldots, u_{n-B}$, together with at most t other symbols. Clearly, t should be rather small. Parity check equations for u_{B+1} with weight t outside the first $B+1$ positions can then be found by finding linear combinations of t columns of G such that

$$u_{i_1} + \ldots + u_{i_t} = \mathbf{u}_0(\mathbf{g}_{i_1} + \ldots + \mathbf{g}_{i_t}) = \sum_{i=1}^{B} c_j u_{i-(B-j)} + u_i.$$

To recover the initial state of the LFSR it is enough to decode l consecutive information bits correctly. However, in our application there is neither a starting state nor an ending state. To deal with this problem we decode over J symbols where $J \approx l + 10B$. Optimal decoding (ML decoding) of convolutional codes uses the Viterbi algorithm to decode. This estimate from the Viterbi algorithm is then used to provide the corresponding estimate of the initial state of the LFSR.

[1]This work was supported by the Foundation for Strategic Research - PCC under Grant 9706-09.

II. Theoretical analysis

The principle of the analysis is the following. We start by calculating the average number of parity check equations that we find by the proposed algorithm, which gives us the rate of the convolutional code. Let $E[m]$ be the expected number of parity check equations. Then it can be shown that

$$E[m] = \frac{\binom{N-J}{t}}{2^{l-B}}.$$

In our case, we consider an "embedded" convolutional code. Then the received symbol $r_n^{(i)}$ corresponding to codeword symbol $v_n^{(i)}$ is given as the sum of t keystream symbols, $r_n^{(i)} = z_{j_{1i}} + \ldots + z_{j_{ti}}$. If $P(z_i = u_i) = 1/2 - \delta$ it can be shown that $P(r_n^{(i)} = v_n^{(i)}) = 1/2 - \epsilon$, where

$$\epsilon = 2^{t-1}\delta^t.$$

Given the number of equations and the error probability of the BSC we can use results from convolutional coding to get a bound on the burst error probability of the convolutional code. This burst error probability determines the probability that the proposed attack fails. Finally, we fix the rate to be $R = R_0$, where R_0 is the computational cutoff rate. Based on these assumptions, Theorem 1 gives the required initial correlation for given length N, LFSR length l, and algorithm parameters B and t.

Theorem 1 *With probability $1 - p_e, p_e < 1$, the proposed attack succeeds if*

$$\delta \geq \frac{1}{2} \cdot \left(\frac{4 \ln 2 \cdot 2^{l-B}}{\binom{N-J}{t}} \right)^{\frac{1}{2t}},$$

where the correlation probability is $P(z_i = u_i) = 1/2 + \delta$, and $p_e < J2^{-B}$.

The result of Theorem 1 agrees well with the simulation results presented in [1].

References

[1] T. Johansson, and F. Jönsson, "Improved Fast Correlation Attacks on Stream Ciphers via Convolutional Codes", *Advances in Cryptology-EUROCRYPT'99*, Lecture Notes in Computer Science, vol. 1592, Springer-Verlag, 1999, pp.347–362.

[2] W. Meier, and O. Staffelbach, "Fast correlation attacks on certain stream ciphers", *Journal of Cryptology*, vol. 1, 1989, pp. 159–176.

[3] T. Siegenthaler, "Decrypting a class of stream ciphers using ciphertext only", *IEEE Trans. on Computers*, vol. C–34, 1985, pp. 81–85.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Compared Performance of Fast Correlation Attacks on Stream Ciphers

Anne Canteaut
INRIA projet CODES
B.P. 105
78153 Le Chesnay - France
Anne.Canteaut@inria.fr

Michaël Trabbia[1]
INRIA projet CODES
B.P. 105
78153 Le Chesnay - France
michael.trabbia@enst.fr

Abstract — **We show that fast correlation attacks based on Gallager decoding algorithm with parity-check equations of weight 4 or 5 usually provide better performance than all previously known attacks.**

I. Introduction

In a binary additive stream cipher the ciphertext is obtained by adding bitwise the plaintext to a pseudo-random sequence s. This running-key is produced by a pseudo-random generator whose initialization is the secret key of the cipher. A classical method for generating a running-key is to combine n LFSRs by a Boolean function f. Correlation attacks introduced by Siegenthaler [5] exploit the existence of a correlation between the running-key and the output of one constituent LFSR for recovering the initialization of each LFSR separately. When the combining function is t-th order correlation-immune, this attack should examine $(t+1)$ LFSRs together.

Proposition 1 *Let t denote the maximal correlation-immunity order of the combining function f. Then there exists a subset of $t+1$ variables, $\{x_{i_1}, \ldots, x_{i_{t+1}}\}$, and a Boolean function g with $t+1$ variables such that $p_g = Pr[f \neq g] < 1/2$. Moreover, the lowest possible value of p_g is achieved by the affine function $g = \sum_{j=1}^{k} x_{i_j} + \varepsilon$ where $\varepsilon \in \{0,1\}$.*

Let σ denote the sequence produced by these $(t+1)$ LFSRs combined by the affine function g. The running-key sequence s can then be seen as the result of the transmission of σ through the binary symmetric channel with error probability p_g. The sequence σ corresponds to the output of a unique LFSR of length L whose feedback polynomial P is derived from the feedback polynomials of the constituent LFSRs. Any subsequence of length N of σ is then a codeword of an $[N, L]$-linear code $\mathcal{C}$. The attack aims at recovering L consecutive bits of σ from the knowledge of N bits of s. This can be done by decoding $(s_n)_{n<N}$ relatively to $\mathcal{C}$. Meier and Staffelbach attack uses the iterative decoding process due to Gallager [1] with parity-check equations of weight 3. Johansson and Jönsson recently proposed two new techniques for fast correlation attacks based on convolutional codes [2] and on turbo codes [3].

II. Attack based on Gallager algorithm

The preprocessing step of the attack consists in generating all parity-check equations involving d bits of the sequence $(\sigma_n)_{n<N}$. They correspond to all polynomials $Q(X)P(X)$ of weight d and of degree at most N, where P is the feedback polynomial of the LFSR generating σ. The number of such equations involving the n-th bit of σ is approximatively

$$m(d) \simeq \frac{N^{d-1}}{(d-1)!2^L} \cdot$$

[1]also with Ecole Polytechnique - 91128 Palaiseau Cedex - France

Using these parity-check equations we recover $(\sigma_n)_{n<N}$ from $(s_n)_{n<N}$ using Gallager soft-input/soft-output decoding algorithm [1]. Simulations provide an approximation of the minimum value of $m(d)$ for convergence of the decoding algorithm:

$$m(d) \geq \frac{K_d}{C_{d-2}(p)}$$

where $C_{d-2}(p)$ is the capacity of the binary symmetric channel with error-probability $p_{d-2} = \frac{1}{2}(1-(1-2p)^{d-2})$, $K_d \simeq 1$ if $d \geq 4$ and $K_3 \simeq 2$.

III. Comparison with previous attacks

The attack presented in [2] uses a convolutional code with memory B. This code is defined by all equations involving σ_n and $d-1$ bits of σ outside positions $n-1, \ldots, n-B$. The number of such equations is approximatively

$$m_B(d) \simeq \frac{N^{d-1}2^B}{(d-1)!2^L} \cdot$$

The attack then consists in decoding a sequence r such that $Pr[r_n \neq \sigma_n] = p_{d-1}$. Viterbi algorithm then converges if

$$m_B(d) \leq \frac{K'}{C_{d-1}(p)} - 1$$

where K' slightly depends on L ($K' = 3$ for $L = 21$ and $K' = 2.5$ for $L = 40$). It follows that this attack with $d = 3$ achieves the same performance than Gallager algorithm with $d = 4$ only for high values of B. This makes the decoding step intractable due to the complexity and the memory requirement of Viterbi algorithm. The only advantage of the attack based on convolutional codes is the lower complexity of the preprocessing step; but this part is performed once for all.

As an example, for $L = 40$ and $N = 400,000$, the maximum error-probability achieved by our attack with $d = 4$ is $p = 0.44$. In this case, the preprocessing step and the decoding step take respectively 9 hours and 1.5 hour on a DEC alpha workstation. For these parameters, the attacks described in [2] and [3] respectively achieved $p = 0.40$ with $d = 3$ and $B = 15$ and $p = 0.41$ with $d = 3$, $M = 8$ and $B = 13$.

References

[1] R.G. Gallager. Low-density parity-check codes. *IRE Trans. Inform. Theory*, IT-8:21–28, 1962.

[2] T. Johansson and F. Jönsson. Improved fast correlation attack on stream ciphers via convolutional codes. In *EUROCRYPT'99*, LNCS 1592, pp. 347–362. Springer-Verlag, 1999.

[3] T. Johansson and F. Jönsson. Fast correlation attacks based on turbo code techniques. In *CRYPTO'99*, LNCS 1666, pp. 181–197. Springer-Verlag, 1999.

[4] W. Meier and O. Staffelbach. Fast correlation attack on certain stream ciphers. *J. Cryptology*, pp. 159–176, 1989.

[5] T. Siegenthaler. Decrypting a class of stream ciphers using ciphertext only. *IEEE Trans. Computers*, C-34(1):81–84, 1985.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Novel Fast Correlation Attacks via Iterative Decoding of Punctured Simplex Codes

Miodrag J. Mihaljević[1]
Mathematical Institute,
Serb. Academy Sci. and Arts
Kneza Mihaila 35
Belgrade, Yugoslavia
emihalje@ubbg.etf.bg.ac.yu.

Marc P.C. Fossorier[1]
Dept. of Electrical Engineering
University of Hawaii
2540 Dole St. Holmes Hall 483
Honolulu, HI 96822, USA
marc@spectra.eng.hawaii.edu

Hideki Imai[1]
University of Tokyo
Institute of Industrial Science
7-22-1, Roppongi, Minato-ku,
Tokyo, 106-8558 Japan
imai@iis.u-tokyo.ac.jp

Abstract — **A powerful family of algorithms for the fast correlation attack [1] with significantly better performance, assuming the same inputs, than previously reported methods, is proposed. The family is based on the iterative decoding principle in conjunction with a novel method for constructing the parity-checks.**

Let Ω_n be the set of all considered parity-check equations related to the n-th parity bit of an (N, L) punctured simplex code (N, L) codeword defined as follows:
Each parity-check equation is the *mod*2-sum of the n-th row of the parity-check matrix $\mathbf{H} = [\mathbf{P}^T, \mathbf{I}_{N-L}]$ and at most W other rows, providing that values on the positions $i = B + 1, B + 2, ..., L$, are all zeros, where $B < L$ is a predetermined parameter, and where the m-th row of the matrix $\mathbf{P}^T$ is equal to the first row of the m-th power of the LFSR $L \times L$ state transition matrix .

Theorem 1: For any (N, L) punctured simplex code, an approximation on the expected number μ of parity checks per parity bit, assuming each parity check includes only a certain subset from B fixed bits among the L information bits, and no more than $W + 1$ other check bits, is given by:

$$\mu = 2^{-L+B} \sum_{w=1}^{W} \binom{N-L-1}{w} ,$$

where $0 \leq B \leq L$ and $1 \leq W \leq L - B$.

In the following, the main steps of the family of algorithm are summarized (see [3] for a complete description).

1. *Hypothesis setting*
   From the set of all possible 2^B binary patterns obtained from the first B information bits, select a previously not considered pattern $\hat{x}_1, \hat{x}_2, ..., \hat{x}_B$. If no new pattern is available, terminate the procedure.
2. *Iterative decoding*
   Identify the sets Ω_n of parity-check equations, $n = L + 1, L+2, ..., N^*$, and choose the desired iterative decoding of the (N^*, L)-code codeword $[z_1, z_2, ..., z_{N^*}]$ using the following iterative decoding approaches:
   - Bit Flipping (BF),
   - A Posteriory Probability (APP),
   - Belief Propagation (BP),
   - Belief Propagation Based Bit Flipping (BP-BF).

   Generate an estimation of the codeword parity bits $\hat{x}_{L+1}, \hat{x}_{L+2}, ..., \hat{x}_{N^*}$.
3. *Final correlation check*
   Using the sequence $\hat{x}_{L+1}, \hat{x}_{L+2}, ..., \hat{x}_{N^*}$, perform information set decoding.

The performance of the previous family of algorithms is experimentally considered when the LFSR characteristic polynomial is $1 + u + u^3 + u^5 + u^9 + u^{11} + u^{12} + u^{17} + u^{19} + u^{21} + u^{25} + u^{27} + u^{29} + u^{32} + u^{33} + u^{38} + u^{40}$ (i.e. assuming the same example as was considered in [2]).
Figure 1 depicts the percentage of error free information sets obtained for different values of crossover probability p with the employed types of algorithms and $N^* = 4096$.

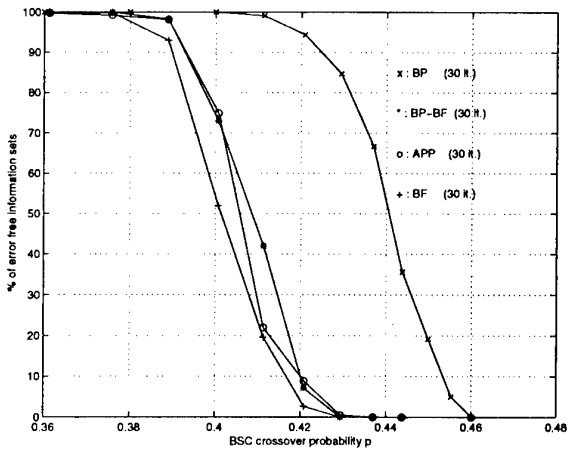


Figure 1: Percentage of error free information sets as a function of the BSC crossover probability p for the (4096,40) truncated simplex code with $B = 22$ and $W + 1 = 3$.

[1]This work was supported by JSPS Grant RFTF 96P00604 and by NSF Grant CCR-97-32959.

References

[1] W. Meier and O. Staffelbach, "Fast correlation attacks on certain stream ciphers," *Journal of Cryptology*, vol. 1, pp. 159-176, 1989.

[2] T. Johanesson and F. Jonsson, "Fast correlation attacks based on turbo code techniques", Advances in Cryptology - CRYPTO'99; *Lecture Notes in Computer Science*, vol. 1666, pp. 181-197, Dec. 1999.

[3] M. J. Mihaljević, M. P.C. Fossorier and H. Imai, "A family of iterative decoding techniques for certain crypto applications", submitted to *IEEE Trans. Inform. Theory*, 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Using Low Density Parity Check Codes in the McEliece Cryptosystem

Chris Monico
Department of Mathematics
University of Notre Dame
Notre Dame, Indiana 46556
e-mail: cmonico@nd.edu
http://www.nd.edu/~cmonico/

Joachim Rosenthal[1]
Department of Mathematics
University of Notre Dame
Notre Dame, Indiana 46556
email: Rosenthal.1@nd.edu
http://www.nd.edu/~rosen/

Amin Shokrollahi
Bell Labs
600 Mountain Avenue
Murray Hill, NJ 07974
email:
amin@research.bell-labs.com

Abstract — **We examine the implications of using a Low Density Parity Check Code (LDPCC) in place of the usual Goppa code in McEliece's cryptosystem. Using a LDPCC allows for larger block lengths and the possibility of a combined error correction/encryption protocol.**

I. Introduction

If one wishes to use a LDPCC in the McEliece system, there are several ways to proceed. An efficient way seems to be the following:

As usual, suppose Bob wishes to send Alice a secure message over an insecure channel. Alice chooses a random $(n-k)\times n$ sparse parity check matrix, H, for a binary LDPCC, $\mathcal{C}$, that admits decoding of any pattern of t or fewer errors with, say, belief propagation. She also randomly chooses sparse invertible matrices $S \in GL(k,\mathbb{F}_2)$ and $T \in GL(n-k,\mathbb{F}_2)$. She then calculates $\tilde{H} := TH$ and has keys:

Public Key: $(\tilde{H}, S, t)$
Private Key: (H, T)

Now, if Bob wants to send Alice the message m, he first computes the generator matrix, G, for the code $\mathcal{C}$ in row reduced echelon form, and then computes $\tilde{G} = S^{-1}G$. He then applies the encryption map:

$$m \mapsto m\tilde{G} + e =: y$$

where e is a random error vector of weight at most t. Alice's decryption procedure is then as follows: Since $\tilde{G}$ and G define the same code, $\mathcal{C}$, she can use H to decode the word y to $m\tilde{G} = mS^{-1}G$. Since G is in row reduced echelon form, this reveals mS^{-1} in the k coordinates of $m\tilde{G}$ in which G has only one nonzero entry (i.e., the *systematic coordinates* of G). Right multiplication by S finally recovers Bob's message m.

This seems relatively efficient because the keys consist of sparse matrices, allowing considerable compression. Hence, one could have key sizes comparable to those of a $(1024, 512)$ McEliece system, but for a code of size $(16384, 8192)$.

II. Security

The security of this system is based on two observations:

- If T is chosen with the proper parameters, $\tilde{H}$ will most likely not admit decoding with, e.g. belief propagation, for the correction of up to t errors.
- It *seems* difficult to recover a matrix, H', equivalent to $\tilde{H}$ that admits decoding with, e.g. belief propagation, for the correction of up to t errors. In particular it seems difficult to recover the specific degree structure of the parity check matrix H.

However, a simple observation shows that if T is chosen too sparsely, this latter task is *not* difficult. In what follows, if $u = (u_1, \ldots, u_n)$ and $v = (v_1, \ldots, v_n)$ are two vectors over $\mathbb{F}_2$, $u * v := (u_1v_1, \ldots, u_nv_n)$ denotes the intersection of the binary vectors u, v. This is a vector whose support is exactly $\mathrm{supp}(u) \cap \mathrm{supp}(v)$. Equivalently, it can be considered as the 'AND' of u and v.

Let $h_1, \ldots, h_{n-k}$ denote the row vectors of H and $\tilde{h}_1, \ldots, \tilde{h}_{n-k}$ the row vectors of $\tilde{H}$. Notice that the h_i are sparse vectors and each $\tilde{h}_j$ is a linear combination of the h_i. Furthermore, if T is sparse, each $\tilde{h}_j = h_{j_1} + \cdots + h_{j_{w_j}}$ with the w_j small. That is, each $\tilde{h}_j$ is a linear combination of a small number of rows of H. If the w_j are too small (i.e., T is too sparse), then with reasonable probability one has that $\tilde{h}_j * h_{j_m} = h_{j_m}$ for many of the $1 \le j \le n-k$, $1 \le j_m \le j_{w_j}$. In this case, since each h_{j_m} appears in several of the $\tilde{h}_j$, we can, with non-negligible probability, find j_1, j_2 such that

$$\tilde{h}_{j_1} * \tilde{h}_{j_2} = h_i$$

for some i. Thus, in time $k(k-1)/2$, we can recover some of the original rows of H by computing the intersection of all pairs of rows, checking to see if the intersection is in $Rowsp(\tilde{H})$. Having found some of the original rows, we can determine, with high probability, which of the $\tilde{h}_j$ have these rows as components in their linear combinations. We thus subtract each original row from the $\tilde{h}_j$ that have many nonzero coordinates in common with it. Then go back to computing the intersection of all pairs of rows again, and keep repeating until we've found sufficiently many original rows to allow decoding.

III. Conclusion

Empirical evidence has shown this attack and some variants of it, to be effective enough that we consider this system insecure unless T is chosen to be dense. Thus, there seems to be no advantage to using a parity check matrix as the public key. However, this system is still of possible interest in the following case: If one is using a LDPCC for error correction, some security can be added at very little extra cost.

References

[1] R.J. McEliece, "A Public Key Cryptosystem Based on Algebraic Coding Theory," *Technical Report DSN Progress Report #42-44*, Jet Propulsion Laboratory, Pasadena, California, 1978.

[2] R.G. Gallager, "Low Density Parity Check Codes," *MIT Press*,Cambridge, MA, 1963.

[3] T. Richardson, M.A. Shokrollahi, and R. Urbanke. Design of provably good low-density parity check codes. *IEEE Trans. Inform. Theory (submitted)*, 1999.

[1]The research is supported in part by NSF grant DMS-96-10389.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

A Class of Signal Processing Algorithms for Good Power/Bandwidth Tradeoffs with OFDM Transmission

Rui Dinis and António Gusmão
CAPS-Instituto Superior Técnico, 1049-001 Lisboa, Portugal
Phone: + 351 21 8419358, Fax: 351 21 8465303, e-mail: rdinis@ist.utl.pt

Abstract — **This paper presents a wide class of signal processing algorithms which employs a nonlinear operation in the time domain and is capable of providing good power/bandwidth tradeoffs with OFDM transmission. A suitable analytical approach is proposed for efficiently evaluating performances within this class of algorithms, and several performance results are shown and discussed in detail.**

A well-known, major drawback of conventional OFDM schemes (Orthogonal Frequency Division Multiplexing) is their high PMEPR (Peak-to-Mean Envelope Power Ratio), leading to amplification difficulties: in order to avoid the out-of-band radiation levels which are inherent to nonlinear distortion, power amplifiers for OFDM transmission are required to have strongly linear characteristics and/or a significant input backoff has to be adopted. Therefore, a reduced power efficiency is the price to pay for a high bandwidth efficiency.

In this paper we propose a technique to reduce the envelope fluctuations with OFDM transmission, while preserving low out-of-band radiation levels and small inband "self-interference" effects. This technique is related to those proposed in [1]-[3] but introduces further flexibility. The signals to be transmitted are generated as follows: an augmented block $\{S'_k; k = 0, 1 \ldots, N' - 1\}$ is obtained by adding $N' - N$ zeros to the data block $\{S_k; k = 0, 1 \ldots, N - 1\}$, where $N' = NM$, for a selected integer M; the IDFT of this frequency-domain block is computed, leading to the block $\{s'_n; n = 0, 1 \ldots, N' - 1\}$; each time-domain sample, s'_n, is submitted to a nonlinear operation, leading to the modified sample $s_n^C = f_C(|s'_n|)\exp(j\arg(s'_n))$; a DFT brings the "nonlinearly corrected" block back to the frequency domain, where a shaping operation is performed by a multiplier bank with selected coefficients $G_k, k = 0, 1, \ldots, N' - 1$, so as to obtain the final frequency-domain block $\{S_k^{CF}; k = 0, 1, \ldots, N' - 1\}$; etc. For a given input block size N, a specific algorithm can be designed through the selection of M, $f_C(\cdot)$ and $\{G_k; k = 0, 1, \ldots, N' - 1\}$.

Adding $N' - N$ zeros to each initial frequency-domain block and computing the IDFT of the augmented block is equivalent to oversampling, by a factor $M = N'/N$, the "OFDM burst" which should directly correspond to the case where $M = 1$. The nonlinear operation $f_C(\cdot)$ corresponds to a bandpass memoryless nonlinearity, characterized by an "AM/AM conversion" function $f_C(\cdot)$ and an "AM/PM conversion" function equal to zero, and can be used to reduce the envelope fluctuations and the PMEPR values. The subsequent frequency-domain operation using the set $\{G_k; k = 0, 1, \ldots, N' - 1\}$ can provide a complementary filtering effect. For instance, by adopting $G_k = 1$ for the N "data subcarriers", and $G_k = 0$ for the remaining $N' - N$ ones, we completely eliminate the out-of-band distortion effects of the nonlinear function $f_C(\cdot)$; however, this leads to some regrowth of the envelope fluctuations. A suitable $M > 1$ reduces the in-band "self-interference" which is due to the nonlinear distortion inherent to $f_C(\cdot)$ (e.g., an "envelope clipping" function), as compared with that concerning $M = 1$.

Whenever the number of subcarriers is high, conventional OFDM signals are known to exhibit a Gaussian-like nature. One can take advantage of this for evaluating performances by analytical means, so as to find an appropriate triple choice (M, $f_C(\cdot)$ and $\{G_k; k = 0, 1, \ldots, N' - 1\}$) for any given application. All we really need in our case is to use well-established results on bandpass memoryless nonlinearities with Gaussian inputs [3, 4]. In this paper, we employ these results to derive a suitable characterization of the frequency-domain block $\{S_k^{CF}; k = 0, 1, \ldots, N' - 1\}$ which replaces the frequency-domain block $\{S_k; k = 0, 1, \ldots, N-1\}$ of conventional OFDM.

By assuming that $E[S_k] = 0$ and $E[S_k S_{k'}^*] = 2\sigma_S^2$ for $k = k'$ and zero otherwise, it is shown that the transmitted frequency-domain samples can be decomposed into two uncorrelated terms, a "useful" term and a "self-interference" term, as follows: $S_k^{CF} = \alpha S'_k G_k + D_k G_k$, where $\alpha = E[|s'_n| f_C(|s'_n|)]/E[|s'_n|^2]$. It is shown that $E[D_k] = 0$ and $E[D_k D_{k'}^*] = 0$ for $k \neq k'$; when $M = 1$, $E[|D_k|^2]$ is shown not to depend on k, but this is no longer true when $M > 1$. Moreover, for any k, D_k exhibits quasi-Gaussian characteristics under the 'high N' assumption mentioned above (say $N \geq 64$).

The characterization of the transmitted frequency-domain block, including the appropriate values for $E[|D_k|^2]$, is then used for both power spectrum and BER computations. The main issue here is to evaluate the impact of the transmitted, noise-like, "self-interference" on both bandwidth efficiency and power efficiency. For this purpose, our analytical approach provides quite accurate results through a modest computational effort.

A set of performance results is presented and discussed in detail, showing that good power/bandwidth tradeoffs can be achieved within the proposed class of algorithms.

References

[1] X.Li and L.J.Cimini, Jr., "Effects of Clipping and Filtering on the Performance of OFDM", *IEEE Comm. Let.*, May 1998.

[2] T.May and H.Rohling, "Reducing the Peak-to-Average Power Ratio in OFDM Radio Transmission Systems", *IEEE VTC'98*, Ottawa, May 1998.

[3] R.Dinis and A.Gusmão, "On the Performance Evaluation of OFDM Transmission Using Clipping Techniques", *IEEE VTC'99 (Fall)*, Amsterdam, September 1999.

[4] H.Rowe, "Memoryless Nonlinearities with Gaussian Input: Elementary Results", *Bell System Tech. Journal*, Vol. 61, Sep. 1982.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On the Existence and Construction of Good Codes with Low Peak-to-Average Power Ratios

Kenneth G. Paterson
Hewlett-Packard Laboratories,
Filton Road, Stoke Gifford,
Bristol BS34 8QZ, UK
kp@hplb.hpl.hp.com

Vahid Tarokh
AT& T Labs – Research,
180 Park Avenue, Florham Park,
New Jersey 07932, USA
tarokh@research.att.com

Abstract — **The peak-to-average power ratio PAPR($\mathcal{C}$) of a code $\mathcal{C}$ is an important characteristic of that code when it is used in OFDM communications. We establish bounds on the region of achievable triples $(R, d, \text{PAPR}(\mathcal{C}))$ where R is the code rate and d is the minimum Euclidean distance of the code. We prove a lower bound on PAPR in terms of R and d and show that there exist asymptotically good codes whose PAPR is at most $8 \log n$. We give explicit constructions of error-correcting codes with low PAPR by employing bounds for hybrid exponential sums over Galois fields and rings.**

I. Introduction

A major barrier to the widespread acceptance of OFDM is the high peak-to-average power ratio (PAPR) of uncoded OFDM signals. By appropriately coding the OFDM signals, this PAPR can be reduced. It is also possible to introduce error-correction capability by using such a code. Here we investigate the fundamental trade-offs between the parameters R, d and PAPR of a code $\mathcal{C}$.

Our codewords $\mathbf{c} \in \mathcal{C}$ are complex vectors of length n with $||\mathbf{c}||^2 = n$. The OFDM signal corresponding to $\mathbf{c}$ as a function of time t is the real part of:

$$S_{\mathbf{c}}(t) = \left(\sum_{i=0}^{n-1} c_i \exp(-2\pi j (f_0 + i f_s) t) \right)$$

for $0 \leq t \leq \frac{1}{f_s}$, where f_0 is the carrier frequency and f_s is the bandwidth of each tone. We define PAPR($\mathbf{c}$), the peak-to-average power ratio of the OFDM signal corresponding to $\mathbf{c}$, to be

$$\frac{1}{n} \max_t [\Re(S_{\mathbf{c}}(t))]^2.$$

We define $\text{PAPR}(\mathcal{C}) = \max_{\mathbf{c} \in \mathcal{C}}(\text{PAPR}(\mathbf{c}))$.

Statement of The Problem: What is the achievable region of triples $(R, d, \text{PAPR}(\mathcal{C}))$?

II. Bounds on the PAPR of codes

We define the curve $\Omega \subset \mathbb{C}^n$ by

$$\Omega = \{(\exp(2\pi j \zeta t), \ldots, \exp(2\pi j (\zeta + n - 1)t)) : 0 \leq t < 1\}$$

where $\zeta = f_0/f_s$. Typically, $\zeta >> 1$. There is a geometric interpretation to the PAPR of a code, showing that the closer a code lies to the curve $\Omega \cup -\Omega$, the larger its PAPR:

Lemma 1 *Let d_* denote the minimum Euclidean distance between the codewords of $\mathcal{C}$ and the points of $\Omega \cup -\Omega$. Then $d_* \leq \sqrt{2n}$ and*

$$PAPR(\mathcal{C}) = n(1 - \delta)^2$$

where $\delta = d_*^2/2n$.

Using the above lemma together with a packing argument, we can prove a lower bound on $PAPR(\mathcal{C})$ as a function of R and d. This bound is rather complex to state and we do not include it here. We also have the following analogue of the Gilbert-Varshamov bound, establishing a region of pairs (R, d) in which asymptotically good sequences of codes with low PAPR are guaranteed to exist:

Theorem 2 *Let $R \geq 0$ and $\Delta \geq 0$ be such that*

$$2^R \sqrt{2\Delta(1 - \frac{\Delta}{2})} < 1.$$

Then for all sufficiently large n, there exists a code $\mathcal{C}$ of length n, rate R and minimum Euclidean distance $d = \sqrt{2\Delta n}$ with $PAPR(\mathcal{C}) \leq 8 \log n$.

III. Codes from exponential sums

We can explicitly describe families of codes with PAPR growth of order $(\log n)^2$, where n is the code length. The families we consider are length $n = 2^m$, 2^e-PSK codes and are derived from special cases of what we call *lengthened trace codes*. The lengthened trace codes are linear over $\mathbb{Z}_{2^e}$ and their codewords can be roughly characterised as having a representation as the trace of a polynomial function evaluated on a Galois field ($e = 1$) or Galois ring ($e > 1$). The technique we use to bound PAPR applies to any code whose DFT is uniformly small. We use bounds for hybrid exponential sums over Galois fields and rings to bound the DFT coefficients of the code families. As a sample of our results we state:

Theorem 3 *Let C_t be the length $n = 2^m$ code obtained by adding to the dual of a primitive t error correcting BCH code the complements of all codewords and then an overall parity check. Then any non-constant codeword of the $\{+1, -1\}$-valued version of C_t has PAPR at most*

$$(2t - 1)^2 \left(\frac{2 \log 2}{\pi} (m + 1) + 3 \right)^2.$$

Similar results can be obtained for weighted degree trace codes and the quaternary versions of the Kerdock and Delsarte-Goethals codes using bounds for hybrid exponential sums over Galois rings due to Shanbag, Kumar and Helleseth. None of our families is asymptotically good, however. The explicit construction of such families with low PAPR remains an open problem.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On the Error Performance of 8-VSB TCM Decoder for ATSC Terrestrial Broadcasting of Digital Television

Dojun Rhee [1]
LSI Logic Corporation
e-mail: drhee@lsil.com

Robert H. Morelos-Zaragoza
SONY Computer Science Laboratories, Inc.
e-mail: morelos@csl.sony.co.jp

Abstract — **The error performance of various 8-VSB TCM decoders for reception of terrestrial digital television is analyzed. In previous work, 8-state TCM decoders were proposed and implemented for terrestrial broadcasting of digital television. In this paper, the performance of a 16-state TCM decoder is analyzed and simulated. It is shown that not only a 16-state TCM decoder outperforms one with 8-states, but it also has much smaller error coefficients.**

I. Introduction

The Digital Television standard [1,2] describes a broadcasting system designed to transmit high quality video and audio as well aas data over a single 6 MHz channel. In order to maximize service area, the terrestrial broadcast mode incorporate both an NTSC rejection filter (in the receiver) and trellis coding. When the NTSC rejection filter is activated in the receiver, a trellis decoder for the combination of a four-state trellis encoder and the filter is used. In the paper, the error performance of various TCM decoders is studied, with and without the NTSC rejection (1-D) filter. In the previous results [1,2], a combined 8-state trellis decoder is employed for the case with NTSC rejection filter. We propose a 16-state TCM decoder and analyze and simulate its error performance. The results show that the error performance improves, with respect to 8-state TCM decoders, at the cost of doubling the memory requirements. In return, a 16-state TCM decoder has much smaller error coefficients and does not require precoding to operate.

II. Encoder model for ATSC terrestrial broadcasting of digital television

In the ATSC terrestrial broadcasting system specification, the 8-VSB transmission subsystem employs a rate-2/3 4-state Ungerboeck trellis code, with the uncoded bit precoded. The 4-state feedback encoder and the bits-to-8 PAM symbol mapper are shown in Fig. 1 (a). The NTSC interference rejection (comb) filter is a one tap linear-feed-forward (1-D) filter. Its purpose is to reduce the analog NTSC interference that is caused by a carrier tone. However, the received signals are also modified. The 8 signal levels are converted to 15 levels. While providing needed co-channel interference benefits, it is well-known that the (1-D) filter degrades white noise performance by 3 dB. This is because the filter output is the subtraction of two full gain paths and, as white noise is uncorrelated from symbol to symbol, the noise power doubles. There is an additional 0.3 dB degradation due to error propagation introduced by precoding.

III. Approximated error performance analysis

In the approximations presented in this section, we interpret the trellis code with decoding depth k, as a terminated zero-tail (ZT) $(3k, 2k-m)$ block code [3]. (For the four-state trellis decoder, $m = 2$, while for 8- and 16-state trellis decoders, $m = 3$ and $m = 4$, respectively.) When plotting the expressions with respect to the energy per bit-to-noise ratio (E_b/N_0), a rate correction of R_L (dB) is applied, to account for the rate loss due to trellis termination, where $R_L = (2k-m)/2k$. With the NTSC interference rejection filter in the receiver, the number of states in the decoder increases, due to a signal constellation of increased dimensionality. In the guide to the ATSC system[2], a (1-D) filter is recommended that increases the number of signal levels from 8 of the original 8-PAM constellation to 15 at the output of the filter. To analyze the performance of the eight-state trellis decoder, a truncated union bound is computed using the technique of [3] as follows. A polynomial state transition matriz $\Pi 9X)$ for the 8-state trellis is used, with branch weights equal to X^d, where d denotes the squared Euclidean distance (SED) with respect to the all-zero branch and X is an indeterminant. For each set of three parallel branches between two states i, j, an element $\pi_{i,j}(X)$ in matrix Π is a polynomial $\pi_{i,j}(X) = X^{d_1} + X^{d_2} + X^{d_3}$, where $d_j, j = 1,2,3$, denotes the SED from the branch output to the all-zero sequence output. Using symbolic mathematical software, the value of the k-th power $\Pi^k(X)$ is computed and the coefficients of $\pi_{0,0}^{(k)}(X)$ yield the weight distribution of the ZT $(3k, (2k-3))$ block code. For the 8-state trellis decoder, with $k = 54$, $\pi_{0,0}^{(54)}(X) = 5696X^{56} + 1520X^{48} + 404X^{40}$ and for 16-state trellis decoder, $\pi_{0,0}^{(54)}(X) = 840X^{56} + 248X^{48} + 101X^{40}$. As shown above, the error coefficients for the MSED for the 16-state trellis decoder is much smaller than that of 8-state trellis decoder.

IV. Conclusion

The simulation and approximated error performance shows that a TCM decoder with 16-states outperforms one with 8-state by approximately 0.33 dB at a BER of 10^{-5}. Finally, while the 8-state decoder must use a precoder for the uncoded bit to be able to decode properly, the proposed 16-state decoder does not and has a better error performance.

References

[1] ATSC Standard A/53, ATSC Digital Television Standard, 1995.

[2] Guide to the Use of The ATSC Digital Television Standard A/54, ATSC Digital Television Standard, 1995.

[3] J. K. Wolf and A. J. Viterbi, "On the Weight Distribution of Linear Block Codes Formed from Convolutional Codes", *IEEE Trans. Comm.*, vol. 44, no. 9, pp. 1049-1051, Sept. 1996.

[1]This work was supported by LSI Logic Corp.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Channel Capacity of Clipped OFDM Systems

Hideki Ochiai[1] and Hideki Imai
Institute of Industrial Science, University of Tokyo
7-22-1 Roppongi, Minato-ku, Tokyo, 106-8558, Japan
e-mail: ochiai@iis.u-tokyo.ac.jp

Abstract — **Channel capacity of OFDM systems with digital clipping is discussed, under the assumption that the distortion terms are Gaussian-distributed.**

I. Introduction

One of the major problems in the orthogonal frequency division multiplexing (OFDM) technique is the high peak-to-average power ratio (PAPR) property of the signal waveform, and digital clipping may be employed in order to reduce the PAPR before amplification. The performance of the clipping in terms of the PAPR reduction capability and the degradation in the bit error rate is discussed in e.g., [1–3]. Without coding, clipping may be a severe source of the performance degradation. However, in most applications of the OFDM, channel coding may be applied so as to reduce the required energy to achieve the targeted bit error performance. Therefore, it is important to study the performance of the clipped *coded* OFDM signals. In this paper, the channel capacity of the clipped OFDM signals is derived and evaluated.

II. System Model

Let N be the number of subcarriers and J be an oversampling factor of the OFDM signals before clipping. Thus, NJ-point IDFT will be used to construct the OFDM signals. In order to efficiently reduce the PAPR of the OFDM signals, the clipping should be performed with oversampling [1,3]. We assume that the clipping is followed by the rectangular filter such that the OFDM signal is tightly band-limited. As a clipping model, soft envelope limiter is considered, where the clipping ratio γ is defined as $\gamma = A_{max}/\sqrt{P_{in}^{total}}$ with A_{max} and P_{in}^{total} being the maximum permissible amplitude and the average power of the OFDM signal before clipping, respectively.

III. Channel Capacity

By the central limit theorem, the distribution of distortion components of the clipped OFDM signal can be shown to approach Gaussian for large N. Let $P_{in}[k]$ and $P_{out,s}[k]$ denote the average (useful) signal power of the kth subcarrier before and after clipping, respectively. Let $P_d[k]$ also denote the average distortion power of the kth subcarrier. Then, without any constraint in the input signal except the total input power $\sum_k P_{in}[k] = P_{in}^{total}$, the average channel capacity *per subcarrier* will be given by

$$C = \frac{1}{N} \max_{P_{in}[k]} \sum_{k=0}^{N-1} \log_2(1 + \mathrm{SNDR}_k) \quad \text{bits/subcarrier.} \quad (1)$$

[1]This work was supported in part by the Research Fellowship from the Japan Society for the Promotion of Science for Young Scientists.

The inverse of the signal-to-noise-plus-distortion ratio of the kth subcarrier is given by

$$\mathrm{SNDR}_k^{-1} = \frac{P_d[k]}{P_{out,s}[k]} + \frac{1}{N\mathrm{SNR}_c} \left\{ \frac{P_{in}^{total}}{P_{in}[k]} + \frac{P_d^{total}}{P_{out,s}[k]} \right\} \quad (2)$$

where P_d^{total} is the total average distortion power and $\mathrm{SNR}_c = P_{out}^{total}/P_{noise}$ is the channel signal-to-noise ratio, with P_{out}^{total} and P_{noise} being the total power of the output signal and AWGN at the receiver, respectively. Note that since the rectangular filter is employed, $P_{out}^{total} = \sum_{k=0}^{N-1} P_{out,s}[k] + P_d^{total}$ and $P_d^{total} = \sum_{k=0}^{N-1} P_d[k]$.

Since $P_d[k]$ is a function of all the $P_{in}[k]$, the maximization of (1) seems quite involved. Therefore, we further assume the constraint that the power allocation of each subcarrier is equal, i.e., $P_{in}[k] = P_{in}^{total}/N$ for all k. Then, (2) reduces to

$$\mathrm{SNDR}_k^{-1} = \frac{1}{\mathrm{SDR}_k} + \frac{1}{\mathrm{SNR}_c} \left\{ 1 + \frac{1}{N} \sum_{k=0}^{N-1} \frac{1}{\mathrm{SDR}_k} \right\} \quad (3)$$

where the signal-to-distortion ratio of the kth subcarrier is defined as $\mathrm{SDR}_k = \frac{P_{out,s}[k]}{P_d[k]}$, which can be easily calculated as a function of γ by use of infinite series expansion of the autocorrelation function of the input signal [4]. As a numerical example, Fig. 1 shows the asymptotic value of the average capacity for $\mathrm{SNR}_c \to \infty$ without constraint on the input signaling and $N = 512$. The derivation of channel capacity of other cases such as QPSK or 16QAM signaling is straightforward.

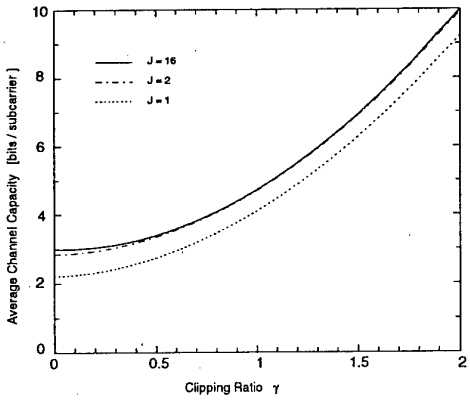


Fig.1 Asymptotic average channel capacity, $N = 512$. (The case $\gamma = 0$ corresponds to hard envelope limiter.)

References

[1] R. O'Neill and L. B. Lopes, "Envelope variations and spectral splatter in clipped multicarrier signals," in *Proc. PIMRC'95*, pp. 71–75.

[2] X. Li and L. J. Cimini, Jr., "Effects of clipping and filtering on the performance of OFDM," in *Proc. VTC'97*, pp. 1634–1638.

[3] R. Dinis, A. Gusmão, "On the performance of evaluation of OFDM transmission using clipping techniques," in *Proc. VTC'99 fall*, pp. 1634–1638.

[4] E. Costa, M. Midrio, and S. Pupolin, "Impact of amplifier nonlinearities on OFDM transmission system performance," *IEEE Commun. Lett.*, pp. 37–39, Feb. 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Construction and Performance of q-ary Turbo Codes for use with M-ary Modulation Techniques

ISIT 2000
Gregory S. White (gswhit@ftw.rsc.raytheon.com)
Raytheon
Daniel J. Costello, Jr. (Daniel.J.Costello.2@nd.edu)
Department of Electrical Engineering
University of Notre Dame
Notre Dame, Indiana 46556

This paper describes a construction technique for q-ary Turbo Codes that computes good recursive systematic convolutional q-ary constituent codes with constraint length $\nu \leq 5$ for $q = 2^m$, $m = 2, 3$, and 4. The construction technique, based on the algorithm in [1], determines the codes with maximum d_i for $i = 2, 3$, and 4 and minimum codeword multiplicity, where d_i is the minimum weight of all code sequences with input weight i. Due to the large number of encoder states involved, standard weight distribution calculations are difficult. The construction algorithm employed is a computer search that generates all possible terminating sequences of weight 2, 3, and 4 to use as inputs to the set of allowable encoders. The best codes with maximum d_i and minimum multiplicity are determined. The performance of these Turbo codes using M-ary ($M = 4, 8, 16$) non-coherent modulation (FSK) is computed by determining performance bounds assuming the parallel concatenation of two constituent codes [2]. M-ary FSK with q-ary Turbo Coding can provide an efficient modulation/coding solution. The emphasis is on matching the modulation alphabet with the Turbo coding alphabet to implement simple modulation / coding approaches that perform at a lower required E_b/N_0 and greater bandwidth efficiency than current coding approaches using these modulation techniques.

The code construction algorithm consists of searching all possible feedback polynomials of the form $H(D)=h_mD^m+h_{m-1}D^{m-1}+ \bullet \bullet \bullet + h_1D+1$ to determine a maximal length generator. This implies that the polynomial is primitive. Once a primitive polynomial H(D) is determined, the minimum parity weight p_i and codeword multiplicity N_i corresponding to input weights $i = 2, 3$, and 4 are computed. The p_i and N_i are computed by generating all possible terminating weight 2, 3, and 4 sequences to use as inputs into the encoder for all feedforward polynomials $G(D)=g_mD^m+g_{m-1}D^{m-1}+ \bullet \bullet \bullet +g_1D+1$. The construction algorithm determines all polynomials G(D) and H(D) with maximum p_i and minimum N_i for $i = 2, 3$, and 4 as described in [1]. Some of the associated weight spectra as determined by the algorithm are shown in Tables 1 and 2.

Table 1: Partial Weight Spectrum of 4-ary R=1/2 Constituent Codes

ν	# of states	p_2, N_2	p_3, N_3	p_4, N_4
1	4	2, 3	2, 3	2, 3
2	16	6, 3	3, 3	2, 3
3	64	18, 3	5, 3	3, 3
4	256	66, 3	8, 3	5, 3
5	1024	258, 3	22, 3	8, 9

Table 2: Partial Weight Spectrum of 8-ary R=1/2 Constituent Codes

ν	# of states	p_2, N_2	p_3, N_3	p_4, N_4
1	8	2, 7	2, 7	2, 7
2	64	10, 7	3, 7	3, 14
3	512	66, 7	6, 7	4, 7
4	4096	512, 7	5, 7	6, 7
5	32768	4097, 7	52, 7	3, 7

[1] S. Benedetto, R. Garello, and G. Montorsi, "A Search for Good Convolutional Codes to be Used in the Construction of Turbo Codes," *IEEE Trans. Commun.*, vol. 46, pp.1101-1105, September 1998.

[2] S. Benedetto, and G. Montorsi, "Unveiling Turbo Codes: Some Results on Parallel Concatenated Coding Schemes," *IEEE Trans. Information Theory.*, vol. 42, pp.409-428, March 1996.

This work was supported in part by NSF grant NCR95-22939, NASA grant NAG5-8355, and Raytheon Systems Company.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Multistage Turbo Decoding for Multilevel Superposition Coded Modulation Schemes

Marcelo Eduardo Pellenz[1] and Jaime Portugheis[2]
[1]PPGIA, CCET, PUCPR, R.Imaculada Conceição, 1155, 80215-901, Curitiba,PR, Brazil marcelo@ppgia.pucpr.br
[2]DECOM, FEEC, UNICAMP, CP 6101, 13083-970 Campinas, SP, Brazil jaime@decom.fee.unicamp.br

Abstract — **The design of multilevel superposition coded modulation schemes using turbo codes is addressed. A multistage decoding algorithm with reduced decoding delay is proposed. Simulation results over an impulsive noise channel are obtained.**

Recently a superposition coded modulation scheme (SCM) for transmission over a broadcast AWGN channel was proposed in [1]. The scheme uses a nonuniformly spaced 32-QAM signal constellation and multilevel coding associated with a nonstandard partition [2]. The QAM constellation consists of four 8-PSK subconstellations. The proposed scheme has two information classes, *class A* (the more important) and *class B* (the less important). In the multilevel construction, class A is associated with the first two levels (1 and 2) and class B is associated with the other levels (3,4 and 5), i. e., with the 8-PSK subconstellation. The nonstandard partition allows parallel decoding of levels 1, 2, 3 and 4. This important feature encourages the use of turbo codes as component codes of the multilevel construction in applications where there is a delay constraint. For low-to-medium bit error rates, the performance of class B can be significantly improved by using a standard partition associated with the 8-PSK subconstellation. On the other hand, the standard partition eliminates the decoding parallelism of levels 3 and 4. To circumvent this problem we propose a new multistage decoding (MSD) algorithm which partially recovers this parallelism. Consider a standard MSD (SMSD) algorithm where each component code is decoded with three iterations. We propose to use the decoding structure shown in Fig. 1 instead of SMSD for decoding the component codes of levels 3,4 and 5 (class B). After the first iteration in the third stage the subset information is passed to the fourth stage and the first iteration in this stage begins. In the same way, after this first iteration the subset information is passed to the fifth stage and the first iteration in this stage begins. The remaining iterations in each stage are now done in parallel. If D is the delay of each iteration, the total delay of the new algorithm is 5D while a SMSD algorithm has a total delay of 9D. In Fig. 1 the dashed boxes indicate additional iterations that could be done in the third and fourth stages during the same decoding interval. The decoding structure described in Fig. 1 can be easily generalized for cases where number of iterations in each stage is greater than three and/or the subset information can be passed to the subsequent stage after more than one iteration.

Fig. 2 shows simulation results for class B over an impulsive noise channel with hit probability and impulsive-to-noise power ratio equal to 0.1 and 10, respectively. The superposition gain of the SCM approach [3] was obtained for this impulsive noise channel based on a cutoff rate parameter and it justifies the approach's choice. In each partition level the turbo encoder consists of a parallel concatenation of two identically punctured 16-state RSC encoders with rates 1/2. The resulting rate distribution for class B levels is $R_3 = 0.44$, $R_4 = 0.70$ and $R_5 = 0.88$. Each turbo encoder uses a pseudo-random interleaver of size $N = 400$. All the results were obtained for MSD algorithms with 6 iterations per stage. The results for the new MSD (NMSD) algorithm are for the case of 1 (NMSD-1) and 2 (NMSD-2) initial iterations before passing information to the next stage. For a bit error rate (BER) equal to 10^{-3}, the performance degradation of NMSD-1 algorithm (delay=8D) relative to SMSD algorithm (delay=18D) is about 0.17 dB. For BER $< 10^{-3}$, the performance degradation of NMSD-2 is negligible (delay=10D). Fig. 2 also shows the performance of class B with parallel multistage decoding (PMSD) of stages 3 and 4 (one initial iteration before passing information to the fifth stage: delay=7D) which has 0.3 dB degradation relative to NMSD-1 at BER= 10^{-3}. Therefore, the new algorithm has an excellent trade-off between performance and decoding delay.

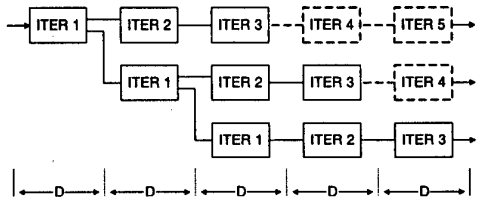


Figure 1: The proposed multistage decoding algorithm.

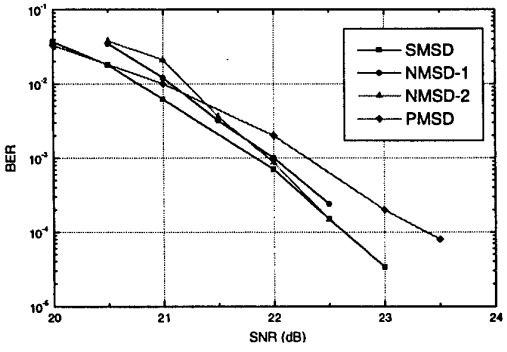


Figure 2: Performance of the new algorithm.

[0]This work was supported partially by Fundação de Amparo à Pesquisa do Estado de São Paulo under Grant 97/09347-9.

References

[1] M. E. Pellenz and J. Portugheis, "A coded modulation scheme for a broadcast AWGN channel," in *Proc. SBT/IEEE Int. Telecommun. Symp.*, pp. 458–461, August 1998.

[2] R. H. Morelos-Zaragoza, O. Y. Takeshita, H. Imai, M. P. C. Fossorier and S. Lin, "Coded modulation for satellite broadcasting," in *Proc. Globecom 1996*, pp. 31–35, 1996.

[3] S. Gadkari and K. Rose, "Time-division versus superposition coded modulation schemes for unequal error protection," IEEE Trans. Commun., vol. 47, no. 3, pp. 370–379, Mar. 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Turbo Trellis Coded Modulation on Partially Coherent Fading Channels

Allen Risley[1]
Advanced Hardware Architectures
2365 NE Hopkins Court
Pullman, WA 99163-5601 USA
e-mail: allen@aha.com

Benjamin Belzer
School of EECS
Washington State University
Pullman, WA 99164-2752 USA
e-mail: belzer@eecs.wsu.edu

Yatian Zhu
Synopsis, Inc.
700 East Middlefield Road
Mountain View, CA 94043 USA
e-mail: yzhu@synopsis.com

Abstract — **We design parallel concatenated trellis coded modulation (PC-TCM) schemes at 1 bit/sec/Hz for 8-PSK and 8-QAM over the following discrete two-dimensional (2D) channels: (a) a slow-fading Rayleigh channel with discrete carrier tracking by a phase locked loop (PLL), where the PLL signal-to-noise ratio (SNR) is proportional to the fading amplitude squared; (b) an additive white Gaussian noise (AWGN) channel with a PLL; and (c) a fast-fading Rician channel with carrier phase estimation for the line-of-sight (LOS) path only. The fading gain and phase error are assumed independent over successive symbols. The codes for channels (a) and (b) perform within 1 dB of constellation-constrained capacity at bit error rates of 10^{-6}, while those for channel (c) perform within 1.2 dB of constellation-constrained capacity for LOS-to-diffuse power ratios of 3 dB.**

I. Introduction

This work extends previous results on PC-TCM for AWGN and fading channels [1, 2], to the case of partially coherent fading channels. We consider two important causes for partial coherence: PLL phase error on slow-fading channels, and low LOS-to-diffuse power ratios on fast-fading channels. Equiprobable signaling is assumed throughout the paper.

We consider the discrete-time channel model for a correlator receiver with PLL

$$Y = AX\exp(j\phi) + N, \tag{1}$$

where X and Y are the complex channel input and output, A is the (real-valued) fading gain with $E[A^2] = 1$, ϕ is the phase error, and N is 0 mean complex AWGN with i.i.d. component variances equal to $N_0/2$. A and ϕ are independent of N. For channel (a), A is Rayleigh distributed and is known at the receiver. For channel (b), $A = 1$. For (a) and (b), ϕ has conditional Tikhonov PDF $p(\phi|A) = \exp[\rho\cos(\phi)]/(2\pi I_0(\rho))$, where loop SNR $\rho = (E_s/N_0)(\alpha A^2)/(2B_LT)$ is a function of average signal energy E_s, discrete carrier power fraction α, PLL bandwidth B_L, and symbol interval T. For channel (c), A is Rician distributed with LOS-to-diffuse power ratio β, A is unknown at the receiver, and ϕ has the angular PDF corresponding to the Rician amplitude PDF.

II. Code Design

Our codes use the bit-interleaved architecture of [1], with an additional $\times 2$ signal expansion for additional gain on fading channels. Our 1 bit/sec/Hz rate 2/6 PC-TCM consists of two 16-state rate 2/4 systematic convolutional encoders, each of which punctures one of the two systematic inputs for an effective rate of 2/3. Each encoder addresses one 8-point constellation.

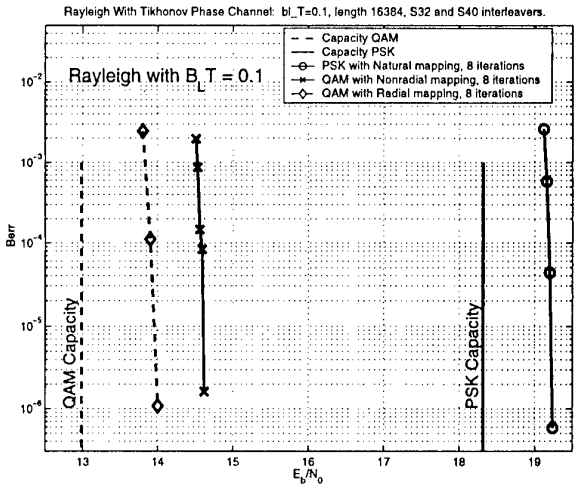


Fig. 1: PC-TCM simulation results on the slow-fading Rayleigh channel with PLL phase estimation and $B_LT = 0.1$.

We search over linear Ungerboeck encoders to maximize d^2_{eff}, the minimum squared Euclidean distance (s.E.d.) between symbol sequences corresponding to input sequences differing by weight two. We choose one encoder that provides a high and nearly equal d^2_{eff} for all constellations and mappings studied. We prove that s.E.d. is in fact the maximum likelihood code design metric for channel (c). For channels (a) and (b), the selected codes give very good performance despite the fact that s.E.d. is not the optimal design metric.

III. Simulation Results

Figure 1 presents 8-iteration turbo-decoding simulations for channel (a), with the product $B_LT = 0.1$. The MAP algorithm uses the closed form conditional channel PDF. We tested two bit mappings for the two-radius 8-QAM: the first mapped the systematic bit to the two radii, and the second attempted to minimize bit transitions between nearest neighbors. The radial mapping is best at $B_LT = 0.1$, but shows no advantage at $B_LT = 0.01$. The best case mappings perform within 1 dB of constellation constrained capacity for both 8-QAM and 8-PSK in all simulated cases.

References

[1] S. Benedetto, D. Divsalar, G. Montorsi, and F. Pollara, "Parallel concatenated trellis coded modulation," in *Proc. IEEE Int. Conf. Commun.*, pp. 974-978, June 1996.

[2] D. Divsalar and F. Pollara, "Turbo trellis coded modulation with iterative decoding for mobile satellite channels," presented at the International Mobile Satellite Conference (IMSC'97), June 1997. Available at http://www331.jpl.nasa.gov/public/tcodes-bib.html.

[1]This work was partially supported by the Spokane Intercollegiate Research and Technology Institute, grant number Y923112.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On the Performance of Turbo Coded Modulation Systems with DD and NDA Phase Synchronization

Piotr Tyczka* and Stephen G. Wilson**

*Institute of Electronics and Telecommunications, Poznań University of Technology, ul.Piotrowo 3A, 60-965 Poznań, Poland
Email: tyczka@et.put.poznan.pl

**Department of Electrical Engineering, University of Virginia, Charlottesville, VA 22903, USA, Email: sgw@virginia.edu

Abstract – **In this paper, carrier phase recovery of turbo coded modulation systems in the AWGN channel is studied. A decision-directed (DD) and non-data-aided (NDA) synchronization structures are considered. Simulation results are shown to illustrate performance of turbo coded BPSK and QPSK employing these synchronizers.**

I. Introduction and Problem Statement

Introduced in 1993 parallel concatenated convolutional codes, termed *turbo codes* [1], are very powerful error correction technique which outperforms all previously known coding schemes. Turbo codes are capable of operating very close to the Shannon limit on AWGN channels with a reasonable encoding and decoding complexity. Decoding algorithm works in an iterative manner, decoding the constituent codes of the turbo code separately and passing the symbol-likelihood information from one decoder to the other.

Coherent demodulation of carrier-modulated signals requires precise knowledge of signal frequency, phase and symbol period. Good estimation of these parameters by synchronization circuits in the receiver is essential for an overall system performance. For turbo coded signals the synchronization problem becomes especially difficult since turbo codes operate in the region of low SNR. Consequently, a question arises whether adequate synchronization can be obtained from the modulated signal itself and how much performance degradation one may expect with practical synchronization schemes compared to perfect synchronization case.

Decision-directed ML joint phase and timing synchronization for turbo codes has been studied in [2]. In this paper, we focus our attention on carrier phase recovery for turbo coded BPSK and QPSK schemes. We consider both decision-directed (DD) and non-data-aided (NDA) estimation schemes. In the communication system we analyze, the binary data stream is first differentially encoded and then, in frames of length N, passed to the turbo encoder. The output of the turbo encoder is fed to a BPSK or QPSK modulator. After transmission in an AWGN channel, the received signal is first downconverted to baseband and then carrier phase estimation followed by phase rotation are performed. Channel observations are then passed to the turbo decoder and finally, its outputs are differentially decoded to obtain the estimates of sent data bits. To solve the problem of ambiguity in the phase estimate, rotationally invariant turbo code is used.

II. DD and NDA Phase Recovery Structures

The DD synchronizer we examined is shown in Figure 1. In this structure, based on received samples r_k rotated in phase according to obtained phase estimates, tentative decisions on data are made. The tentative decisions are used then to remove data from the received signal. Phase estimates $\hat{\theta}$ are obtained from samples z_k in the phase estimator according to the ML rule:

$$\hat{\theta} = \tan^{-1}\left(\sum_{i=1}^{L} z_{k-i}^{Q} \Big/ \sum_{i=1}^{L} z_{k-i}^{I} \right) \qquad (1)$$

where L is the window length of the estimator. Phase estimates $\hat{\theta}$ are used then to multiply the input samples r_k. The resultant samples y_k are passed to a turbo decoder.

It is known that for M-PSK signals at low SNR when no reliable data estimates exist, NDA (i.e. data-independent) approach to carrier phase recovery can be employed. As a NDA carrier phase estimation scheme we investigated the Viterbi and Viterbi (V&V) synchronizer [3]. It is an efficient feedforward phase tracking scheme for M-PSK modulation, which uses nonlinear function that can be optimized to minimize phase error variance. The carrier phase estimate in our V&V synchronizer is calculated as:

$$\hat{\theta} = \frac{1}{M}\arg\left(\sum_{k=1}^{K} |r_k|^2 \cdot \exp(jM \arg(r_k)) \right) \qquad (2)$$

where K is the duration of the observation window measured in symbol intervals.

III. Numerical Results

For performance analysis of considered synchronizers in turbo systems, computer simulations were performed. We examined rate-1/2 turbo code with a 16-state $(37/31)_8$ RSC encoder and block lengths of 256, 1024 and 16384 bits. Window lengths of the estimators were selected following the results of cycle slipping analysis. Phase estimators with windows of size 30, 60 and 80 samples were studied.

The simulation results show that for both modulation schemes the DD synchronizer performs better than V&V with the same window size. However, energy loss for BPSK is of only 0.1-0.2 dB. For QPSK we observe larger SNR penalty – 0.5-0.7 dB. Comparing achieved performances with those of perfectly synchronized schemes it is seen that the turbo decoder with the DD scheme exhibits the loss of about 0.1-0.5 dB at BER=10^{-4}, depending on the window size and block length.

References

[1] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo codes," *Proc. 1993 IEEE Internat. Conf. on Commun. (ICC'93)*, Geneva, Switzerland, May 1993, pp. 1064-1070.

[2] L. Lu and S. G. Wilson, "Synchronization of turbo coded modulation systems at low SNR," *Proc. 1998 IEEE Internat. Conf. on Commun. (ICC'98)*, Atlanta, GA, USA, June 1998.

[3] A. J. Viterbi and A. M. Viterbi, "Nonlinear estimation of PSK-modulated carrier phase with application to burst digital transmission," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 543-551, July 1983.

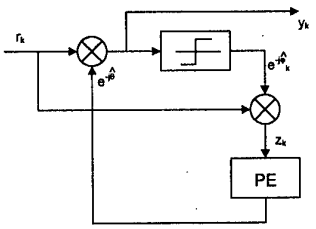


Fig. 1. Decision-directed synchronizer: PE - phase estimator.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Fast calculation of the number of the mimimum weight words for CRC codes

Peter S. Kazakov[1]
Department of Mediamatics,
Delft University of Technology,
P.O.Box 5031, 2600GA Delft,
The Netherlands

Abstract — **We investigate the main parameter in the function of undetected error probability for shortened binary cyclic codes - the number of minimum weight words A_d. Method for calculations is presented.**

I. Introduction

Let C be an $[n,k,d]$ binary cyclic code, generated by the polynomial $g(x), \deg(g) = p = n-k$. Every codeword $c(x) \in C$ can be represented as $x^p f(x) + x^p f(x)(modg(x))$, where $f(x) = f_{n-p-1}x^{n-p-1} + f_{n-p-2}x^{n-p-2} + \cdots + f_1 x + f_0$. Let $\{A_i\}_{i=0}^n$ be the weight distributions of C. A CRC code $D[n-n_c, k-n_c]$ is obtained from C by shortening in the first n_c positions. Let us denote by $A_d^{n_c}$ the number of the words of minimum weight for $D[n-n_c, k-n_c]$. For a BSC let us denote by $\varepsilon \in [0, 1/2]$ the channel error rate. Then the probability of undetected error for C is $P_{ud}(C,\varepsilon) = \sum_{i=d}^n A_i \varepsilon^i (1-\varepsilon)^{n-i}$. For low values of ε the most important parameter of the function $P_{ud}(C,\varepsilon)$ is A_d. We present a method for fast calculation of the value of A_d. This will allow us to investigate the performance of several standards for $n - n_c > 1000$. Previous algorithms for calculation of P_{ud} are due to Fujiwara-Kasami-Kitai-Lin [2] and Castagnoli-Bräuer-Herrmann [1].

II. The Method for General Case

Let $n = ord(g(x))$. We have $D[n-1, k-1] = C \cap \{c : f_{n-p-1} = 0\}$, $D[n-2, k-2] = C \cap \{c : f_{n-p-1} = f_{n-p-2} = 0\}$ and so on.

Definition 1 *Denote* $\check{C}_d = \{c : c(x) = x^p f(x) + x^p f(x)(modg(x)) \in C, wt(c) = d\}$, $Q(i) = \#\{c(x) : c(x) \in \check{C}_d, f_i = 1\}$, $Q_j(i) = \#\{c(x) : c(x) \in \check{C}_d, f_i = f_j = 1\}$.

As $C[n,k]$ is a cyclic code we have $Q = Q(0) = \cdots = Q(n-p-1) = dA_d/n$. It is clear that $Q_j = Q_j(0) = Q_{j+1}(1) = \cdots = Q_{j+n-p-1}(n-p-1)$. Let $S \subseteq \{1, \ldots, n-p-1\}$.

Definition 2 $Q_S(i) = \#\{c(x) : c(x) \in \check{C}_d, f_i = f_j = 1$ *for all* $j \in S\}$.

We have $Q_S = Q_S(0) = Q_{S+1}(1) = Q_{S+2}(2) = \ldots$ and $A_d^2 = A_d - 2Q + Q_1$; $A_d^3 = A_d - 3Q + 2Q_1 + Q_2 - Q_{1,2}$. Counting by the inclusion-exclusion principle, we obtain:

Theorem 3 *For a binary CRC code* $D[n-n_c, n-p-n_c]$ *generated by* $g(x), ord(g) = n$ *and* $1 \le n_c \le n$ *we have*

$$A_d^{n_c} = A_d - n_c Q + \sum_{i=1}^{n_c-1} \sum_{j=i+1}^{n_c} Q_{j-i} - \cdots + (-1)^d \sum_{i_1=1}^{n_c-d+1} \cdots \sum_{i_d=i_{d-1}+1}^{n_c} Q_{i_2-i_1,\ldots,i_d-i_1}.$$

III. The Method for Hamming Code

Let $g(x)$ be a primitive polynomial which generates a Hamming code $C[n,k]$, $n = 2^p - 1$. We have $Q_1 = \cdots = Q_{n-p-1} = 1$ and $Q = 2^{p-1} - 1$. By definition, we have $Q_{m,j} = 1$ iff $g(x) | x^m + x^j + 1$ and $Q_{m,j} = 0$ otherwise. Consequently $Q_{m,j}$ depends on $g(x)$ and we also write $Q_{m,j}(g)$. For the Hamming case Theorem 3 has a following form:

Theorem 4 *For binary shortened Hamming codes with* $n = 2^p - 1$, $k = n - p$ *we have*

$$A_3^{n_c} = \frac{(2^p-1)(2^{p-1}-1)}{3} - n_c(2^{p-1}-1) + \frac{n_c(n_c-1)}{2} - \sum_{j=1}^{n_c-2} \sum_{m=j+1}^{n_c-1} (n_c - m) Q_{m,j}.$$

IV. Algorithm for Computing

Let $g(x)$ be a primitive polynomial of degree p.

Definition 5 *Let us denote* $g_t(x) = \gcd(g(x^t), x^n - 1)$, *for* $gcd(t,n) = 1$.

Lemma 6 *If* $(t,n) = 1$ *then* $Q_{i,j}(g) = Q_{it(modn),jt(modn)}(g_t)$.

The polynomial $g_t(x)$ is also primitive of degree p. We calculate $Q_{m,j}$ for $g(x)$. In fact, $g_{t2^l}(x)$, $l = 0, 1, \ldots,$ are the same and we can group the coefficients t into a few sets. For each such set, we calculate the values of $Q_{it(modn),jt(modn)}(g_t)$ and $A_d^{n_c}(g_t)$. It remains to mark the minimum values of $A_3^{n_c}$.

V. Practical Realization for $p = 16$

For $d = 3$ there are 8 classes of polynomials with orders between 32768 and 65535. For each of them we calculate the values of $A_3^{n_c}$ between 32768 and its order for all sets of the class and find the best results.

Similar procedures were developed for $d = 4$.

References

[1] G. Castagnoli, S. Bräuer and M. Herrmann, Optimization of Cyclic Redundancy - Check Codes with 24 and 32 Parity Bits, *IEEE Trans. on Communications*, Vol. 41, No 6, 1993, 883-892.

[2] T. Fujiwara, T. Kasami, A. Kitai and S. Lin, On the Undetected Error Probability for Shortened Hamming Codes, *IEEE Trans. on Communications*, Vol. 33, No 6, 1985, 570-574.

[1] E-mail:peterkazakov@yahoo.com. On leave from IMI-BAS, P.O.Box 323, 5000 Veliko Tarnovo, Bulgaria.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

An Algorithm for Computing Weight Distribution of Coset Leaders of Binary Linear Block Codes

Masaya Maeda and Toru Fujiwara
Department of Informatics and Mathematical Science
Osaka University
1-3 Machikaneyama, Toyonaka, Osaka, 560-8531 Japan
e-mail: {m-maeda,fujiwara}@ics.es.osaka-u.ac.jp

Abstract — **The knowledge on the weight distribution of the coset leaders for a given binary linear code is important for the evaluation of error performance of the code. An algorithm is proposed for computing the weight distribution of the coset leaders. Using this algorithm, we have computed the weight distribution of the coset leaders of (N, K) Reed-Muller codes, binary primitive BCH codes, and their extended codes with $N \leq 128$ and $N - K \leq 42$.**

I. Weight Distribution of Coset Leaders

A minimum Hamming weight vector in a coset of an (N, K) binary linear block code C is called the *coset leader*. Let α_i denote the number of coset leaders of C whose weight is i with $0 \leq i \leq N$. Then, $\sum_{i=0}^{N} \alpha_i = 2^{N-K}$. The sequence $(\alpha_0, \alpha_1, \ldots, \alpha_N)$ is called the *weight distribution of the coset leaders* (WDCL) of C. The knowledge on WDCL is important for the evaluation of error performance of the code.

All the weight distributions of the cosets of some well-structured codes have been computed. Such codes include the r-the order Reed-Muller code of length 2^m with $r = 1$ and $m \leq 5$ and with $r = 2$ and $m = 5$, the two-error-correcting (binary primitive) BCH codes and their extended codes and some three-error-correcting extended BCH codes (see [1] for example). In [2], Wadayama *et al.* has proposed a trellis-based algorithm for computing WDCL. Using the algorithm, they have computed WDCL of Reed-Muller codes, BCH codes, and extended BCH codes with $N \leq 128$ and $N - K \leq 28$.

II. Algorithm for Computing WDCL

The algorithm proposed in [2] for computing WDCL uses a *syndrome trellis*. The straight forward way to search minimum weight paths is applying the Viterbi algorithm to the entire syndrome trellis. This computing method is simple, but the space complexity is $O(2^{N-K})$. The algorithm we propose requires smaller space complexity. The key to improve required space complexity is that we compute WDCL using two smaller syndrome trellises.

We first form a check matrix H of C in (n_1, n_2)-*normal form* as show in Figure 1. Let V_m be the set of m-tuples over GF(2), and let $w(\boldsymbol{s}, H_i), i = 1, 2$ be the weight of the coset leader $\boldsymbol{u} \in V_{n_i}$ of the code with parity check matrix H_i and $\boldsymbol{u}H_i^T = \boldsymbol{s} \in V_{r_i+r'}$. The weights, $w(\boldsymbol{s}, H_i)$ with every $\boldsymbol{s} \in V_{r_i+r'}$, are computed using two syndrome trellises constructed for H_1 and H_2 with total space complexity of $O(2^{\max\{r_1,r_2\}+r'})$. Then the weights of the coset leaders of C can be computed using the following theorem.

Theorem 1. *For $\boldsymbol{s}_1 \in V_{r_1}, \boldsymbol{s}_2 \in V_{r_2}$, and $\boldsymbol{s}' \in V_{r'}$, $w(\boldsymbol{s}_1 \circ \boldsymbol{s}' \circ \boldsymbol{s}_2, H) = \min_{\boldsymbol{s}'' \in V_{r'}} \{w(\boldsymbol{s}_1 \circ \boldsymbol{s}'', H_1) + w((\boldsymbol{s}' + \boldsymbol{s}'') \circ \boldsymbol{s}_2, H_2)\}$.* □

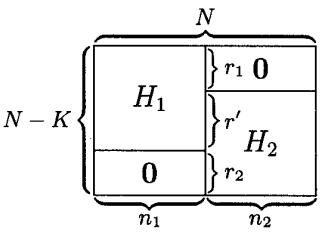


Figure 1: Check matrix in (n_1, n_2)-normal form.

Here $\boldsymbol{u} \circ \boldsymbol{v}$ denote the concatenation of vectors $\boldsymbol{u}$ and $\boldsymbol{v}$. The additional space complexity to compute the above formula is only $O(N)$. Therefore the total space complexity of our algorithm is $O(N + 2^{\max\{r_1,r_2\}+r'})$.

III. Computational Results

Using the proposed algorithm, we have newly computed WDCLs for the $(64, 22)$ and $(128, 99)$ Reed-Muller codes, the $(63, 24)$, $(63, 30)$, and $(127, 92)$ binary primitive BCH codes, and the $(64, 24)$, $(64, 30)$, $(128, 92)$, and $(128, 99)$ extended binary primitive BCH codes. The WDCLs for the $(64, 30)$ extended binary primitive BCH code and the $(128, 99)$ Reed-Muller code are shown in Table 1.

Table 1: WDCLs for the EBCH(64,30) and RM(128,99) codes.

	EBCH(64,30)	RM(128,99)
α_0	1	1
α_1	64	128
α_2	2,016	8,128
α_3	41,664	341,376
α_4	635,376	5,293,995
α_5	7,624,512	42,330,624
α_6	74,974,368	148,487,892
α_7	607,475,136	225,763,328
α_8	3,598,400,997	114,645,440
α_9	7,749,340,480	0
α_{10}	4,915,906,912	0
α_{11}	225,452,736	0

References

[1] P. Charpin, "Weight distributions of cosets of two-error-correcting binary BCH codes, extended or not," *IEEE Trans. Inform. Theory*, vol. 40, pp. 1425–1442, Sept. 1994.

[2] T. Wadayama, K. Wakasugi, and M. Kasahara, "A trellis-based algorithm for computing weight distribution of coset leaders for binary linear codes," *Proc. the 1998 Int. Symp. on Inform. Theory & Appl.*, pp. 693–696, Mexico City, Oct. 1998.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

The Weight Distributions of Some Product Codes

Richard Andrew
College of Aeronautics, Cranfield University, Bedford, UK.
e-mail: r.andrew@ieee.org

Abstract — **General expressions are derived for the weight distributions of the binary product codes $\mathcal{S}_{m_1} \otimes \mathcal{S}_{m_2}$, $\mathcal{R}_{m_1} \otimes \mathcal{R}_{m_2}$, $\mathcal{S}_{m_1} \otimes \mathcal{R}_{m_2}$, $\mathcal{E}_{m_1} \otimes \mathcal{S}_{m_2}$, and $\mathcal{E}_{m_1} \otimes \mathcal{R}_{m_2}$, where $\mathcal{S}_m$ is the $[2^m - 1, m, 2^{m-1}]$ simplex code, $\mathcal{R}_m$ is the $[2^m, m+1, 2^{m-1}]$ first order Reed Muller code, and $\mathcal{E}_m$ is the $[m, m-1, 2]$ even weight code.**

I. Summary

Previous Work: The weight distributions of most families of product codes are unknown. MacWilliams and Sloane [1] give the weights which occur in the product of simplex codes. Tolhuizen et al. [2] have determined the number of codewords of low weight for arbitrary linear row and column codes. The weight enumerator of the dual of the product of even parity codes is also known [3].

Preliminaries: Consider linear $[n_i, k_i, d_i]$ codes $\mathcal{C}_i$ for $i = 1, 2$ over $GF(q)$. Their direct product $\mathcal{C}_1 \otimes \mathcal{C}_2$ is a $[n_1 n_2, k_1 k_2, d_1 d_2]$ linear code whose codewords $\mathcal{A}$ form an $n_1 \times n_2$ matrix whose columns are codewords of $\mathcal{C}_1$ and whose rows are codewords of $\mathcal{C}_2$. $\mathcal{A}$ contains a $k_1 \times k_2$ submatrix $\mathcal{M}$ of information symbols. Define as *information columns*, those columns of $\mathcal{A}$ coinciding with columns of $\mathcal{M}$; define remaining columns as *parity check columns*. The parity check columns of $\mathcal{C}_1 \otimes \mathcal{C}_2$ are defined by the same linear combinations of information columns as the parity check bits of $\mathcal{C}_2$ are linear combinations of the information bits. Clearly, rank $\mathcal{A}$ = rank $\mathcal{M}$.

Main Results: The weight distributions of five families of product code are given in Theorems 1—5. Outline proofs are given only for Theorems 1—2.

Theorem 1 *In the product $\mathcal{S}_{m_1} \otimes \mathcal{S}_{m_2}$ of simplex codes, $A_i = 0$ unless $i = \mu(r) = 2^{m_1+m_2-1} - 2^{m_1+m_2-1-r}$ for $r = 0, 1, \ldots, \min\{m_1, m_2\}$. Then $A_0 = 1$, and*

$$A_{\mu(r)} = \prod_{i=0}^{r-1} \frac{(2^{m_1} - 2^i)(2^{m_2} - 2^i)}{2^r - 2^i}$$

for $r = 1, 2, \ldots, \min\{m_1, m_2\}$.

Outline of proof: If rank $\mathcal{M} = r$, the $2^{m_2} - 1$ columns of $\mathcal{A}$ comprise all $2^r - 1$ non-zero codewords of an r-dimensional subcode of $\mathcal{S}_{m_1}$ repeated 2^{m_2-r} times, and additionally, $2^{m_2-r} - 1$ zero columns. $A_{\mu(r)}$ equals the number of distinct $m_1 \times m_2$ matrices of rank r.

Theorem 2 *In the product $\mathcal{R}_{m_1} \otimes \mathcal{R}_{m_2}$ of first order Reed Muller codes, $A_i = 0$ unless $i = \mu(r) = 2^{m_1+m_2-1} \pm 2^{m_1+m_2-1-r}$ for $r = 0, 1, \ldots, m$ or $i = 2^{m_1+m_2-1}$. Then $A_0 = A_{2^{m_1+m_2}} = 1$, and*

$$A_{\mu(r)} = \prod_{i=0}^{r-1} \frac{(2^{m_1+1} - 2^{i+1})(2^{m_2+1} - 2^{i+1})}{2^r - 2^i}$$

for $r = 1, 2, \ldots, \min\{m_1, m_2\}$. There is no explicit expression for $A_{2^{m_1+m_2-1}}$ which is determined by $\sum A_i = 2^{(m_1+1)(m_2+1)}$.

Outline of proof: If rank $\mathcal{M} = r$, the 2^{m_2} columns of $\mathcal{A}$ comprise all codewords of either (i) a coset of $x \in \mathcal{R}_{m_1}$ on an $r-1$-dimensional subcode of $\mathcal{R}_{m_1}$ repeated 2^{m_2-r+1} times, or (ii) an r-dimensional subcode of $\mathcal{R}_{m_1}$ repeated 2^{m_2-r} times. $A_{\mu(r)}$ equals the number of distinct $\mathcal{M}$ corresponding to (ii) in which the subcode does not contain the codeword of weight 2^{m_1}.

Theorem 3 *In the product $\mathcal{S}_{m_1} \otimes \mathcal{R}_{m_2}$ of a simplex code and a first order Reed Muller code, $A_i = 0$ unless $i = \mu(r) = 2^{m_1+m_2-1} - 2^{m_1+m_2-1-r}$ for $r = 0, 1, \ldots, \min\{m_1, m_2\}$ or $i = 2^{m_1+m_2-1}$. Then $A_0 = 1$, and*

$$A_{\mu(r)} = \prod_{i=0}^{r-1} \frac{(2^{m_1} - 2^i)(2^{m_2+1} - 2^{i+1})}{2^r - 2^i}$$

for $r = 1, 2, \ldots, \min\{m_1, m_2\}$. There is no explicit expression for $A_{2^{m_1+m_2-1}}$ which is determined by $\sum A_i = 2^{m_1(m_2+1)}$.

Theorem 4 *In the product $\mathcal{E}_{m_1} \otimes \mathcal{S}_{m_2}$ of an even weight and a simplex code, $A_i = 0$ unless $i = \mu(r) = r2^{m_2-1}$ for $r = 0, 2, 3, \ldots, m_1$. Then $A_0 = 1$, and*

$$A_{\mu(r)} = 2^{-m_2} \binom{m_1}{r} \{(2^{m_2} - 1)^r + (-1)^r (2^{m_2} - 1)\}$$

for $r = 2, 3, \ldots, m_1$.

Theorem 5 *The product $\mathcal{E}_{m_1} \otimes \mathcal{R}_{m_2}$ of an even weight and first order Reed Muller code has non-zero codewords of weight*

$$\mu(i) = (m_1 + i)2^{m_2-1}, \qquad 0 \le |i| \le m_1 - 2$$

and, iff m_1 is even, a single codeword of weight $m_1 2^{m_2}$. The number of codewords of weight $\mu(i)$ is

$$A_{\mu(i)} = H_i + \sum_{j=|i|}^{\lfloor \frac{m_1+|i|}{2} \rfloor - 1} \binom{m_1}{2j - |i|} \binom{2j - |i|}{j} B_{m_1-2j+|i|}$$

where

$$B_r = \frac{(2^{m_2} - 1)^r + (-1)^r (2^{m_2} - 1)}{2^{m_2+1-r}}$$

for $r = 2, 3, \ldots, m_1$, and $H_i = \binom{m_1}{\frac{m_1+i}{2}}$ if $m_1 + i \equiv 0 \pmod 4$, and is 0 otherwise.

References

[1] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*. Amsterdam, North-Holland, 1977.

[2] L.Tolhuizen, C.Baggen and E.Hekstra-Nowacka, 'Union Bounds on the Performance of Product Codes', *Proc. IEEE Int. Symp. on Information Theory*, p. 267, Cambridge, MA, 1998.

[3] C. Leung, 'Evaluation of the Undetected Error Probability of Single Parity-Check Product Codes', *IEEE Trans. Comms.* vol. COM-31, pp. 250–253, 1983.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Determination of the Asymptotic Largest Minimum Distance of Block Codes

Tzong-Yow Lee
Dept. of Mathematics
University of Maryland
College Park, MD 20742, U.S.A
e-mail: tyl@math.umd.edu

Po-Ning Chen
Dept. of Communication Engineering
National Chiao Tung University
Hsin Chu, Taiwan 30050, R.O.C.
e-mail: poning@cc.nctu.edu.tw

Yunghsiang S. Han
Dept. of Computer Science and Information Engineering
National Chi Nan University
Nan Tou, Taiwan, R.O.C.
e-mail: yshan@csie.ncnu.edu.tw

Abstract — **In this paper, we present a general formula for the asymptotic largest minimum distance (in blocklength) of deterministic block codes under *generalized* distance functions (not necessarily additive, symmetric and bounded). An alternative expression for the same formula, which is useful in characterizing the general Varshamov-Gilbert bound, is next addressed.**

I. Introduction

The problem of determining the asymptotic largest minimum distance among block codes can be described as follows. Determine the asymptotic ratio (in n) of n-fold largest minimum distance among M selected codewords divided by the code blocklength n, subject to a fixed rate $R \triangleq \log(M)/n$ over a given code alphabet and a given measurable function on the 'distance' between two code symbols.

Research on this problem has been done for years. Up to the present, only bounds on this ratio are established. Recently, channels without statistical assumptions such as memoryless, information stability, stationarity, causality, and ergodicity, etc., are successfully handled by employing the notions of *liminf in probability* and *limsup in probability* of the information spectrum [2]. Inspired by such probabilistic methodology, together with random-coding scheme with expurgation, a spectrum formula on the largest minimum distance of deterministic block codes for *generalized* distance functions (not necessarily additive, symmetric and bounded) is established [1]. An alternative expression for the same formula in term of large deviations is next addressed.

II. Formulas for the Asymptotic Largest Minimum Distance of Block Codes

Denote the n-tuple code alphabet by $\mathcal{X}^n$. For any two elements $\hat{x}^n$ and x^n in $\mathcal{X}^n$, we use $\mu_n(\hat{x}^n, x^n)$ to denote the n-fold measure on the "distance" of these two elements. A codebook with block length n and size M is represented by

$$\mathcal{C}_{n,M} \triangleq \left\{\mathbf{c}_0^{(n)}, \mathbf{c}_1^{(n)}, \mathbf{c}_2^{(n)}, \ldots, \mathbf{c}_{M-1}^{(n)}\right\},$$

where $\mathbf{c}_m^{(n)} \triangleq (c_{m1}, c_{m2}, \ldots, c_{mn})$, and each c_{mk} belongs to $\mathcal{X}$. We define the *minimum distance* and the *largest minimum distance* respectively as

$$d_m(\mathcal{C}_{n,M}) \triangleq \min_{\substack{0 \le \hat{m} \le M-1 \\ \hat{m} \ne m}} \mu_n\left(\mathbf{c}_{\hat{m}}^{(n)}, \mathbf{c}_m^{(n)}\right)$$

and

$$d_{n,M} \triangleq \max_{\mathcal{C}_{n,M}} \min_{0 \le m \le M-1} d_m(\mathcal{C}_{n,M}).$$

Note that there is no assumption on the code alphabet $\mathcal{X}$ and the sequence of the functions $\{\mu_n(\cdot,\cdot)\}_{n \ge 1}$. For simplicity, $\hat{X}^n$ and X^n are used specifically to denote two independent random variables having common distribution P_{X^n} throughout. The natural logarithm is employed unless otherwise stated.

Theorem 1 (distance-spectrum formula)

$$\sup_{\mathbf{X}} \bar{\Lambda}_{\mathbf{X}}(R) \ge \limsup_{n \to \infty} \frac{d_{n,M}}{n} \ge \sup_{\mathbf{X}} \bar{\Lambda}_{\mathbf{X}}(R+\delta)$$

and

$$\sup_{\mathbf{X}} \underline{\Lambda}_{\mathbf{X}}(R) \ge \liminf_{n \to \infty} \frac{d_{n,M}}{n} \ge \sup_{\mathbf{X}} \underline{\Lambda}_{\mathbf{X}}(R+\delta)$$

for every $\delta > 0$, where

$$\bar{\Lambda}_{\mathbf{X}}(R) \triangleq \inf\left\{a \in \Re : \limsup_{n \to \infty}\left(Pr\left\{\frac{\mu(\hat{X}^n, X^n)}{n} > a\right\}\right)^M = 0\right\}$$

and

$$\underline{\Lambda}_{\mathbf{X}}(R) \triangleq \inf\left\{a \in \Re : \liminf_{n \to \infty}\left(Pr\left\{\frac{\mu(\hat{X}^n, X^n)}{n} > a\right\}\right)^M = 0\right\}.$$

We next derive an alternative expression for the formulas derived above.

Lemma 1 (large deviation formulas for $\bar{\Lambda}_{\mathbf{X}}(R)$ and $\underline{\Lambda}_{\mathbf{X}}(R)$)

$$\bar{\Lambda}_{\mathbf{X}}(R) = \inf\left\{a \in \Re : \bar{\ell}_{\mathbf{X}}(a) < R\right\}$$

and

$$\underline{\Lambda}_{\mathbf{X}}(R) = \inf\left\{a \in \Re : \underline{\ell}_{\mathbf{X}}(a) < R\right\}$$

where $\bar{\ell}_{\mathbf{X}}(a)$ and $\underline{\ell}_{\mathbf{X}}(a)$ are respectively the sup- and the inf-large deviation spectrums of $(1/n)\mu_n(\hat{X}^n, X^n)$, defined as

$$\bar{\ell}_{\mathbf{X}}(a) \triangleq \limsup_{n \to \infty} -\frac{1}{n} \log Pr\left\{\frac{1}{n}\mu_n(\hat{X}^n, X^n) \le a\right\}$$

and

$$\underline{\ell}_{\mathbf{X}}(a) \triangleq \liminf_{n \to \infty} -\frac{1}{n} \log Pr\left\{\frac{1}{n}\mu_n(\hat{X}^n, X^n) \le a\right\}.$$

[1] This work was supported by National Science Council, Taiwan, R.O.C., from NSC 87-2213-E-009-139- and by Univ. of Maryland, College Park, MD, U.S.A.

References

[1] P.-N. Chen, T.-Y. Lee and Y.-S. Han, "Distance-spectrum formulas on the largest minimum distance of block codes," to appear, *IEEE Trans. Inform. Theory*, May 2000.

[2] S. Verdú and T. S. Han, "A general formula for channel capacity," *IEEE Trans. Inform. Theory*, Vol. 40, No. 4, pp. 1147–1157, July 1994.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Regressive Channel Coding with Sequential Decoding for Embedded Source Coders

Thomas Stockhammer
Inst. for Communications Eng.
Munich University of Technology
D-80290 Munich, Germany
e-mail: stockhammer@ei.tum.de

Christian Weiß
Inst. for Communications Eng.
Munich University of Technology
D-80290 Munich, Germany
e-mail: weiss@lnt.ei.tum.de

Joachim Hagenauer
Inst. for Communications Eng.
Munich University of Technology
D-80290 Munich, Germany
e-mail: hagenauer@lnt.ei.tum.de

Abstract — **An adaptive error protection scheme for embedded source coders is presented. Convolutional codes of very high memory and regressive redundancy are applied to encode the data frame of the source. The channel decoder with scalable complexity and delay employs modified sequential decoding. In contrast to conventional coding systems, the principal idea of this new algorithm, the 'Far End Error Decoder (FEED)' is to delay the first error as far to the end of the frame as possible rather than to aim at a low average error rate. The proposed system is particularly appropriate for transmitting over strongly varying channels.**

I. Introduction

In todays heterogeneous network and application world communications takes place between users with a wide range of different bandwidth resources, computational capabilities, performance requirements and transmission conditions. This has initiated a growing interest in multiresolution or progressive transmission source coding. Multiresolution source coders are data compression algorithms in which simple low-rate source descriptions are embedded in more complex high-rate descriptions. Therefore, we refer to these coders as embedded source coders. While for multiresolution coders [1] the refinement steps are large, we usually have very small step sizes in case of progressive coding. In principle each bit could refine the information, i.e., lower the distortion. Theoretical analysis [1, 2] and practical applications in image coding [3] show that the loss due to progressive transmission is almost negligible, considering the advantages provided by progressive source coders.

However, the performance of these coders in error prone environments like, e.g., mobile channels degrades significantly as only a single error in the low-rate description usually results in a useless high-rate description. To avoid the complete loss of the low-rate description unequal error protection (UEP) schemes are applied to embedded source coders [5]. Additionally, using data after the first (undetected) channel decoding error for source reconstruction in general does not improve, but might even decrease the quality. Therefore, localizing the first error is essential. This requires an outer error detection code if the inner code is a convolutional code. To avoid a huge overhead due to this error detection coding, the source data has to be blocked in relatively large units. Hence, standard coding schemes are not appropriate for embedded source coders. We will present an error protection scheme adapted to embedded source coders.

II. Far End Error Decoding

Following the discussion above, the progressively coded source does not require a certain frame or bit error rate but rather an error-free part from the beginning of the frame as far to the end as possible. The key feature of our channel coding system therefore is the Far End Error Decoder (FEED) which delays the first decoding error as far out as possible. To achieve this we employ

- very high memory systematic convolutional codes,
- a regressive redundancy profile by puncturing (results from channel and source optimized UEP and rate allocation based on cutoff rate consideration),
- a modified sequential decoding algorithm with a certain computational resource per frame [4], and
- determination of the virtual error free part.

For more details see [4]. The principle of our new method is not to deliver the whole data block to the source decoder but to deliver only the error free part from the beginning of the data block up to the first bit error. This is quite natural as the interpretation of the later bits by the source decoder after an error occured is wrong anyway as outlined before.

III. Conclusions

The decoding method is self-adaptive to varying and unknown channel conditions (interference, fading, packet loss) and provides graceful degradation. The presented source and channel coding system is appropriate for compound channels where the transmitter is usually not aware of the transmission conditions (Internet, mobile channels) or it has to transmit to several or many users with different receiving conditions at the same time (broadcast). Additionally, our new method provides a trade-off between complexity and quality due to the sequential decoding unit. Therefore, we conclude that the far end error decoding (FEED) algorithm is a well adapted error protection method for the huge amount of existing and upcoming progressive source coding algorithms.

References

[1] M. Effros, "Distortion-Rate Bounds for Fixed- and Variable-Rate Multiresolution Source Codes" *IEEE Trans. Info. Theory*, pp. 1887-1920, Sep. 1999.

[2] M. J. Dürst, "The Progressive Transmission Disadvantage" *IEEE Trans. Info. Theory*, pp. 347-350, Jan. 1997.

[3] A. Said and W.A. Pearlman, "A new, fast, and efficient image codec based on set partitioning in hierarchical trees" *IEEE Trans. on Circuits and Systems for Video Technology*, pp. 243-250, Jun. 1996.

[4] J. Hagenauer, T. Stockhammer, C. Weiß, and A. Donner "Progressive Source Coding Combined with Regressive Channel Coding on Varying Channels" *Proc. 3rd ITG Conference Source and Channel Coding*, pp. 123-130, Jan. 2000.

[5] P.G. Sherwood and K. Zeger, "Error Protection for Progressive Image Transmission Over Memoryless and Fading Channels," *IEEE Trans. Comm.*, pp. 1555–1559, Dec. 1998.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Probability of Deficient Decoding in Sequential Decoding

Takeshi Hashimoto
Dept. Electronic Engineering, University of Electro-Communications
Chofu, Tokyo 182-8585, Japan
e-mail: hasimoto@itl.ee.uec.ac.jp

Abstract — **The deficient probability is the probability that a sequential decoder fails to decode the received data. For Jelinek's sequential decoder model, we give an asymptotically tight bound for it here.**

I. Introduction

Jelinek introduced the term "deficient decoding" to refer to decoding failure caused either by decoding error, by buffer overflow, or by other impairment [1]. It is well known [2] that the number of computational efforts obeys the Pareto distribution for DMC's and that it is this distribution that hinders proper decoding at high rates. It is believed that the probability of deficient decoding decreases proportionally to $N^{1-\rho}$ as a function of the decoder buffer size N whenever the rate satisfies $E_o(\rho)/\rho = R$. Simulation results confirm this statement but there has been no rigorous proof for it.

II. Convolutional code and the Fano algorithm

Consider a DMC with input and output alphabets A and B respectively and suppose that message sequences $\mathbf{u} = u_1 u_2 \ldots$ over GF(q) appear with equal probability. For each u_i, the encoder of rate $R = \frac{1}{\nu}\log q$ first calculates $s_{i,1}s_{i,2}\ldots s_{i,\nu}$ by

$$s_{i,j} = \sum_{k=0}^{K-1} u_{i-k} g_{k+1,j}, \qquad j = 1, 2, \ldots, \nu, \tag{1}$$

adds a bias sequence over GF(q) as

$$z_{i,j} \triangleq s_{i,j} + v_{i,j}, \qquad j = 1, 2, \ldots, \nu, \tag{2}$$

and generates channel input $x_{i,1}x_{i,2}\ldots x_{i,\nu}$ according to the transformation

$$z \to x, \qquad \text{whenever } z \in F(x) \text{ for } x \in A, \tag{3}$$

where $\{F(a),\ a \in A\}$ is a partition of GF(q) into $|A|$ subsets.

When $g_{i,j}$ and $v_{i,j}$ are selected randomly and independently of each other from GF(q), then (1)-(3) define a random ensemble of convolutional codes with the symbol probability $r(a) = |F(a)|/q$. For this input probability assignment r, we let $P(b) \triangleq \sum_{a\in A} r(a)P(b|a)$.

In the q-ary *code tree*, a message $\mathbf{u}^\ell = u_1 u_2 \ldots u_\ell$ uniquely specifies a *path* of length ℓ and, hence, a *node* at level ℓ.

For a channel output sequence $\mathbf{y}^\ell = y_1 y_2 \ldots y_\ell$, we assign each node $\mathbf{u}^\ell$ with its weight

$$L(\mathbf{u}^\ell) \triangleq \sum_{i=1}^{\ell} \left[\log \frac{P(y_i|x_i)}{P(y_i)} - \nu R\right] \tag{4}$$

where $\mathbf{x}^\ell = x_1 x_2 \ldots x_\ell$ is the codeword for $\mathbf{u}^\ell$ and $P(y_i) = \prod_{j=1}^{\nu} P(y_{i,j})$. The Fano algorithm searches the code tree for the path with the largest weight.

We assume the decoder model shown in Fig. 1, where the *search unit* can retain a code tree of maximally N branches in height, and the *control unit* controls the process of sequential decoding of search depth S.

III. Probability of deficient decoding

We show the following result.

Theorem 1 *Suppose that $\rho R = E_o(\rho)$ for $\rho > 1$. Then, for an arbitrarily given $\varepsilon > 0$, the best attainable deficient probability P_G satisfies* $\inf P_G \approx \frac{\delta}{\sigma^\rho N^{\rho-1}}$ *for sufficiently large σ, S, and N, where δ is a positive number dependent on ρ.*

References

[1] F. Jelinek, *Probabilistic Information Theory.* McGraw-Hill, 1968.

[2] S. Lin and D.J. Costello, Jr., *Error Control Coding: Fundamentals and Applications.* Prentice-Hall, 1983.

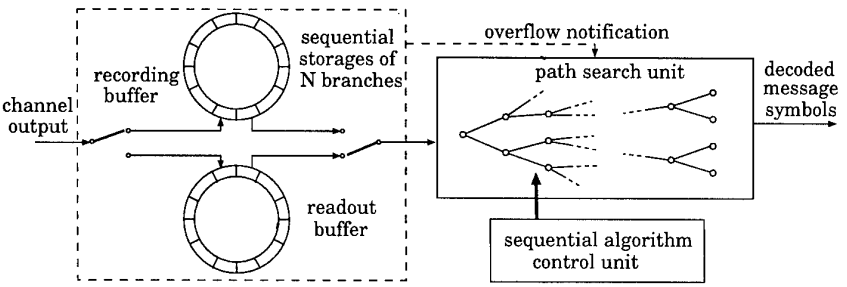


Figure 1: Sequential decoder model

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Bootstrap Sequential Decoding at High Spectral Efficiencies*

Hermano A. Cabral and Daniel J. Costello, Jr.
Dept. of Electrical Engineering
University of Notre Dame
Notre Dame, IN 46556
email: Costello.2@nd.edu

I. Introduction

Recently, sequential decoding of large memory codes has been investigated[1] for 8-PSK, 16-QAM, and larger constellations. The results show that high reliability can be achieved at channel signal-to-noise ratios (SNR's) where the code rate is nearly equal to R_0, yielding 1–1.5dB coding gain over Viterbi decoding of small memory codes. Since *Bootstrap Hybrid Decoding* (BHD)[2] is known to improve the cut-off rate of a sequential decoder for binary modulation, further improvements can be expected using this method applied to TCM.

In this paper we present a lower bound to the computational cut-off rate for the extension of the BHD scheme to TCM. Our analysis is based on the original derivation for the case of binary modulation contained in [2]. Numerical evaluations of the expressions obtained for the cases of hard-decision 8-PSK and 8-level quantized 4AM modulation show significant improvements over the usual cut-off rate, similar to the results obtained in [2] for BPSK modulation. These results suggest that performance close to capacity can be achieved with sufficiently powerful TCM systems and bootstrap sequential decoding.

II. Bootstrap Hybrid Decoding and TCM

Bootstrap Hybrid Decoding can be described as follows. The encoder takes a set of $m-1$ information sequences and computes their sum. It then encodes all m sequences using a TCM encoder and sends them over a noisy channel. Upon receiving all m sequences, the sequential decoder attempts to decode each sequence using a modified likelihood function that exploits the parity constraint introduced by the encoder. If it succeeds in decoding a sequence, it assumes the estimate is correct and subtracts it from the parity constraint. It then updates the likelihood function based on the new parity constraint and proceeds to decode the remainder of the undecoded sequences, until only one sequence remains. It follows that the decoding of each sequence helps in decoding the remaining ones, resulting in a bootstrapping effect.

III. A Lower Bound on R_0

Consider a quantized AWGN channel with input alphabet I, output alphabet J, and a set of transition probabilities $\{p(y|x); y \in J, x \in I\}$. Let $E_\infty(\sigma)$ be the Gallager function for this channel,

$$E_\infty(\sigma) = -\log \sum_{y\in J} [\sum_{x\in I} p(y|x)^{\frac{1}{1+\sigma}} \cdot p(x)]^{1+\sigma}. \qquad (1)$$

Let R be the code rate and σ_∞ be defined by $R = E_\infty(\sigma_\infty)/\sigma_\infty$. For the BHD scheme, we have to take into account the effect of the parity constraint, and thus the Gallager function is written as

$$E_k(\sigma) = -\log \sum_{\mathbf{Y}\in J^m} [\sum_{x\in I} p(\mathbf{Y}|x)^{\frac{1}{1+\sigma}} \cdot p(x)]^{1+\sigma}, \qquad (2)$$

where $J^m = J \times J \times \cdots \times J$ (m times). Let σ_k be defined by $R = E_k(\sigma_k)/\sigma_k$. Let k_R be the value of k that makes the quantities $k\sigma_\infty$ and σ_k the closest.

The main theorem can now be stated as follows:

Theorem 1 *Let R be the code rate in each of the m streams in the BHD scheme. Let C be the number of computations per decoded bit performed by the BHD decoder. Then, the l-th moment of C, $E[C^l]$, is finite as long as*

$$\min\{\sigma_{k_R}, (k_R+1)\sigma_\infty\} > l,$$

where σ_∞, σ_k, and k_R were defined above.

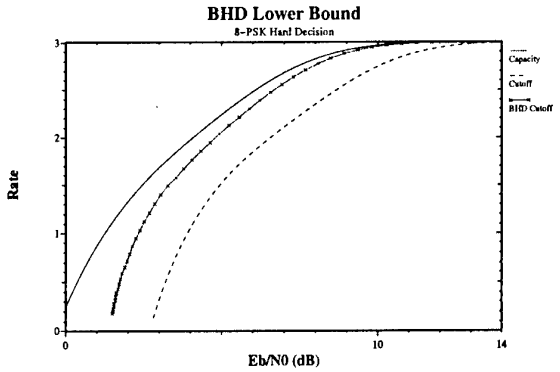


Fig. 1: Lower Bound on the cut-off for the BHD scheme with hard-decision 8-PSK.

IV. Conclusions

A lower bound to the computational cut-off rate for the BHD scheme applied to TCM was presented. Its numerical evaluation for hard-decision 8-PSK modulation (see figure 1) and 8-level quantized 4AM modulation shows that performance close to capacity is possible, and simulations with unquantized channel outputs show performance within 0.5dB of turbo TCM schemes, at a lower computational complexity. Due to its very low undetected frame error probability, the BHD scheme is very attractive in applications where reliability is of prime importance.

References

[1] F. Wang and D. Costello, Jr, "Erasure-Free Sequential Decoding of Trellis Codes." *IEEE Trans. Inform. Theory*, vol. 40, pp. 1803–1817, Nov. 1994.

[2] F. Jelinek and J. Cocke, "Bootstrap Hybrid Decoding for Symmetrical Binary Input Channels." *Information and Control*, vol. 18, no. 3, pp. 261–298, April 1971.

*This work was supported in part by NASA Grant NAG5-8355, NSF Grant NCR95-22939, and CNPq Grant 200617/94-0.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On Analysis of noiseless decision feedback scheme using fixed size list decoder for tree codes

Toshihiro Niinomi
Kanagawa Institute of Tech.,
1030 Shimo-Ogino, Atsugi-shi,
Kanagawa, 243-0292 Japan
e-mail:
niinomi@ele.kanagawa-it.ac.jp

Toshiyasu Matsushima
School of Science and Engineering,
Waseda University,
3-4-1 Ohkubo, Shinjyuku-ku,
Tokyo,169-0072 Japan

Shigeichi Hirasawa
School of Science and Engineering,
Waseda University,
3-4-1 Ohkubo, Shinjyuku-ku,
Tokyo,169-0072 Japan

Abstract — **In this paper, the generalized proof are shown for the coding theorem of [1]. Consequently, the further discussion is obtained.**

I. Introduction

Despite list decoder is seldom employed for applications, Generalized Viterbi Algorithm(GVA) use list decoder for its mean process [2]. In the analysis of the GVA, the error probability is dominated by that of list decoder. Therefore, we proposed the decision feedback scheme with GVA, which has the constructive decision rule for list decoding with feedback [1].

In this paper, the more strict bound and a certain generalization of the proof of [1] are shown. As a result, the further properties can be clarified. Throughout this paper, DMC characterized by $P = \{P_{ij},\ j \in A, i \in B\}$, and noiseless feedback is assumed.

II. The algorithm [1]

We are concerned with a q-ary tree code, each branch of which is assigned with v input alphabet. So, the rate of the code is defined by $R = \frac{1}{v}\ln q$ .A N information sequence of q-ary alphabet specifies a path, denoted by $\mathbf{u}_i{}^N$. Let the subsequence of path $\mathbf{u}_i{}^N$ from the root to the n-th level be $\mathbf{u}_i{}^n$. Furthermore, L(branches) is defined as decoding constraint length of the GVA.

{ *Initial condition and Recursive procedure* }

(Step 1)*Initial condition* : At the level $n-1$, each state of q^{L-1} has their list, namely S survivors. Each survivor of the list is labeled "Accept".

For the level n $(L \le n \le N)$, repeat (Step 2)~(Step 4), recursively.

(Step 2)*Path extension*: At the level n, all retained paths are extended by one branch as $\mathbf{u}^n = \mathbf{u}^{n-1}u$. Then each metric of Sq^L paths is calculated.

(Step 3)*Path selection*: At each state of q^{L-1}, the best S paths are selected among the qS paths as the list.

(Step 4)*Testing*: We denote the selected list as $\mathcal{L}$, $\mathcal{L} = \{\mathbf{u}^n_{(1)}, \mathbf{u}^n_{(2)}, \cdots, \mathbf{u}^n_{(S)}\}$, and $\mathbf{u}^n_{(S+1)}$ is the $S+1$-th most path at the state [1]. The listed paths are labeled "Accept" or "Reject" by the following decision rule. However, a path once labeled "Reject" is kept its label "Reject". The rule is if $\frac{Pr(\mathbf{y}^{vn}|\mathbf{u}_{(1)}{}^n)}{Pr(\mathbf{y}^{vn}|\mathbf{u}_{(S+1)}{}^n)} \le \Delta, \Delta \ge 1$ holds, $\mathbf{u}^n_{(i)}, i = 1, 2, \cdots, S$ are labeled "Reject". Otherwise, $\mathbf{u}^n_{(i)}, i = 1, 2, \cdots, S$ are labeled "Accept". If there is no survivor labeled "Accept" at any q^{L-1} state, the retransmission is required and restart from Step 1.

{ *Final path selection at the check tail* }

By $L-1$ known symbols, q^{L-1} lists are reduced to one list with Step 2 ~Step 4. Then, by $T-(L-1)$ known symbols, the best path is selected among the S survivors of the final list. If the label of the best path is "Reject", the retransmission is required and restart from Step 1.

[1]For the received sub-sequence $\mathbf{y}^{vn}$ from root to level n , we denote the likelihood of the k-th most path as $Pr(\mathbf{y}^{vn}|\mathbf{u}_{(k)}{}^n)$.

III. Main results

Though the analysis in [1] depends on each tree configuration [5], the bounds newly obtained are independent. So, we newly observe the case that S is very large. For obtaining the feedback exponent $-\frac{1}{vL}\ln Pr(E_2)$ of Forney [4], we take Δ as $-\frac{1}{vL}\ln Pr(E_1) \to 0$ $(L \to \infty)$, where $Pr(E_1)$ and $Pr(E_2)$ is Pr[The decoding error occurs, or, the retransmission is required.] and Pr[The decoding error occurs.], respectively. We show this result as Theorem.

[Theorem]As $S \to \infty$, the exponent approaches to $e_1^{(\infty)}(R)$,

$$e_1^{(\infty)}(R) = \max_{\mathbf{q},\alpha,\beta\in\mathcal{D}_4}\left\{E_o(1,\alpha,\beta,\mathbf{q}) + \alpha\cdot e_F^{(1)}(R)\right\},$$

$$\mathcal{D}_4 = \{\alpha \ge 0,\ \beta \ge 0, \epsilon_e = E_o(1,\alpha,\beta,\mathbf{q}) - \beta R > 0\}.$$

$$E_o(S,\sigma_x,\rho_x,\mathbf{q})$$

$$= -\ln\left[\sum_{j\in B}\left(\sum_{i\in A} q_i P_{ji}^{1-S\sigma_x}\right)\left(\sum_{k\in A} q_k P_{jk}^{\sigma_x/\rho_x}\right)^{S\rho_x}\right],$$

$$e_F^{(S)}(R) = \max_{\mathbf{q},\nu\in\mathcal{D}_3} E_{oF}(S,\nu,\mathbf{q}),$$

$$\mathcal{D}_3 = \{E_{oF}(S,\nu,\mathbf{q}) - \nu SR > 0,\quad \nu > 0\}$$

$$E_{oF}(S,\nu,\mathbf{q}) = S\sum_{k\in B}\sum_{j\in A} q_j P_{kj}\ln\left[\frac{P_{kj}^{1/\nu}}{\sum_{j\in A} q_j {P_{kj}}^{1/\nu}}\right]^{\nu}$$

IV. Conclusion

We show the properties of the decision feedback scheme using fixed size list decoder, especially the size of list is very large. The exponents we have obtained have the similar properties to those of the GVA.

References

[1] T.Niinomi, T.Matsushima and S.Hirasawa, "A decision feedback scheme using list decoding for tree codes", IEICE Trans. A, Vol.83, No.1, Jan. 2000 (in Japanese).

[2] T.Hashimoto, "A list-type reduced-constraint generalization of the Viterbi algorithm", IEEE Trans. Inf.Theory vol.IT-33, pp.866-876, Nov.1987.

[3] T.Hashimoto, "On the error exponent of convolutionaly coded ARQ", IEEE Trans. Inf.Theory vol.IT-40, pp.567-575, Mar.1994.

[4] G.D.Forney,Jr., "Exponential error bounds for erasure, list and decision feedback schemes", IEEE Trans.Inf.Theory vol.IT-14, pp.206-220, Mar.1968.

[5] G.D.Forney,Jr., "Convolutional codes II : Maximum likelihood decoding", Inf.Control. vol.25, pp.222-266, Jul.1974.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Performance of Universal Portfolios in the Stock Market[1]

Tom Cover
Information Systems Laboratory
Stanford University
Packard Bldg., Rm 254
Stanford, CA 94305
cover@isl.stanford.edu

David Julian
Information Systems Laboratory
Stanford University
Packard Bldg., Rm 251
Stanford, CA 94305
djulian@stanford.edu

Abstract — **We compare the theoretical and empirical performance of horizon-free universal portfolios for a large number of stock pairs using real stock market data in two scenarios: with and without side information, and with and without short selling.**

I. Summary

The horizon-free μ-weighted universal portfolio is a sequential investment algorithm that has been shown to perform as well as the best constant rebalanced portfolio to first order in the exponent (cf. [1]). Additionally, a number of theoretical properties of the universal portfolio have been derived. We are interested in the performance of the universal portfolio in the actual stock market and how this performance compares with the theory. To this end, we determine the performance of horizon-free universal portfolios for a large number of stock pairs using real stock market data in two scenarios: with and without side information, and with and without short selling.

First, we observe for a large number of stock pairs that the n-day universal portfolio return $\hat{S}_n$ consistently performs near the best achievable constant rebalanced portfolio return S_n^*, and a factor of 28 better than the minimax lower bound of $V_n S_n^*$ established in [3], where $V_n = \left[\sum \binom{n}{n_1,\ldots,n_m} 2^{-nH(n_1/n,\ldots,n_m/n)}\right]^{-1}$, thus indicating that the market is not maximally hostile. We also compute the ratio $S_n^*/\hat{S}_n$ for real data and compare it to the theoretical asymptote $\frac{|J_n|^{(1/2)}}{(m-1)!(2\pi/n)^{(m-1)/2}}$, where m is the number of stocks and J_n is the sensitivity matrix (cf. [1].).

We then extend the universal portfolio by using side information to assign days to certain states, and utilize state constant rebalanced portfolios as in [2]. For a state constant rebalanced portfolio the trading days are divided up into subsequences based on the state information. A constant rebalanced portfolio is then used independently on each subsequence of days. One example of side information y_i for a pair of stocks is to assign each day i to one of two states, 1 or 2, corresponding to the stock with the larger windowed moving average of price relatives for the last k days. The best constant rebalanced portfolio b_i^* and the universal portfolio $\hat{b}_i$ are based on the current and past state information y^i and past price relatives $\mathbf{x}^{i-1}$. The best constant rebalanced portfolio return $S_n^*(\mathbf{x}^n|y^n)$ is the product of the best constant rebalanced portfolio returns for the subsequence of days associated with each state:

$$S_n^*(\mathbf{x}^n|y^n) = \left(\max_b \prod_{\substack{i=1 \\ i:y_i=1}}^{n} b^t X_i\right)\left(\max_b \prod_{\substack{i=1 \\ i:y_i=2}}^{n} b^t X_i\right).$$

Similarly, $\hat{S}_n$ is the product of the wealth factors associated with the independent running of the universal portfolio on the subsequences of trading days associated with each of the states. For actual stock market data we observe that this simple nonanticipative algorithm achieves factors as large as 10^5 for some stock pairs over a twenty year period. When the side information of the windowed moving average is used for two portfolios without short selling, the log optimal portfolio b^* for each state often exhibits a "bang-bang" effect, where all the wealth is allocated to a single stock. This "bang-bang" effect often has all the wealth pouring into the stock which has been underperforming. Additionally, the "bang-bang" effect indicates that even more wealth can be generated by selling one stock short and buying more of the other. Consequently, we analyze the effect of short selling and the tradeoffs between return and amount of leverage. We also compare the performance of the μ-weighted universal portfolio with the exponentiated gradient universal portfolio as in [4]. Next, we look at the performance of the universal portfolio with and without side information, and with and without short selling for a portfolio of fifty stocks.

Finally, we explore the use of several heuristic methods for increasing the rate at which the universal portfolio learns the stock market. These methods include several ways of creating a fake market associated with the actual market, computing portfolios in the fake market, and mapping portfolios from the fake market back to the actual market.

References

[1] T. Cover, "Universal Portfolios," *Mathematical Finance*, 1(1):1-29, January 1991.

[2] T. Cover and E. Ordentlich, "Universal portfolios with side information," *IEEE Transactions on Information Theory*, 42(2):348-363, March 1996.

[3] E. Ordentlich and T. Cover, "The cost of achieving the best portfolio in hindsight," *Mathematics of Operations Research*, 23(4):960-982, November 1998.

[4] D. Helmbold, R. Schapire, Y. Singer, and M. Warmuth, "On-line portfolio selection using multiplicative updates," *Mathematical Finance*, 8(4):325-347, October 1998.

[1]This work was supported in part by NSF grant NCR-9628193. MURI DAAD19-99-1-0252 and JSEP grant DAAG55-97-1-0115.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

An Adaptive Algorithm for Log-optimal Portfolio and its Theoretical Analysis

Zhongxing Ye[1]
Dept. of Applied Mathematics
Institute of Contemporary Finance
Shanghai Jiao Tong University
Shanghai 200030, P. R. China
e-mail: zxye@mail.sjtu.edu.cn

Jianguo Huang[1]
Dept. of Applied Mathematics
Shanghai Jiao Tong University,
Shanghai, 200240, P. R. China
e-mail: jghuang@online.sh.cn

Abstract — **An adaptively random searching algorithm is proposed for log-optimal portfolio. Under reasonable conditions the convergence of this algorithm is shown. The numerical results using this algorithm for real data from Shanghai Stock Exchanges are sastisfactory.**

I. Introduction

Suppose one wishes to invest in a stock market consisting of m stocks. We denote the market by a random vector $\mathbf{X} = (X_1, X_2, \cdots, X_m)^T$, where X_i denotes the price relative of i-th stock, $i = 1, 2, \cdots, m$. $\mathbf{X}$ is supposed to be drawn according to the distribution $F(\mathbf{x}), \mathbf{x} \in \mathbf{R}^m$. A portfolio $\mathbf{b} = (b_1, b_2, \cdots, b_m)^T$, $b_i \geq 0$, $\sum b_i = 1$, is an allocation of investment capital. The expected log return $W(\mathbf{b})$ is defined by $W(\mathbf{b}) = E[\ln(\mathbf{b}^T\mathbf{x})] = \int \ln(\mathbf{b}^T\mathbf{x})dF(\mathbf{x})$. The problem is to find the optimal portforlio $\mathbf{b}^*$ to reach the maximal expected log return W^* which is defined by $W^* = \max_{\mathbf{b}} W(\mathbf{b})$. A systematic discussion can be found in Cover and Thomas' book [1, Chapter 15]. Optimization algorithms abound for this problem. Readers can refer to Cover[2], Ye and Zhang[3] and the references cited therein for details. In this paper we suggest an adaptively random searching algorithm wiich is different from the above-mentioned algorithms. The main body of the result is derived from a more general framework of constrained stochastic gradient method.

II. Main Results

The purpose is to solve the problem of finding $\mathbf{b}^*$ to achieve

$$W^* = \max_{\mathbf{b}} W(\mathbf{b}) = \max_{\mathbf{b}} \int \ln(\mathbf{b}^T\mathbf{x})dF(\mathbf{x}), \qquad (1)$$

based upon the observed data $\mathbf{x}(1), \mathbf{x}(2), \cdots, \mathbf{x}(t), \cdots$, where $\mathbf{b}(t)$ is the observed stock return vector for t-th day.

First we take a quadratic parameter transformation $b_i = w_i^2$ to change the original constraint manifold, a $(m-1)$-dimensional simplex, $B = \{\mathbf{b} : b_i \geq 0, \sum_i b_i = 1\}$ into a $(m-1)$-dimensional unit surface,

$$S^{m-1} = \{\mathbf{w} = (w_1, w_2, \cdots, w_m) : \sum_i w_i^2 = 1\}.$$

Then the problem considered becomes

$$\text{Maximize} W(\mathbf{w}) = \text{Maximize} E[f(\mathbf{w}, \mathbf{X})],$$

where $f(\mathbf{w}, \mathbf{x}) = \log(\sum_{i=1}^m w_i^2 x_i)$.

Next we propose the following algorithm to solve the above problem:

Step 0 Given any initial guess $\mathbf{w}^{(0)} \in S^{m-1}$, $t = 0$;

Step 1 Compute the modified quantities

$$\mathbf{w}^{(t+1)} = (w_1^{(t+1)}, w_2^{(t+1)}, \cdots, w_m^{(t+1)})^T$$

by the formula $\mathbf{w}^{(t+1)} = \mathbf{w}^{(t)} + \Delta\mathbf{w}^{(t)}$, where $\Delta\mathbf{w}^{(t)} = \eta(t)\text{grad}_M f(\mathbf{w}^{(t)}, \mathbf{x}^{(t)})$, $t = 0, 1, \cdots$, $\eta(t)$ is some chosen positive step size, called learning rate in general. The gradient vector is easy to compute by

$$\text{grad}_M f(\mathbf{w}^{(t)}, \mathbf{x}^{(t)}) = \{\frac{x_i(t)w_i^{(t)}}{\sum_{j=1}^m (w_j^{(t)})^2 x_j(t)} - w_i^{(t)}\}_{i=1}^m.$$

Step 2 Halt if the iteration of time reaches some predetermined number, or the norm of the difference $\mathbf{w}^{(t+1)} - \mathbf{w}^{(t)}$ is small than some given control precision; otherwise, $(t+1) \to t$, go to step 1.

The learning rate sequence $\{\eta(t)\}$ satisfies that

$$\eta(t) > 0, \sum_t \eta(t) = +\infty, \eta(t) \to 0, \text{as } t \to +\infty.$$

It is shown that under some reasonable conditions, this algorithm converges and results in the optimal portfolio $\mathbf{b}^* = (w_1^{*2}, w_2^{*2}, \cdots, w_m^{*2})^T$ which achieves

$$W^* = \max_{\mathbf{b}} W(\mathbf{b}).$$

The numerical results based on this algorithm with real data from Shanghai Stock Exchanges are satisfactory.

References

[1] T. M. Cover and J. A. Thomas, "Elements of Information Theory," *John Wiley & Sons,* Inc., New York,1991.

[2] T. M. Cover, "Universal Portfolios," *Math. Finance*, vol.1, pp. 1-29, 1991.

[3] Z. Ye and Y. J. Zhang, "Improved genetic algorithm for optimal portfolio with risk control," *J. Shanghai Jiao Tong Univ.*, vol.1, no.2, pp. 9-16,1996.

[1]This work was supported by the National Natural Science Foundation of China under the Grant No. 79790130 and 19901018.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Iterative Computation of Rate-Distortion Bounds for Scalable Source Coding

Ertem Tuncel and Kenneth Rose[1]
Dept of ECE, University of California Santa Barbara, CA 93106

We consider N-layer scalable source coding of a finite memoryless source $X \sim p_x$. Let $\mathbf{X}_i$ denote $X_1, \ldots, X_i$, where X_i is the reproduction at the ith layer. From [5], we know that a scalable coder can achieve the sequence of decreasing distortions $\mathbf{D} = \{D_i\}_{i=1}^N$ and increasing rates $\mathbf{R} = \{R_i\}_{i=1}^N$, if and only if there exists a conditional distribution $Q_{\mathbf{x}_N|x}$ such that

$$\begin{aligned} E\langle d(X, X_i)\rangle &\leq D_i \quad i = 1, \ldots, N \\ I(X; \mathbf{X}_i) &\leq R_i \quad i = 1, \ldots, N \, . \end{aligned}$$

The $2N$-dimensional achievability region $\boldsymbol{\mathcal{A}}$ is convex. Hence, in order to find a point on the boundary of $\boldsymbol{\mathcal{A}}$ with an inward normal vector $(\boldsymbol{\alpha} = \{\alpha_i\}_{i=1}^N, \boldsymbol{\beta} = \{\beta_i\}_{i=1}^N)$, we must solve the following minimization problem:

$$F_{\boldsymbol{\alpha},\boldsymbol{\beta}} = \inf_{Q_{\mathbf{x}_N|x}} \sum_{i=1}^N \alpha_i I(X; \mathbf{X}_i) + \beta_i E\langle d(X, X_i)\rangle \, .$$

The above problem was first addressed by Effros [4, Section V]. A new system of equations and inequalities regarding the optimal marginal $q_{\mathbf{x}_N}$ was formed, and all tentative solutions (extracted from the equations) were tried until the one satisfying the optimality conditions (the inequalities in the system) was found. (See [1, Section 2.6] for the details of the approach for the ordinary rate-distortion problem.) However, it was not clear how $q_{x_{i+1}|\mathbf{x}_i}$ should be defined when $q_{\mathbf{x}_i} = 0$. In fact, we showed that satisfaction of the conditions given in [4] for some assumed $q_{x_{i+1}|\mathbf{x}_i}$ when $q_{\mathbf{x}_i} = 0$, does not necessarily imply the optimality of $q_{\mathbf{x}_N}$. Moreover, this approach becomes impractical as the size of the output alphabet grows. (For an extreme example, consider continuous source and reproduction alphabets.) As a remedy, we propose an iterative algorithm which is a generalization of the Blahut-Arimoto (BA) algorithm [2] for rate-distortion computation. The algorithm is initialized with arbitrary nonzero reproduction probabilities, and monotonically approaches the optimal reproduction distribution. We also revise the optimality conditions to handle the complications that arise whenever $q_{\mathbf{x}_i} = 0$.

Let $\mathbf{Q} = \{Q_{\mathbf{x}_N|x}\}$ and $\mathbf{q} = \{q_{\mathbf{x}_N}\}$ denote, in vector notation, a random encoding, and a reproduction distribution, respectively.

Lemma 1:

$$F_{\boldsymbol{\alpha},\boldsymbol{\beta}} = \inf_{\mathbf{Q}} \inf_{\mathbf{q}} F_{\boldsymbol{\alpha},\boldsymbol{\beta}}(\mathbf{Q}, \mathbf{q}) \, ,$$

where

$$F_{\boldsymbol{\alpha},\boldsymbol{\beta}}(\mathbf{Q}, \mathbf{q}) \triangleq \sum_{i=1}^N \beta_i E_{\mathbf{Q}}\langle d(X, X_i)\rangle + \alpha_i \mathcal{D}(Q_{\mathbf{x}_i|x} p_x \| q_{\mathbf{x}_i} p_x)$$

Thus, the problem is that of double minimization and, as will be shown, is solvable by alternating minimization.

Lemma 2:

a) Given $\mathbf{Q}$, $\arg\inf_{\mathbf{q}} F_{\boldsymbol{\alpha},\boldsymbol{\beta}}(\mathbf{Q}, \mathbf{q})$ is the marginal

$$q_{\mathbf{x}_N}(\mathbf{Q}) = \sum_x p_x Q_{\mathbf{x}_N|x}$$

b) Given $\mathbf{q}$, $\arg\inf_{\mathbf{Q}} F_{\boldsymbol{\alpha},\boldsymbol{\beta}}(\mathbf{Q}, \mathbf{q})$ is given by

$$Q_{\mathbf{x}_N|x}(\mathbf{q}) = \frac{q_{\mathbf{x}_N} \exp\{-\sum_{i=1}^N \beta_i' d_{x,x_i} + \alpha_i' \log f^i_{x,\mathbf{x}_i}\}}{\sum_{\mathbf{z}_N} q_{\mathbf{z}_N} \exp\{-\sum_{i=1}^N \beta_i' d_{x,z_i} + \alpha_i' \log f^i_{x,\mathbf{z}_i}\}} \, ,$$

where $\alpha_i' = \alpha_i / \sum_{j=i}^N \alpha_j$ and $\beta_i' = \beta_i / \sum_{j=i}^N \alpha_j$, and

$$f^i_{x,\mathbf{x}_i} = \sum_{z_{i+1}} q_{z_{i+1}|\mathbf{x}_i} \exp\{-\beta_{i+1}' d_{x,z_{i+1}}\} (f^{i+1}_{x,\mathbf{x}_i,z_{i+1}})^{1-\alpha_{i+1}} \, ,$$

for $i = 1, \ldots, N-1$, and $f^N_{x,\mathbf{x}_N} = 1$.

Theorem 1: Let $\mathbf{q}^{(0)}$ be positive everywhere, and let $\mathbf{Q}^{(n)} = \mathbf{Q}(\mathbf{q}^{(n-1)})$, and $\mathbf{q}^{(n)} = \mathbf{q}(\mathbf{Q}^{(n)})$ for $n = 1, 2, 3, \ldots$. Then the sequence $\mathbf{q}^{(0)}$, $\mathbf{Q}^{(1)}$, $\mathbf{q}^{(1)}$, $\mathbf{Q}^{(2)}$, $\ldots$, converges to

$$(\mathbf{Q}^*, \mathbf{q}^*) = \arg\inf_{\mathbf{Q},\mathbf{q}} (F_{\boldsymbol{\alpha},\boldsymbol{\beta}}(\mathbf{Q}, \mathbf{q})) \, .$$

The proof follows the same line as the proof for the optimality of BA, given in [3]. Finally, the optimality conditions are given by

Theorem 2: A given $\mathbf{q}$ is optimal if and only if there exists a legitimate $q_{x_{i+1}|\mathbf{x}_i}$ for all $q_{\mathbf{x}_i} = 0$, so that

$$v_{\mathbf{x}_N} \leq v_{\mathbf{x}_{N-1}} \leq \cdots \leq v_{x_1} \leq 1 \, ,$$

for all $\mathbf{x}_N$, where

$$v_{\mathbf{x}_j} = \sum_x \frac{p_x f^j_{x,\mathbf{x}_j} \exp\{-\sum_{i=1}^j \beta_i' d_{x,x_i} + \alpha_i' \log f^i_{x,\mathbf{x}_i}\}}{\sum_{\mathbf{z}_N} q_{\mathbf{z}_N} \exp\{-\sum_{i=1}^N \beta_i' d_{x,z_i} + \alpha_i' \log f^i_{x,\mathbf{z}_i}\}} \, .$$

References

[1] T. Berger. *Rate Distortion Theory. A Mathematical Basis for Data Compression.* Prentice-Hall, Englewood Cliffs, N.J., 1971.

[2] R. E. Blahut. Computation of channel capacity and rate-distortion functions. *IEEE Trans. on Information Theory*, 18(4):460–473, July 1972.

[3] I. Csiszár. On the computation of rate-distortion functions. *IEEE Trans. on Information Theory*, 20(1):122–124, January 1974.

[4] M. Effros. Distortion-rate bounds for fixed- and variable-rate multiresolution source coding. *IEEE Trans. on Information Theory*, 45(6):1887–1910, September 1999.

[5] B. Rimoldi. Successive refinement of information: Characterization of the achievable rates. *IEEE Trans. on Information Theory*, 40(1):253–259, January 1994.

[1]This work was supported in part by the NSF under grant no. MIP-9707764, the UC MICRO program, Conexant Systems, Inc., Fujitsu Laboratories of America, Inc., Lernout & Hauspie Speech Products, Lucent Technologies, Inc. and Qualcomm, Inc.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Iterating the Arimoto-Blahut Algorithm for Faster Convergence

Jossy Sayir[1]
FTW, Maderstr. 1, A-1040 Vienna.
j.sayir@ieee.org

I. Introduction

The Arimoto-Blahut algorithm ([1], [2]) determines the capacity of a discrete memoryless channel through an iterative process in which the input probability distribution is adapted at each iteration. While it converges towards the capacity-achieving distribution for any discrete memoryless channel, the convergence can be slow when the channel has a large input alphabet. This is unfortunate when only a small number of the input letters are assigned non-zero probabilities in the capacity-achieving distribution. If we knew which input letters will end up with a probability of zero, we could eliminate these letters and operate the algorithm on a subset of the input alphabet. The algorithm would converge towards the same solution faster.

We present an algorithm which makes use of this fact to speed up the convergence of the Arimoto-Blahut algorithm in such situations. The algorithm starts with an input alphabet consisting of two symbols, then grows the alphabet by one symbol at every iteration until it includes all the symbols with non-zero probabilities. At every iteration, the Arimoto-Blahut algorithm is used to compute a capacity relative to a partial input alphabet. When our algorithm terminates, it will have found the same solution as the Arimoto-Blahut algorithm applied to the complete input alphabet. However, we cannot guarantee that our algorithm will include only symbols with non-zero probabilities in the partial alphabet it ends up with.

II. The Algorithm

Let X be the input random variable to a discrete memoryless channel, and let X take on values over the finite alphabet $\mathcal{A}$. Let Y be the output random variable of the channel and let C be its capacity. We define

$$I(X=x;Y)=\sum_y P_{Y|X}(y|x)\log\frac{P_{Y|X}(y|x)}{\sum_{x'}P_{Y|X}(y|x')P_X(x')}$$

as in [3]. Let $C_{\mathcal{A}'}$ denote the capacity of the discrete memoryless channel induced when all but the letters in the subset $\mathcal{A}'$ of $\mathcal{A}$ are forcibly assigned a probability of zero. We give an outline of our algorithm:

1. Determine $(x,y)\in\mathcal{A}^2$ which maximizes $C_{\{x,y\}}$ over all choices of x and y. Define $\mathcal{A}'=\{x,y\}$ and $C'=C_{\mathcal{A}'}$.
2. If $\mathcal{A}'=\mathcal{A}$, then $C=C'$ and the algorithm terminates. Otherwise, for all $x\in\mathcal{A}\setminus\mathcal{A}'$, compute $I(X=x;Y)$. If the values computed are all smaller or equal to C', then $C=C'$ by [3, Theorem 4.5.1] and the algorithm can be terminated at this point.
3. Add the symbol x that maximized $I(X=x;Y)$ in step 2 to the set $\mathcal{A}'$. Recompute $C'=C_{\mathcal{A}'}$ using the Arimoto-Blahut algorithm. Return to step 2.

The algorithm is certain to obtain the correct solution for the following reasons:

- When the algorithm exits in step 2 because all the values of $I(X=x;Y)$ are smaller or equal to C', the solution is guaranteed to be correct by [3, Theorem 4.5.1].
- The algorithm must eventually exit. In the worst case, it will end up including all the symbols of $\mathcal{A}$ into $\mathcal{A}'$. In this case, the last occurrence of step 3 applies the Arimoto-Blahut algorithm to the complete input alphabet. This will be the case when our iterated algorithm is applied to channels whose capacity-achieving input distributions have only non-zero terms.

As already mentioned, there is no guarantee that the algorithm will only include symbols whose probabilities in the capacity-achieving distribution are non-zero into its partial alphabet $\mathcal{A}'$. However, the practical examples for which the algorithm was tested seem to indicate that it is highly unlikely.

III. Practical Implementation and Conclusion

The practical need for such an algorithm arose in an attempt to compute the optimal coding distributions for universal lossless source coding over sets of discrete memoryless sources with monotone non-increasing probability distributions with a fixed average. The problem of determining the optimal coding distribution for universal coding over a set of probability distributions is equivalent to the problem of computing the capacity of a discrete memoryless channel [4].

For an alphabet size of 256, the problem of determining the optimal coding distribution for the set of monotone non-increasing distributions with a fixed average corresponds to the computation of the capacity of a channel with an input alphabet of up to 16'000 letters. Of those 16'000 letters, only about 100 letters have non-zero probabilities in the capacity-achieving distribution. Therefore, the algorithm presented here allowed a considerable acceleration of the convergence when compared to a conventional implementation of the Arimoto-Blahut algorithm. A detailed presentation of this application along with more information on the implementation of the algorithm are given in [5].

References

[1] Suguru Arimoto, "An Algorithm for Computing the Capacity of Arbitrary Discrete Memoryless Channels," *IEEE Trans. on Inform. Theory*, **IT-18**, pp. 14-20, January 1972.

[2] Richard E. Blahut, "Computation of Channel Capacity and Rate-Distortion Functions," *IEEE Trans. on Inform. Theory*, **IT-18**, pp. 460-473, July 1972.

[3] Robert G. Gallager (1968), *Information Theory and Reliable Communications*, John Wiley and Sons, New York, ISBN 0-471-29048-3.

[4] Robert G. Gallager, "Source Coding with Side Information and Universal Coding," **unpublished,** submitted to the *IEEE Trans. on Information Theory*, September 1976.

[5] Jossy Sayir (1999), *On Coding by Probability Transformation*, ETH Zürich, PhD Dissert. Nr. 13099, Hartung-Gorre Verlag Konstanz, Germany, ISBN 3-89649-444-9.

[1]This paper documents work performed at the Signal & Inf. Proc. Lab., ETH Zürich, Switzerland.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

To Code Or Not To Code

Michael Gastpar, Bixio Rimoldi and Martin Vetterli[1]
Department of Communication Systems
Swiss Federal Institute of Technology
CH-1015 Lausanne, Switzerland
e-mail: {gastpar, rimoldi, vetterli}@lcavsun1.epfl.ch

Abstract — **The theory and practice of digital communication during the past 50 years has been strongly influenced by Shannon's separation theorem [1]. While it is conceptually and practically appealing to separate source from channel coding, either step requires infinite delay in general for optimal performance. On the other extreme is uncoded transmission, which has no delay but is suboptimal in general. In this paper, necessary and sufficient conditions for the optimality of uncoded transmission are shown. These conditions allow the construction of arbitrary examples of optimal uncoded transmission (beyond the well-known Gaussian example).**

I. Previous and Basic Results

We consider a discrete-time memoryless source represented by the random variable $S \in \mathcal{S}$. The source output S is applied directly to a memoryless channel.[2] The channel output $Y \in \mathcal{Y}$ is our estimate of the source with respect to a distortion measure $d(s,y)$. The source is specified by a probability density (or mass) function $p(s)$ and a distortion measure $d(s,y)$. The channel is specified by a conditional probability density (or mass) function $W(y|s)$ and a channel input cost function $\rho(s)$. Therefore, uncoded transmission achieves (average) distortion $\Delta = Ed(S,Y)$ and (average) input cost $\Gamma = E\rho(S)$.

Definition. Uncoded transmission of the source (p,d) across the channel (W,ρ) is optimal if: *(i)* Δ is the minimum distortion achievable when the maximum input cost is Γ; and *(ii)* Γ is the minimum input cost to achieve distortion at most Δ.

Let $R(D)$ be the rate-distortion function of the source, and $D(R)$ the distortion-rate function. Correspondingly, let $C(P)$ be the capacity-cost function of the channel, and $P(C)$ the cost-capacity function. From the separation theorem, we have the following *Fact:* Uncoded transmission of the source (p,d) across the channel (W,ρ) is optimal if and only if *(i)* $\Delta = D(C(\Gamma))$, and *(ii)* $\Gamma = P(R(\Delta))$.

These two conditions are cumbersome to work with. For most cases of interest, we can find simpler necessary and sufficient conditions. However, let us first exclude certain special cases. Let C_0 denote the capacity of the unconstrained channel (W,ρ), i.e. $C_0 = C(P \to \infty)$.

Condition A. The source (p,d) and the channel (W,ρ) satisfy condition A if *(i)* in case $I(p,W) = 0$, W is the unique achiever of zero mutual information, and *(ii)* in case $I(p,W) = C_0$, p is the unique achiever of C_0.

The condition ensures that $D(R(\cdot))$ and $P(C(\cdot))$ are the identity functions, respectively.

Lemma 1. Granted condition A, uncoded transmission of the source (p,d) across the channel (W,ρ) is optimal if and only if $R(\Delta) = C(\Gamma)$.

This Lemma follows essentially from [2]; however, Condition A was not mentioned there. On a more intuitive level, Lemma 1 implies the following:

Lemma 2. Granted condition A, uncoded transmission of the source (p,d) across the channel (W,ρ) is optimal if and only if *(i)* the source p achieves capacity on the channel (W,ρ) (at input cost Γ), and *(ii)* the channel W achieves the rate-distortion function of the source (p,d) (at distortion Δ).

Unfortunately, in order to compute rate-distortion and capacity-cost functions, we have to resort to numerical methods in general. Thus, neither Lemma 1 nor Lemma 2 give an explicit way to verify whether or not for a given source and channel uncoded transmission is optimal and to construct examples of such source/channel pairs.

II. Main Result

Proposition. Uncoded transmission of the source (p,d) across the channel (W,ρ) for which $0 < I(p,W) < C_0$ is optimal if and only if

$$\begin{aligned} \rho(s) &= c_1 D(W(\cdot|s)||p_Y) + \rho_0 \\ d(s,y) &= -c_2 \log_2 \frac{W(y|s)}{p_Y(y)} + d_0(s), \end{aligned}$$

for some constants $c_1 > 0$, $c_2 > 0$, ρ_0 and an arbitrary function $d_0(s)$, where $D(\cdot||\cdot)$ is the Kullback-Leibler distance and $p_Y(y) = EW(y|S)$ is the pdf of Y.

A proof of this proposition can be found in [3]. A similar result can be obtained for the case $I(p,W) = C_0$. Note that the proposition allows to construct essentially all occurrences of optimal uncoded transmission.

Universality of uncoded transmission. The most interesting applications of uncoded transmission are cases where the separation theorem does not hold, e.g. non-ergodic channels or multi-user communication. Consider a broadcast scenario with one source and many (different) channels. If it turns out that the above proposition is satisfied for the source and each channel individually, then uncoded (broadcast) transmission is (globally) optimal. In this example, uncoded transmission exhibits a property of universality, whereas the performance of any separation-based coding scheme is strictly suboptimal.

References

[1] C. E. Shannon, "A mathematical theory of communication," *Bell Sys. Tech. Journal*, vol. 27, 1948, pp. 379-423 and 623-656.

[2] S. Shamai (Shitz), S. Verdú and R. Zamir, "Systematic Lossy Source/Channel Coding," *IEEE Trans. Info. Theory*, vol. 44, no. 2, March 1998, pp. 564-579.

[3] M. Gastpar, B. Rimoldi and M. Vetterli, "On the optimality of uncoded transmission," Technical Report, EPFL-DSC, Lausanne, 2000.

[1] M. Vetterli is also with the Dept. of EECS, UC Berkeley, USA.

[2] For the framework of this paper, we assume that the channel input alphabet is also $\mathcal{S}$. The extension to arbitrary memoryless encoders and decoders will be presented at a later stage.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Source-Channel Coding Strategies: Tandem Coding vs. Channel-Optimized Quantization

Jongtae Lim and David L. Neuhoff[1]
EECS Department, University of Michigan
Ann Arbor, MI 48109

Abstract — **Two source-channel coding strategies, tandem coding and channel-optimized quantization, are compared on the basis of distortion vs. complexity. For each, formulas for the mean-squared error and complexity used to minimize distortion subject to a complexity constraint. The results suggest there is a threshold such that tandem coding is better than channel-optimized quantization when and only when the complexity constraint is larger than the threshold.**

I. Introduction and System Description

An oft claimed motivation for joint source-channel coding (JSCC) is the potential to obtain good performance with less delay or complexity than with the conventional tandem source-channel coding (TSCC). However, little quantitative support for this claim has appeared in the literature. In this work, we seek to determine the validity of the claim by quantitatively comparing representative systems of each type on the basis of distortion vs. complexity. (Delay is not considered.)

To avoid idiosyncrasies, the source, channel and representative systems are chosen to be as plain vanilla as possible. Specifically, the source is Gauss-Markov; the channel is binary symmetric (BSC); the distortion measure is mean-squared error (MSE); the TSCC, as in [1], is a conventional transform (source) code in tandem with a Reed-Solomon (R-S) channel code, and the JSCC is a channel-optimized transform code (COTC), which is a kind of channel-optimized quantizer. In both cases, a KLT transform is used, and the transform coefficients are encoded with fixed-rate scalar quantizers. (Entropy coding is not used because of its idiosyncratic sensitivity to channel errors.) For COTC, the quantizers and bit allocations are optimized for the BSC as in [2]. For TSCC, the quantizers are optimized for a noiseless channel, with conventional bit allocations, and the (n, k, m) R-S encoder is systematic. When the BSC output is within the error correcting capability, t, of some R-S codeword, the R-S decoder produces the first k symbols of that codeword. Otherwise, the received decoder is said to FAIL, and it simply produces the first k channel output symbols.

II. Distortion, Complexity and Optimization

The MSE of the COTC may be computed as in [2]. That of the TSCC can be computed in the form

$$E[D] = E[D|\text{no fail}]\,\Pr(\text{no fail}) + E[D|\text{fail}]\,\Pr(\text{fail}).$$

When $t \geq 4$, the probability of decoding error given no failure is negligible. Thus, $E[D|\text{no fail}]$ is the usual distortion of the transform code on a noiseless channel. The computation of $\Pr(\text{fail})$ is elementary, and a detailed method for computing $E[D|\text{fail}]$ has been developed.

As a measure of complexity C, we sum estimates of the numbers of arithmetic operations per data sample used in encoding and decoding. For COTC, $C = 4L - 2 + R$, where $L =$ transform dimension and $R =$ number of BSC uses per data sample. For the tandem code, $C = 4L - 2 + Rk/n + (\alpha k + \beta n)(n-k)R/nm$, where $\alpha = 2$ and $\beta = 10$.

Using the above methods for computing the MSE and complexity, an optimization program searched for the best parameters for systems of each type, subject to a complexity constraint. The Gauss-Markov correlation coefficient is fixed at 0.9. The BSC error probability p and the number of BSC uses per data sample R are also fixed at various values. The TSSC parameters are L, n, m, k; the only COTC parameter is L.

III. Results and Conclusions

A representative result of the optimizations is provided by Figure 1. For small values of complexity, channel-optimized transform coding is better. However, as complexity increases, its performance tends to saturate and tandem coding becomes better. In other words, there appears to be a threshold such that tandem coding is better than channel-optimized transform coding when and only when the available complexity is above this threshold. Other results, not shown, indicate that the complexity threshold decreases as the BSC error probability decreases.

References

[1] J. Lim, D. L. Neuhoff and T.C. Nolan, "Allocating complexity between source and channel coding," Workshop on Data Compr. Proc.Techn. for Miss. Guid. Data Links, pp. 669-679, Dec. 1998.

[2] V.A. Vaishampayan and N. Farvardin, "Optimal block cosine transform image coding for noisy channels," IEEE Trans. Commun., vol. 38, pp. 327-336, Mar. 1990.

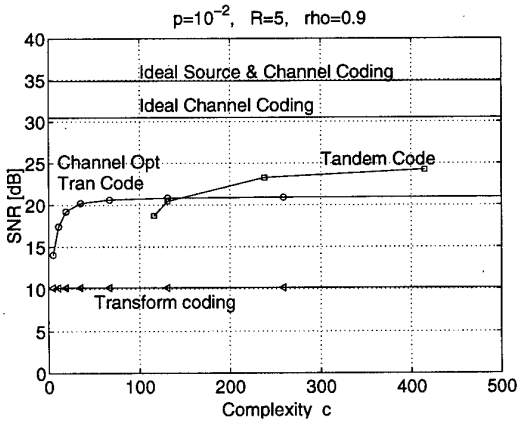


Fig. 1: Performance (SSNR) vs. complexity (op's/sample).

[1]Work supported by ARO MURI grant DAAH04-96-1-0337.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Iterative Source/Channel Decoding based on a Trellis Representation for Variable Length Codes

Rainer Bauer and Joachim Hagenauer
Institute for Communications Engineering (LNT)
Munich University of Technology (TUM)
Arcisstrasse 21
D-80290 Muenchen, Germany
e-mail: {Rainer.Bauer,Joachim.Hagenauer}@ei.tum.de

Abstract — **A new trellis representation for variable length codes (VLC) is proposed which allows soft-in/soft-out decoding of these codes. Applying the BCJR-algorithm on this trellis either symbol-level or bit-level reliability information for the variable length coded sequence can be obtained. By using this soft-in/soft-out VLC decoder for iterative ("turbo") decoding of a serially concatenated scheme consisting of an outer variable length code and an inner convolutional code separated by an interleaver significant gains can be yielded compared to a instantaneously decoded variable length code of the same overall source and channel code rate.**

I. Introduction

Recently several schemes have been proposed to perform decoding of variable length codes by considering the overall sequence rather than decoding the VLC coded symbol stream instantaneously using the prefix property of these codes. Some of these approaches also use trellis representations of variable length encoded symbol sequences and carry out either maximum likelihood (ML)- or maximum a posteriori (MAP)-sequence estimation to decode the source symbols. Although in [2] symbol-level soft-output was proposed, the soft-output was not used for further processing. We present a soft-in/soft-out VLC decoder which can be used in an iterative decoding scheme.

II. Trellis Representation

Consider a source that independently produces outputs selected from an M-ary alphabet $\mathcal{U} = \{0, ..., M-1\}$. A vector $\mathbf{u}$ of K source output values is mapped to a vector $\mathbf{c}$ of codewords taken from a variable length code C for the given symbol alphabet. Let $\mathbf{l} = (l_1, ..., l_M)$ be an M-tuple that defines the lengths of the codewords. The total bit-length of the VLC vector $\mathbf{c}$ is denoted by N. Every sequence consisting of K symbols and N bits can be graphically represented by a trellis-like structure as shown in Figure 1 for $K = 4$ and $N = 6$, where the horizontal axis represents the symbol time and the vertical axis represents the bit time. The alphabet size in the example is $M = 3$ and the lengths of the codewords are $\mathbf{l} = (1, 2, 3)$. Furthermore, let the vector $\mathbf{c}$ be channel coded and transmitted over a noisy channel.

III. Decoder Structure

As the above mentioned trellis is terminated it can easily be seen that maximum a posteriori (MAP) decoding according to the BCJR-algorithm [1] can be applied on this trellis. Thereby decoding can be carried out either on a symbol-by-symbol basis along the horizontal axis or on a bit-by-bit basis along the vertical axis. If decoding is done vertically the output values of the decoder are a posteriori probabilities (APP) for the bits of the variable length coded sequence $\mathbf{c}$. Let us assume a concatenated coding scheme with a variable length code as outer code and a channel code as inner code separated by an interleaver. If the APP-VLC decoder works in the bit-level mode the soft-output can be used as a priori information for a second run of the inner soft-in/soft-out channel decoder. This results in the well known structure of an iterative decoder for a serially concatenated coding scheme.

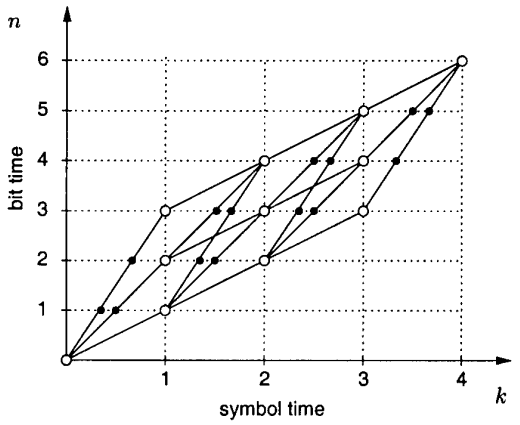


Figure 1: Example for VLC-Trellis

This new iterative approach in source/channel decoding with variable length codes results in significant performance gains compared to a system with instantaneous VLC decoding for both AWGN and fully interleaved Rayleigh-fading channel. Further detail about the proposed approach can also be found in [3].

References

[1] L. R. Bahl, J. Cocke, F. Jelinek, J. Raviv, "Optimal decoding of linear codes for minimal symbol error rate," *IEEE Trans. on Inform. Theory*, vol. IT-20, pp. 284-287, March 1974

[2] M. Park and D. J. Miller, "Decoding entropy-coded symbols over noisy channels using discrete HMMs, in *Proc. Conf. on Information Sciences and Systems (CISS)*, Princeton, USA, March 1998

[3] R. Bauer and J. Hagenauer, "'Turbo-FEC/VLC-Decoding' and its Application to Text Compression", in *Proc. CISS 2000*, Princeton, NJ, March 2000

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Progressive Image Transmission over Compound Packet Erasure Channels

Vinay Chande and Nariman Farvardin [1]
Department of Electrical and Computer Engineering,
University of Maryland
College Park, MD-20742 ,USA
e-mail: {chande,farvar}@eng.umd.edu

Abstract — **We consider the problem of joint source-channel coding for progressive packetized transmission of an image over a packet-loss network whose packet-loss rate is a random variable. We obtain an algorithm for unequal erasure protection which, by design, maintains progressivity, that is, good performance at intermediate transmission budgets.**

Embedded source coders for images are attractive because they provide a single bitstream capable of progressively reproducing the image at different distortions and rates (bit budgets). Maintaining such a progressive capability, when the communication channel is noisy or lossy, requires design of a joint source-channel coding scheme which generates a single bitstream, simultaneously taking into account the distortion-rate performance at a number of transmission budgets. In this work, we undertake the design of a system for progressive image transmission over a lossy packet network with unknown packet-loss characteristics in the absence of any network/transport layer loss recovery mechanism and feedback channel (*e.g.* transmission using User Datagram Protocol (UDP). We assume the packet length to be fixed. We model a network with unknown packet-loss rate as a compound channel. A compound packet erasure channel is a finite-state channel whose packet-loss rate for a session is a random variable with known probability distribution. In each state $s \in \mathcal{S}$, the *channel is memoryless* with an associated packet erasure rate $e(s)$. The state is chosen at the beginning of the transmission session according to a known probability mass function f^s, and *remains unchanged* during the entire session. This model applies to situations such as 1) transmission of the same bitstream to different receivers facing different packet-loss rates, 2) transmission over a time varying channel, where the time-scale of variations in packet-loss rates is much larger than the average length of an image transmission session (*e.g.* over the Internet where the packet-loss rates due to congestions have hourly and daily variations.)

We select a high performance embedded image coder like SPIHT as the source coder. The joint source-channel coder design requires the allocation of unequal erasure protection to (i) incorporate varying sensitivity of source-bits to loss, and (ii) combat the channel variability. In addition, the design requires the *scheduling* of the source and the protection bits in the transmit bitstream to obtain good progressive transmission. We use a rate compatible family $C = \{c_1, c_2, \ldots c_J\}$ of (n, k_0) packet erasure correcting (PEC) codes obtained by puncturing a Reed-Solomon (RS) parent code for different n and fixed k_0. A (n, k_0) PEC code corrects $n - k_0$ packet erasures. The embedded source coder output is divided into fixed length source-blocks of length k_0 packets. Each source-block is encoded with a potentially different channel code, chosen from C according to a *code allocation policy*. The joint source-channel coder generates a single stream of packets and transmits over the lossy network. Some of these packets are lost or dropped by the network. We assume that the location of dropped packets is known. At the receiver, RS codewords are reassembled and source-blocks are recovered. The image is reconstructed only from the longest available (recovered) prefix of the source-block sequence. A code allocation policy π given by a sequence $\{c_\pi^1, c_\pi^2, \ldots, c_\pi^{N(\pi)}\}$ allocates channel code $c_\pi^i \in C$ to the i^{th} source-block out of the source coder. Let $M_T(\pi)$ denote the total number of packets used by policy π. Let, for $c \in C$, $r_c(c)$ denote the coderate. Then $M_T(\pi)$ is computed as, $M_T(\pi) \stackrel{def}{=} \sum_{i=1}^{N(\pi)} k_0 r_c^{-1}(c_\pi^i)$. Let $\overline{PSNR}_\pi$ denote the expected Peak-Signal-to-Noise-Ratio (PSNR) at the receiver while following the policy π over the compound channel. The code allocation problem under the constraint of total transmission budget of M packets is written as,

$$\max_\pi \overline{PSNR}_\pi \text{ subject to } M_T(\pi) \leq M. \qquad (1)$$

Unlike a fading channel, for a compound channel and a policy π, $\overline{PSNR}_\pi$ does not depend on the order of the packets in the bitstream. But the expected PSNR at intermediate budgets is controlled by the order of the packets. The proposed algorithm addresses the simultaneous ordering and code allocation problem. The output bitstream is regarded as a sequence of *embedded* policies, each designed for an intermediate transmission budget [1]. Let $\pi^*(M)$ denote the policy obtained by the proposed algorithm for problem (1) for packet budget M. The algorithm generates $\pi^*(M)$ from policies $\pi^*(j)$ for $1 \leq j < M$, in such a way that the resulting policies are embedded by design. Briefly, the algorithm restricts the search of $\pi^*(M)$ to a union of (i) all policies obtained by adding one parity-check packet to a source-block in policy $\pi^*(M-1)$ and, (ii) all policies of packet-constraint M, obtained by adding an entire source-block encoded with some code $c \in C$ to one of the policies $\pi^*(j)$ for $j < M$. Then, from the (restricted) search space, it selects the policy $\pi^*(M)$ which maximizes the average PSNR. The algorithm is greedy and suboptimal, but for each budget M, it generates a single packet stream which executes $\pi^*(M)$ as well as $\pi^*(j)$ for a number of intermediate budgets $j, 1 \leq j < M$. Simulations for selected channels and images yield over 0.5 dB improvement in average PSNR over equal erasure protection (EEP) schemes across a range of transmission rates. The gains are higher and the designed allocation is farther away from an EEP scheme if the variation in the packet-loss rates is higher.

[1]Prepared through collaborative participation in the Advanced Telecommunications/Information Distribution Research Program (ATIRP) Consortium sponsored by the U.S. Army Research Laboratory under Cooperative Agreement DAAL01-96-2-0002 and supported in part by a grant from the National Security Agency.

References

[1] V. Chande and N. Farvardin, "Joint source-channel coding for progressive transmission of embedded source-coders," in *Proc. Data Compression Conference (DCC)*, (Snowbird, Utah), pp. 52–61, March 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

The Simple Ideal Cipher System

Boris Ryabko[1]
Siberian State University of Telecommunications and Information Sciences
Kirov St. 86, Novosibirsk 630102 Russia
e-mail: ryabko@neic.nsk.su

Abstract — **An ideal cipher system is suggested whose coding time is less in order of magnitude than for known methods.**

I. Introduction

It is well known in cryptography that it is easy to construct an unbreakable secret-key cipher system if a plaintext source generates letters which are independent and equiprobable even if the length of a key sequence is much less than the length of the message [1]. In this paper, we suggest a new secret-key cipher system in which a message generated is transformed into two parts in such a way that the biggest part consists of independent and equiprobable bits and only this part is encrypted. The complexity of the method is exponentially less than that for other known methods.

We use a common definition of a secret-key cipher system. As customary, we assume that the secret key $\bar{k}$ is statistically independent of the plaintex sequence $x_1x_2\ldots$. We also assume that the plaintext digits, key digits, and ciphertext digits take values in the alphabet $A = \{0,1\}$, the key source and the plaintext source are i.i.d., and key digits are equiprobable, but the suggested method is easily generalized for the case of any finite source alphabet and for Markov sources.

In this report a simply realisable ideal system is suggested for the case when the length of a key is much less than the length of an encrypted message.

II. Description of the Cipher System

The description of the suggested cipher system may be divided into two parts as follows: first, a generated sequence of letters is transformed into two subsequences, and, second, the biggest subsequence which consists of independent and equiprobable letters, is encrypted. The first part plays a key role. It is based on the method of P. Elias [2] and the fast algorithm of enumeration from [3].

Let us give some new definitions in order to describe the method. Let S_n^i be the set of all binary words of the length n with i ones, $(n \geq i \geq 0)$, and let for every $x \in S_n^i$ $code(x)$ be lexicographical number of the word x in the set S_n^i which is written in binary number system, the length of $code(x)$ equals $\lceil \log \binom{n}{i} \rceil$ bits.

A generated plaintext can be written in the form of a sequence of blocks of the length n, where $n \geq 2$ is a parameter of the method. Every block $\bar{x}$ is encoded by the sequence of three words $u(\bar{x})v(\bar{x})w(\bar{x})$. Here $u(\bar{x})$ is the number of units in the block $\bar{x}$ and the length of $u(\bar{x})$ is equal to $\lceil \log(n+1) \rceil$ bits. In order to describe $v(\bar{x})$ and $w(\bar{x})$ we define $m_k = \lfloor \log \binom{n}{k} \rfloor \left(= \lfloor \log |S_n^k| \rfloor\right)$ and let $\alpha_{m_k}\alpha_{m_k-1}\ldots\alpha_0$ be a binary notation of $|S_n^k|$. Let $\alpha_{m_k} = 1, \alpha_{j_1} = 1, \ldots, \alpha_{j_s} = 1$ and the other $\alpha_{j_k} = 0$ and let $j_1 > j_2 > \ldots > j_s$. Let $\beta(\bar{x}) = \beta_{m_k}\beta_{m_k-1}\ldots\beta_0$ be the binary notation of the lexicographical number of $\bar{x}$ and let the following inequalities be valid:

$$\begin{aligned} \alpha_{m_k}\alpha_{m_k-1}\ldots\alpha_{j_r}000\ldots0 &\leq \beta(\bar{x}) \\ &< \alpha_{m_k}\alpha_{m_k-1}\ldots\alpha_{j_{r+1}}00\ldots0 \end{aligned} \quad (1)$$

for a certain r. (Obviously such r exists). The word $w(\bar{x})$ is defined as follows

$$w(\bar{x}) = \begin{cases} \beta_{j_r-1}\beta_{j_r-2}\ldots\beta_0, & \text{if } j_r - 1 \geq 0 \\ \Lambda, & \text{if } j_r - 1 < 0, \end{cases} \quad (2)$$

where Λ is an empty word and $j_0 = m_k$ by definition. At last, $v(\bar{x})$ is a binary notation of the length of the word $w(\bar{x})$ and the length of $v(\bar{x})$ is equal to $\lceil \log(m_k+1) \rceil$ bits by definition.

Let us describe the second part of the method. It is convenient to enumerate digits of words $w(x_1\ldots x_n)$, $w(x_{n+1}\ldots x_{2n})$, ... and denote them by $w_0w_1\ldots$. Let $k = k_0k_1\ldots k_{t-1}$ is the key word. The enciphering and deciphering are defined by formulas $z_i = w_i \oplus k_{i \bmod t}$ and $w_i = z_i \oplus k_{i \bmod t}$, correspondingly. Every symbol z_i is put on the place of the letter w_i. So an encrypted sequence may be considered as the sequence $u(\cdot)v(\cdot)z(\cdot)u(\cdot)v(\cdot)z(\cdot)\ldots$, where $z(\cdot)$ is the encrypted word $w(\cdot)$.

Theorem: Let there be given a Bernoulli source which generates letters from the alphabet $A = \{0,1\}$ with (unknown) probabilities p and q, respectively. Let the suggested cipher system be used for encrypting the source messages with the blocklength n. Then the following holds:

i)the suggested system is strongly ideal

ii) The symbols of the sequence $w(x|_1^n)\ w(x|_{n+1}^{2n})\ w(x|_{2n+1}^{3n})$ ... are independent and equiprobable.

iii) $E\left(\left|w(x|_{rn+1}^{(r+1)n})\right|\right) > nh - 2\log(n+1)$, where $h = -(p\log p + q\log q)$ is the entropy of the source, $E(\cdot)$ is an expectation.

iv) the method requires the memory size $O(n\log n)$ bits and has the time of encoding and decoding $O(\log^3 n \log\log n)$ bit operations per letter as $n \to \infty$.

Remark. The source generates h bits of information per letter and, therefore, nh bits per block. The suggested cipher system encrypts symbols of the words $w\left(x|_{rn+1}^{(r+1)n}\right)$, $r = 0,1,2,\ldots$. The claim iii) shows that, informally, almost all generated information is encrypted when n grows.

References

[1] C. Shannon, "Communication theory of secrecy systems," *Bell System. Techn. J.*, vol. 28, no. 4, pp. 656–715, 1949.

[2] P. Elias, "The efficient construction of an unbiased random sequence," *The Annals Math. Statist.*, vol. 43, no. 3, pp. 864–870, 1972.

[3] B. Ryabko and E. Machikina, "The fast and efficient construction of an unbiased random sequence," in *Proc. 1988 IEEE Int. Symp. Inform. Theory*, Cambridge, MA USA, 1998, p. 472.

[1]This work was supported by RFBR Grant 99-01-00586.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Better than "Optimum" Homophonic Substitution

Valdemar C. da Rocha Jr.[1]
lbr@hotlink.com.br, CP 7800,
Comms.Res.Group - UFPE,
50711-970 Recife PE, BRAZIL

James L. Massey
JamesMassey@compuserve.com
Dept. Inform. Theory, Lund Univ.
SE-221 00 Lund, SWEDEN

Abstract — **A perfect homophonic coding technique is devised for which the number of fair coin tosses to select a homophone is bounded for any source with rational letter probabilities. The new scheme enlarges the source alphabet, which paradoxically generally results in less plaintext expansion than does "optimum" homophonic coding of the unaugmented source.**

I. Introduction

In *homophonic coding*, a multiplicity of "homophones" (binary words hereafter) are probabilistically substituted for each plaintext letter so as to reduce the redundancy of the resulting new "plaintext" and hence to increase the unicity distance of the cipher at the cost of some plaintext expansion. Homophonic coding is *perfect* if the new plaintext sequence is irredundant and is *optimum* if it is perfect and its *plaintext expansion* (i.e., the average length of a homophonic word less the entropy of a source letter) is as small as possible [1].

For simplicity, we consider only binary homophonic coding of the output sequence of a K-ary discrete *memoryless* source (DMS). The homophonic coding problem then reduces to that for a single K-ary random variable U, but the theory is easily modified to handle general sources. We assume that U has a probability distribution with rational entries $P_U(u_i) = m_i/n$, $1 \le i \le K$, where m_i and n are positive integers and n is as small as possible. If and only if n is an integer power of 2, the number of fair coin tosses to select a homophone is bounded for perfect homophonic coding of the DMS U [1]. We show now how to achieve this for all n.

II. The New Scheme

The "trick" is to augment the source U with a "dummy" letter Δ to which we assign probability $P_{\tilde{U}}(\Delta) = (2^N - n)/2^N$ where $N = \lceil \log_2 n \rceil$. This forces the choices $P_{\tilde{U}}(u_i) = (n/2^N)P_U(u_i) = m_i/2^N$ for $1 \le i \le K$. The letter probabilities for the augmented source are thus rational numbers with a common denominator of 2^N and hence at most N fair coin flips are required to choose the homophone if optimum standard homophonic coding [1] is now applied. Surprisingly, the resulting plaintext expansion is generally less than for standard "optimum" homophonic coding of the original source.

Example: Consider the binary DMS with $P_U(u_1) = 1/3$ and $P_U(u_2) = 2/3$. "Optimum" homophonic coding uses an unbounded number of fair coin tosses for homophone selection and gives an average word length $E[W] = 2$. The plaintext expansion is $E[W] - H(U) = 2 - h(1/3) \approx 1.082$, where $h(p)$ is the binary entropy function. $N = \lceil \log_2 3 \rceil = 2$, so we augment U with a dummy letter Δ with $P_{\tilde{U}}(\Delta) = (4-3)/4 = 1/4$. Then $P_{\tilde{U}}(u_1) = (3/4)(1/3) = 1/4$ and $P_{\tilde{U}}(u_2) = (3/4)(2/3) = 1/2$ so at most two fair coin flips are needed to select a homophone. All letter probabilities for $\tilde{U}$ are negative integer powers of 2 and hence $E[\tilde{W}] = H(\tilde{U})$. The average number of letters from the original source U that are encoded with the encoding of one letter of $\tilde{U}$ is $p = n/2^N = 3/4$. The plaintext expansion of the new scheme is thus $E[\tilde{W}] - pH(U) = H(\tilde{U}) - pH(U) = 3/2 - (3/4)h(1/3) \approx 0.811$, which is substantially less than the plaintext expansion 1.082 for standard "optimum" homophonic coding of the original source U!

The new scheme can be implemented as follows. One first tests for the occurrence of an event of probability $p = 1 - P_{\tilde{U}}(\Delta) = n/2^N$, which requires at most N flips of a fair coin. If the event occurs, one calls on the source U to emit a letter that then becomes the output of $\tilde{U}$. Otherwise, the dummy letter Δ becomes the output of $\tilde{U}$. Decoding is simple–one just deletes the dummy letters from the reconstructed output sequence of $\tilde{U}$ to obtain the output sequence of U.

III. Bounds on Plaintext Expansion

Proposition 1 *Let U be a K-ary discrete memoryless source whose letter probabilities are all rational numbers, and let n, N and p be as defined above. Then standard optimum homophonic coding [1] of the augmented source $\tilde{U}$ achieves a plaintext expansion $E[\tilde{W}] - pH(U)$ satisfying the bounds*

$$h(p) \le E[\tilde{W}] - pH(U) < h(p) + 2 - 2^{3-N}, \text{ all } N \ge 3, p \ne 1 \quad (1)$$

and, if a) the letter probabilities of U written as fractions with denominator n all have numerators that are integer powers of 2 and b) $n = 2^N - 2^i$ for some i, $0 \le i \le N-2$, satisfying

$$E[\tilde{W}] - pH(U) = h(p). \quad (2)$$

The lower bound in (1) follows immediately from the fact that $E[\tilde{W}] \ge H(\tilde{U}) = h(p) + pH(U)$. The upper bound for $N \ge 3$ follows from the bound in [2] upon noting that when $p \ne 1$ there can be at most $N-1$ terms in the expression for the probability of any letter of $\tilde{U}$ as a sum of distinct negative integer powers of 2.

The equality in (2) follows by noting that conditions a) and b) are necessary and sufficient for the probabilities of all letters of $\tilde{U}$ to be negative integer powers of 2 or, equivalently, to have $E[\tilde{W}] = H(\tilde{U}) = h(p) + pH(U)$. Note that conditions a) and b) are always satisfied when $N = 2$ and $p \ne 1$.

Example: Consider the DMS U with letter probabilities 2/3, 1/6 and 1/6. Here $n = 6$ and $N = 3$. Conditions a) and b) are satisfied so (2) holds and the plaintext expansion is $E[\tilde{W}] - pH(U) = h(p) = h(3/4) \approx 0.811$.

References

[1] H. N. Jendal, Y. J. B. Kuhn and J. L. Massey, "An Information-Theoretic Approach to Homophonic Substitution", pp. 382-394 in *Advances in Cryptology-Eurocrypt'89* (Eds. J.-J. Quisquater and J. Vandewalle), LNCS No. 434. Springer, 1990.

[2] V. C. da Rocha Jr. and J. L. Massey, "On the Entropy Bound for Optimum Homophonic Substitution", *Proc. IEEE Int. Symp. on Inform. Th.*, Ulm, Germany, 29 June - 4 July, 1997, p.93.

[1]This author thanks André Kauffman for helpful discussions and the Brazilian National Council for Scientific and Technological Development (CNPq) for its support under Grant No. 304214/77-9.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Collusion-Secure Fingerprinting and B_2-Sequences

Gérard Cohen[1]
École Nationale Supérieure
des Télécommunications
46 rue Barrault,
75634 Paris 13 France
e-mail: cohen@infres.enst.fr

Simon Litsyn
Tel-Aviv University
Dept. of Electrical
Engineering-Systems,
69978 Ramat Aviv, Israel.
e-mail: litsyn@eng.tau.ac.il

Gilles Zémor
École Nationale Supérieure
des Télécommunications
46 rue Barrault,
75634 Paris 13 France
e-mail: zemor@infres.enst.fr

Abstract — **We discuss a strategy initiated by Boneh and Shaw for Collusion-Secure Fingerprinting. We show that under this strategy, finding fingerprinting schemes that resist coalitions of two users amounts to finding B_2-sequences of binary vectors. A sequence of vectors $v_1, v_2, \ldots, v_n$ is a B_2-sequence if all sums $v_i + v_j$, $1 \leq i \leq j \leq n$, are different : the associated extremal set-theoretic problem is what is the maximal size of a B_2-sequence ? We shed new light on this old combinatorial problem and improve on previously known upper bounds.**

I. Marking Assumptions and duplication

Suppose a *Distributor* wishes to create and distribute a large number of copies of a large binary file $\Phi \in \mathbf{F}_2^N$. In order to trace illegal copies he will *mark* each copy of Φ. The marking process of some copy of Φ consists of changing the bits of Φ belonging to some subset of a privileged set $M \subset \{1, \ldots N\}$ of coordinates called *marks*. The subset of marks associated to a copy of Φ is called a *fingerprint* and can be seen as a binary vector of length $m = |M|$. The set of marks M is unknown to anyone but the distributor. It is supposed to be a small subset of $\{1, \ldots N\}$, so that modifying a fingerprint by randomly changing a few bits of a copy of Φ is inefficient.

The problem of *collusion* occurs when a coalition of c pirate users compare their fingerprinted copies : whenever their set of copies differ on some coordinate they will know it is a mark. They can then produce an illegal copy by changing at will bits on the subset of marks they have found out.

We shall concern ourselves with the case $c = 2$.

Boneh and Shaw use the following *duplication* trick: the set of fingerprints is actually constructed from a *code* $\mathcal{C} \subset \mathbf{F}_2^n$ where $m = tn$. A fingerprint X is constructed from a codeword $x \in \mathcal{C}$ simply by duplicating each symbol t times, i.e. changing 0 to $00\cdots0$ and 1 to $11\cdots1$. Let us call the set of t coordinate positions of X that stem from a single coordinate of x a *block*. The partition of the set M of marks into blocks is kept secret by the distributor. Thus, when two pirate users compare their fingerprinted copies they will have no way of deciding whether two uncovered marks belong to the same block or not, so whenever the pirates decide to change a fraction p of the set of uncovered marks, they will, on average, change a fraction p of the marks belonging to any single block.

Suppose two colluding pirates are in possession of two legal copies fingerprinted by X and Y and that X and Y originate from $x, y \in \mathcal{C}$. The pirates have essentially the following type of strategy : they can pick one of the copies, fingerprinted by X say, and change randomly and independently with probability p every coordinate of the set of uncovered marks. Their only degree of freedom is p.

On the other hand, when confronted with this illegal copy of Φ the distributor will try to trace one of the legal copies it was constructed from, i.e. reconstruct x or y. The distributor has two strategies:

1. He can associate to every block a binary symbol by majority decision.
2. The alternative strategy is to associate to any corrupted block which contains both zeros and ones a third *erased* symbol, say ε. This strategy yields a ternary vector $\zeta \in \{0, 1, \varepsilon\}^n$.

What duplication ensures is that the second strategy need be applied only when the first has failed to produce a legitimate codeword $z \in \mathcal{C}$. With high probability this will happen only when the pirates have chosen p sufficiently separated from 0 and 1. In that case the second strategy will yield with high probability the ternary vector

$$\zeta = \zeta(x, y)$$

defined by $\zeta_i = x_i = y_i$ when $x_i = y_i$ and by $\zeta_i = \varepsilon$ when $x_i \neq y_i$.

If the code $\mathcal{C}$ has the property that $\zeta(x, y)$ always identifies $\{x, y\}$ for any pair of codewords $\{x, y\}$, then, for any sufficiently big duplication parameter t, one of the two decoding strategies will almost always identify x or y.

II. B_2-sequences

Let x and y be two codewords of a code $\mathcal{C} \subset \mathbf{F}_2^n$. Notice that $\zeta(x, y)$ is obtained from the real sum $x + y$ by changing every 2 coordinate into a 1, every 1 coordinate into ε and leaving 0's unchanged. The relevant identifying property that we need from $\mathcal{C}$ is that the real sums $x + y$ are all different for every pair $\{x, y\}$ of codewords. Such a code has been named a B_2-sequence by Lindström [2].

Define by $R = \limsup_{n\to\infty} \frac{1}{n} \log_2 |\mathcal{C}_n|$ the maximum rate of a B_2 -sequence. The previously known best bounds were [2]:

$$0.5 \leq R \leq 0.6 \qquad (1)$$

Using results from [3] we obtain:

Theorem 1

$$R \leq 0.5752....$$

References

[1] D. Boneh and J. Shaw, "Collusion-Secure Fingerprinting for Digital Data", *IEEE Trans. Inf. Theory*, IT-44, (1998) pp. 1897–1905.

[2] B. Lindström, "On B_2-Sequences of Vectors", *J. of Number Theory*, vol. 4, (1972) pp. 261–265.

[3] S. Litsyn, "New upper bounds on error exponents", *IEEE Trans. Inf. Theory*, IT-45, (1999) pp.385-398.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

A Calculus of Conditional Independence and its Applications in Cryptography

Ueli Maurer [1]

Abstract — **We present a simple calculus for deriving conditional independence relations of events and random variables and show how it can be applied to simplify, generalize and sometimes strengthen cryptographic security proofs relying on the indistinguishability of certain types of probabilistic constructions relevant in cryptography.**

The goal of our calculus is similar in spirit to those of other authors [3, 2, 1], but a crucial difference, important in our applications, appears to be that in addition to random variables occurring in the conditional independence relations, we also consider events.

The core of many classic security proofs of cryptographic systems relying on a pseudo-random function (e.g. implemented by a block cipher), is a proof that an idealized version of the system, with the pseudo-random function replaced by a random function, is statistically very close to a perfect system modeling the desired ideal behavior of the system. More precisely, it is proved that no adaptive distinguisher algorithm, even with unbounded computational resources, can distinguish the ideal and the perfect system with non-negligible probability, unless it queries the system for an infeasibly large number of inputs.

Our approach is based on defining appropriate conditioning events for the idealized system such that if the event occurs, then it behaves exactly like the perfect system. In this short abstract we cannot sketch the cryptographic applications.

Definition 1 Two events A and B are *conditionally independent*, given the event C, denoted $[A;B|C]$, if $P(A\cap B\cap C)\cdot P(C) = P(A\cap C)\cdot P(B\cap C)$ or, more briefly, if

$$P(ABC)\cdot P(C) = P(AC)\cdot P(BC).$$

If $P(C) > 0$, this is equivalent to $P(AB|C) = P(A|C)\cdot P(B|C)$. The concept of conditional independence and this notation can be extended to random variables:

Definition 2 Let S,T and U each be an event, a random variable, or a list consisting of events and random variables. S and T are *conditionally independent* given U, denoted $[S;T|U]$, if the conditional independence relation according to Definition 1 holds for all possible triples of events resulting when the random variables in S, T and U take on particular values.

The following theorem states under which condition an event or random variable can be deleted from an independence set or the conditioning set, shifted from an independence set to the conditioning set, or vice versa. Any random variables in an independence set can be deleted and, if accompanied in the set only by other random variables, then it can also be moved to the conditioning set.

[1]Department of Computer Science, ETH Zürich, CH-8092 Zürich, Switzerland. E-mail: maurer@inf.ethz.ch.

Theorem 1 *Consider a fixed random experiment and let S,T,U and V each be an event, a random variable, or a list consisting of events and random variables. If $[S;T|V]$, then $[S;U|TV]$ and $[S;TU|V]$ are equivalent, i.e., one implies the other:*

$$[S;T|V] \wedge [S;U|TV] \Longrightarrow [S;TU|V] \quad (1)$$

and

$$[S;T|V] \wedge [S;TU|V] \Longrightarrow [S;U|TV]. \quad (2)$$

If U is a random variable (or a list of random variables), then

$$[S;TU|V] \Longrightarrow [S;T|V], \quad (3)$$

$$[S;TU|V] \Longrightarrow [S;U|TV], \quad (4)$$

and

$$[S;T|UV] \wedge [S;U|V] \Longrightarrow [S;T|V]. \quad (5)$$

Proof. It suffices to prove the first claim for the case when S,T,U and V all are events. If some of the quantities S,T,U and V are random variables or lists of random variables, the fact that the implication holds for all events obtained by letting these random variables take on particular values implies that it also holds for the random variables. $[S;T|V]$ is equivalent to

$$P(STV)\cdot P(V) = P(SV)\cdot P(TV), \quad (6)$$

$[S;U|TV]$ is equivalent to

$$P(STUV)\cdot P(TV) = P(STV)\cdot P(TUV), \quad (7)$$

and $[S;TU|V]$ is equivalent to

$$P(STUV)\cdot P(V) = P(SV)\cdot P(TUV). \quad (8)$$

Equation (8) is obtained from (6) and (7) by multiplying the left side of (7) with the left side of (6) and the right side of (7) with the right side of (6), and canceling the terms $P(STV)$ and $P(TV)$ appearing on both sides. Similarly, (7) is obtained from (6) and (8) by multiplying the left side of (8) with the right side of (6) and the right side of (8) with the left side of (6), canceling the terms $P(V)$ and $P(SV)$ appearing on both sides. The second part of the proof is omitted. Δ

Note that if S, T, and U are events, then $[S;TU] \Longrightarrow [S;T|U]$ and $[S;TU] \Longrightarrow [S;T]$ are false in general. For instance, let $P(S) = P(T) = P(U) = 0.5$, $P(ST) = P(SU) = P(TU) = 0.2$, and $P(STU) = 0.1$. Then $P(STU) = P(S)P(TU) = 0.1$ but $P(STU)P(U) = 0.05 \neq P(SU)P(TU) = 0.04$.

References

[1] G. Kramer, Directed information for channels with feedback, Ph.D. Thesis, ETH Series in Information Processing, J. Massey (Ed.), vol. 11, Konstanz: Hartung-Gorre Verlag, 1998.

[2] J.L. Massey, Causal interpretation of random variables, *Problemy Peredachi Informatsii*, vol. 32, no. 1, pp. 112–116, July 1996.

[3] J. Pearl, *Probabilistic reasoning in intelligent systems: Networks of plausible inference*, Morgan Kaufmann, San Mateo, Calif., 1988.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Blind Identification of MIMO Systems Based On Source Correlative Filtering

João Xavier Victor Barroso
Instituto Superior Técnico
Instituto de Sistemas e Robótica
Torre Norte, Piso 7
Av. Rovisco Pais, 1049-001
Lisboa, Portugal
{jxavier,vab}@isr.ist.utl.pt

Abstract — **We introduce a closed-form blind channel estimator for multiple-input multiple-ouput (MIMO) finite impulse-response (FIR) systems, based only on second-order statistics (SOS). We rely on correlative filters at each transmitter to induce a spectral assimetry between the users. No additional power or bandwidth, nor synchronization between the sources, are required, and the original data rate is maintained. We show that, under a simple spectral condition on the transmitted random processes, this data preprocessing makes the MIMO channel uniquely determined (up to a phase offset per user) from the SOS of the MIMO system outputs. The closed-form algorithm which attains this channel identifiability bound is briefly discussed.**

I. Problem Formulation

Consider the P-input/N-output MIMO system, $\boldsymbol{y}(t) = \sum_{p=1}^{P} \boldsymbol{H}_p \boldsymbol{s}_p(t) + \boldsymbol{w}(t)$; here, $\boldsymbol{y}(t) \in \mathbb{C}^N$, $\boldsymbol{H}_p \in \mathbb{C}^{N \times M_p}$, $\boldsymbol{s}_p(t) = [s_p(t)\, s_p(t-1) \cdots s_p(t-M_p+1)]^T$, $s_p(t)$ is the scalar signal emitted by the pth user, and $\boldsymbol{w}(t) \in \mathbb{C}^N$ denotes additive noise. Our goal is the blind estimation of the MIMO channel matrix $\boldsymbol{H} \equiv [\boldsymbol{H}_1 \cdots \boldsymbol{H}_P]$ from the SOS of the observed data $\boldsymbol{y}(t)$. We assume: (A1) P (number of users) is known and $\boldsymbol{H}$ is full column rank, and (A2) the $s_p(t)$'s are uncorrelated zero-mean unit-power wide sense stationary processes, and the noise correlation matrices $\boldsymbol{R}_{\boldsymbol{w}}(\tau) = \mathrm{E}\left\{\boldsymbol{w}(t)\boldsymbol{w}(t-\tau)^H\right\}$ are known; $s_p(t)$ and $\boldsymbol{w}(t)$ are independent processes. Here, for simplicity, we also assume (A3) that $M_1, \ldots, M_P$ (users' channel orders) are known.

II. Channel Identifiability

As it is well known, the MIMO channel matrix $\boldsymbol{H}$ is not unambiguously defined from the SOS of its outputs, $\mathcal{R}_{\boldsymbol{y}} \equiv \{\boldsymbol{R}_{\boldsymbol{y}}(\tau) : \tau \in \mathbb{Z}\}$, if the sources are white up to 2nd order, *i.e.*, $r_{s_p}(\tau) = \mathrm{E}\{s_p(t) s_p(t-\tau)^*\} = \delta(\tau)$ (Kronecker delta). To make $\boldsymbol{H}$ identifiable from $\mathcal{R}_{\boldsymbol{y}}$, we propose to color the sources; *i.e.*, the pth user, rather than transmitting the white information sequence, say $a_p(t)$, emits the output of a correlative FIR filter, $s_p(t) = \sum_{l=0}^{L_p-1} f_p(l) a_p(t-l)$. Moreover, suppose that the correlative filters $\boldsymbol{f}_p = (f_p(0), \ldots, f_p(L_p-1))$ are designed as to satisfy: (A4) for each $p \neq q$, there is a correlation lag $\tau = \tau(p,q)$, such that $\sigma(\boldsymbol{A}_p(\tau)) \cap \sigma(\boldsymbol{A}_q(\tau)) = \emptyset$. Here, $\sigma(\boldsymbol{X})$ denote the spectrum (set of eigenvalues) of $\boldsymbol{X}$, and $\boldsymbol{A}_p(\tau) \equiv \boldsymbol{R}_{\boldsymbol{s}_p}(0)^{-1/2} \boldsymbol{R}_{\boldsymbol{s}_p}(\tau) \boldsymbol{R}_{\boldsymbol{s}_p}(0)^{-1/2}$ is the normalized autocorrelation matrix for the vector process $\boldsymbol{s}_p(t)$. Then, we have theorem 1.

Theorem 1. Under (A1)-(A4), $\boldsymbol{H}$ is uniquely determined (up to a phase offset per user) from the SOS of the MIMO system outputs $\mathcal{R}_{\boldsymbol{y}}$.

Condition (A4) on the correlative filters is not very restrictive. In fact, let M_p and L_p ($p = 1, \ldots, P$) be given, where $L_p \geq 1$ (*i.e.*, each correlative filter $\boldsymbol{f}_p$ has memory). Denote by $\mathcal{M}_L$ the set of all unit-norm minimum-phase FIR filters of degree L, let $\mathcal{M} \equiv \prod_{p=1}^{P} \mathcal{M}_{L_p}$ (Cartesian product), and denote by $\mathcal{F}$ the subset of $\mathcal{M}$ which satisfy (A4). Then, theorem 2 holds.

Theorem 2. $\mathcal{F}$ is dense in $\mathcal{M}$.

Proofs of both theorems can be found in [1]. Notice that unit-norm correlative filters are required in order to maintain the original transmitted power. The minimum-phase property is desirable as it permits to estimate the information symbols $a_p(t)$ by directly inverting the filters $\boldsymbol{f}_p$ (once $\boldsymbol{H}$ is identified).

III. Blind Identification Algorithm

We just outline the algorithm three main steps (for details, see [1]). We exploit theorem 1 as the basis of our identification strategy. It guarantees that, if $\boldsymbol{G} : N \times M$ ($M \equiv \sum_{p=1}^{P} M_p$) satisfies the equations $\boldsymbol{R}_{\boldsymbol{y}}(\tau) = \boldsymbol{G}\boldsymbol{R}_{\boldsymbol{s}}(\tau)\boldsymbol{G}^H + \boldsymbol{R}_{\boldsymbol{w}}(\tau)$ ($\tau \in \mathbb{Z}$), then $\boldsymbol{G} = \boldsymbol{H}$ (up to a phase offset per user); here, $\boldsymbol{R}_{\boldsymbol{s}}(\tau)$ are the correlation matrices of $\boldsymbol{s}(t) = [\boldsymbol{s}_1(t)^T \cdots \boldsymbol{s}_P(t)^T]^T$. Since the MIMO system is FIR, we only have to consider a finite number of equations, say for $\tau \in \mathcal{T} = \{\tau_1, \ldots, \tau_k\}$. Let $\boldsymbol{R}(\tau) \equiv \boldsymbol{R}_{\boldsymbol{y}}(\tau) - \boldsymbol{R}_{\boldsymbol{w}}(\tau)$ (denoised output correlation matrices). *Step 1*: we obtain $\boldsymbol{G}_0 = \boldsymbol{H}\boldsymbol{R}_{\boldsymbol{s}}(0)^{1/2}\boldsymbol{Q}^H$, where $\boldsymbol{Q} = [\boldsymbol{Q}_1 \cdots \boldsymbol{Q}_P]$: (unknown) unitary, as the square-root of $\boldsymbol{R}(0)$. *Step 2*: Focus on the pth user, and let $\boldsymbol{B}(\tau) \equiv \boldsymbol{G}_0^+ \boldsymbol{R}(\tau) \boldsymbol{G}_0^{+H} = \sum_{p=1}^{P} \boldsymbol{Q}_p \boldsymbol{A}_p(\tau) \boldsymbol{Q}_p^H$. Due to the unitary structure of $\boldsymbol{Q}$, $\boldsymbol{Q}_p$ satisfies the linear system (in the unknown $\boldsymbol{X}$) $\mathcal{L}$: $\boldsymbol{B}(\tau)\boldsymbol{X} - \boldsymbol{X}\boldsymbol{A}_p(\tau) = \boldsymbol{0}$, $\tau \in \mathcal{T}$. It turns out that, due to (A4), $\boldsymbol{Q}_p$ is the *unique* solution (within a scalar factor). Thus, solving $\mathcal{L}$ and re-scaling, yields $\boldsymbol{U}_p = \boldsymbol{Q}_p e^{i\theta_p}$. *Step 3*: Let $\boldsymbol{U} = [\boldsymbol{U}_1 \cdots \boldsymbol{U}_P]$. Then, $\boldsymbol{G} \equiv \boldsymbol{G}_0 \boldsymbol{U} \boldsymbol{R}_{\boldsymbol{s}}(0)^{-1/2}$ is a copy of $\boldsymbol{H}$ (up to a phase offset per user).

References

[1] J. Xavier, V. Barroso, and J. M. F. Moura, "Closed-form correlative coding (CFC_2) blind identification of MIMO Systems: isometry fitting to second order statistics," *submitted for publication*, August 1999

[2] J. Xavier, V. Barroso, and J. M. F. Moura, "Closed form blind channel identification and source separation in SDMA systems through correlative coding," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 8, pp. 1506–1517, October 1998

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Blind Source Separation Based on Multi-User Kurtosis Criteria

Constantinos B. Papadias
Wireless Communications Research
Bell Labs, Lucent Technologies
Holmdel, NJ 07733, USA
papadias@bell-labs.com

Abstract — **A novel technique for the blind source separation (BSS) of mutually independent and identically distributed i.i.d. discrete-time sequences is presented. The observed signals are assumed mixed through a narrow-band (memoryless) multiple-input-multiple-output (MIMO) noisy channel and are then processed by a linear MIMO receiver, whose outputs should ideally match the transmitted signals. In the proposed approach (called the Multi-User Kurtosis (MUK) algorithm), the linear receiver's matrix setting is computed adaptively based on the optimization of a constrained statistical criterion that involves only second and fourth order statistics of the receiver's output. At each iteration, the algorithm combines a stochastic gradient adaptation with a Gram-Shmidt orthogonalization that enforces its criterion's constraints. The analysis of its stationary points (presented in [1], [2]), reveals that it is globally convergent to a zero forcing -ZF (or decorrelating) solution, both in the absence of noise and in the presence of spatio-temporally white additive Gaussian noise.**

I. Summary

We consider the standard instantaneous mixture BSS problem: p i.i.d. and mutually independent zero-mean discrete-time sequences $a_l(k)$, $l=1,\ldots,p$, that share the same pdf, are transmitted through a $p \times q$ MIMO linear memoryless channel. The received signal model then takes the familiar form $Y(k)=\mathbf{H}A(k)+\mathbf{n}(k)$, where $A(k)=[a_1(k) \cdots a_p(k)]^T$ is the $p \times 1$ vector of source signals, $\mathbf{H}$ is the $q \times p$ channel matrix, $Y(k)$ is the $q \times 1$ vector of received signal snapshots, $\mathbf{n}(k)$ is the $q \times 1$ vector of additive noise samples, all at time instant k, and T denotes matrix or vector transpose. The received vector signal $Y(k)$ is subsequently filtered by a $q \times p$ "spatial equalizer" $\mathbf{W}$ which produces the $p \times 1$ vector output $\mathbf{z}(k)=[z_1(k) \cdots z_p(k)]^T$. The vector output $\mathbf{z}(k)$ is hence given by $\mathbf{z}(k)=\mathbf{W}^T Y(k)=\mathbf{W}^T\mathbf{H}A(k)+\mathbf{n}'(k)=\mathbf{G}^T A(k)+\mathbf{n}'(k)$, where $\mathbf{G}=\mathbf{H}^T\mathbf{W}$ is the $p \times p$ global response matrix and $\mathbf{n}'(k)=\mathbf{W}^T\mathbf{n}(k)$ is the filtered noise at the receiver output.

The MUK algorithm, which is presented in [2], is derived from the following optimization criterion

$$\begin{cases} \max\limits_{\mathbf{G}} & F(\mathbf{G})=\sum\limits_{j=1}^{p}|K(z_j)| \\ \text{subject to:} & \mathbf{G}^H\mathbf{G}=\mathbf{I}_p \end{cases} \tag{1}$$

where $K(x)=E\left(|x|^4\right)-2E^2\left(|x|^2\right)-|E\left(x^2\right)|^2$ is the kurtosis of x, $\mathbf{I}_p$ is the $p \times p$ identity matrix and H denotes Hermitian transpose (we also assume $\sigma_a^2=E(|a_l(k)|^2=1)$. The algorithm requires the received signal $Y(k)$ to be spatially pre-whitened, corresponding to a unitary channel $\mathbf{H}$. At each iteration, it first updates the receiver matrix through the following recursion

$$\mathbf{W}'(k+1)=\mathbf{W}(k)+\mu\,\text{sign}(K_a)\,Y^*(k)\mathcal{Z}(k) \tag{2}$$

where μ is the stepsize (a small positive scalar), $K_a=K(a_l(k))$, $\mathcal{Z}(k)=[|z_1(k)|^2 z_1(k)\cdots|z_p(k)|^2 z_p(k)]$, ($*$ denotes complex conjugate), and then it projects each column of $\mathbf{W}'(k+1)$ to the corresponding column of $\mathbf{W}(k+1)$ through

$$W_j(k+1)=\frac{W_j'(k+1)-\sum\limits_{l=1}^{j-1}(W_l^H(k+1)W_j'(k+1))W_l(k+1)}{\|W_j'(k+1)-\sum\limits_{l=1}^{j-1}(W_l^H(k+1)W_j'(k+1))W_l(k+1)\|} \tag{3}$$

where $\|X\|^2=X^HX$. The resulting MUK algorithm is described in Table 1. In [1], [2], the following theorem was shown regarding the convergence of the MUK algorithm:

1.	$k=0$: initialize $\mathbf{W}(0)=\mathbf{W}_0$
2.	for $k>0$
3.	Obtain $\mathbf{W}'(k+1)$ from (2)
4.	Obtain $W_1(k+1)=W_1'(k+1)/\|W_1'(k+1)\|$
5.	for $j=2:p$
6.	Compute $W_j(k+1)$ from (3)
7.	Go to 5
8.	$\mathbf{W}(k+1)=[W_1(k+1)\cdots W_p(k+1)]$
9.	Go to 2

Table 1: The MUK algorithm

Theorem 1 *Both in the absence of noise and in the presence of additive noise with mutually independent i.i.d. and circularly symmetric Gaussian components (of variance σ_n^2 each), and assuming that $Y(k)$ is perfectly pre-whitened (corresponding to a unitary $\mathbf{H}$), the only maxima of the MUK algorithm correspond to a decorrelating (zero-forcing) detector, i.e. to a solution of the following type*

$$\mathbf{G}=\Phi\Pi \tag{4}$$

where $\Phi=diag([e^{i\phi_1}\cdots e^{i\phi_p}])$, $i=\sqrt{-1}$, $\phi_1,\ldots,\phi_p$, are arbitrary phases, and Π is a $p \times p$ permutation matrix.

References

[1] C. B. Papadias. "Blind signal separation in narrow band BLAST systems". *CISS 2000 Conference*, pages TP3-7–TP3-10, Princeton, NJ, USA, March 15-17, 2000.

[2] C. B. Papadias. "A multi-user kurtosis algorithm for blind source separation". *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2000)*, Istanbul, Turkey, June 5-9, 2000.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Independent Component Analysis for Blind Multiuser Detections

Anthony Kuh[1]
Dept. of Electrical Engineering
University of Hawaii at Manoa
Honolulu, HI96822
USA
e-mail:
kuh@spectra.eng.hawaii.edu

Xiaohong Gong
Dept. of Electrical Engineering
University of Hawaii at Manoa
Honolulu, HI96822
USA
e-mail:
xhgong@spectra.eng.hawaii.edu

Abstract — **We apply a novel signal processing method based on Independent Component Analysis (ICA) to blind multiuser receivers. ICA is well suited for blind multiuser detection problems as the criterion used to separate signals is a mutual information minimization principle which attemps to separate independent signals from mixed signals. When the cross-correlations between signature sequences are big, ICA has better performance than decorrelating receivers and linear MMSE receivers.**

I. CDMA System Description

We consider the following CDMA system where the signal at a given receiver consists of the sum of N transmitted user signals embedded in additive white Gaussian noise [2].

$$y(t) = \sum_{k=1}^{N} \sum_{i=-M}^{M} A_k b_k S_k(t - iT - \tau_k) + \sigma n(t) \qquad (1)$$

where A_k is the received amplitude of the kth user's signal, and $b_k \in \{-1, +1\}$ is the bit transmitted by the kth user. S_k is the deterministic signature sequence assigned to the kth user. The length of the packets transmitted by each user is $2M + 1$. $\tau_k \in [0, T)$ is the delay of the kth user and $\tau_k = 0$ corresponds to a synchronous channel model. $n(t)$ is white Gaussian noise with unit power spectral density and σ is the noise deviation.

II. Independent Component Analysis

Independent Component Analysis (ICA) is a linear transformation of data such that the elements become statistically independent. ICA is well suited for blind multiuser detection problem. In CDMA communications, user signals are independent from each other. The channel output is the linear mixture of multiuser signals and additive white Gaussian noise.

$$X = As \qquad (2)$$

where X is the channel output, A is a mixing matrix, and s is a vector containing original user signals and additive white Gaussian noise. ICA will determine a weight vector such that

$$\hat{s} = WX \qquad (3)$$

here $\hat{s}$ is the estimate of independent source signals and the components of $\hat{s}$ are called Independent Components (IC). In order to make the components of $\hat{s}$ as independent as possible, ICA will find a linear transformation that can minimize the output mutual information [1].

[1]This work is supported in part by NSF Grant No.9625557.

III. XICA Algorithm and Simulation Results

The XICA algorithm combines the fixed-point algorithm proposed by Hyvarinen [1] and a detection scheme. After the fixed-point algorithm converges, we can get the demixing matrix W and by using the detection scheme that we propose, we can separate the desired user signals from others. The detection scheme works as follows: First, calculate the correlation between the desired user signature sequence and each column of $\hat{A}$ which is the inverse of W matrix. Then take the IC with the largest absolute correlation and this IC is the desired user signal.

If we use Gold code as spreading sequences, the performance of ICA is similar to the linear MMSE receiver and the decorrelating receiver. By using a set of spreading sequences that have bigger correlations and smaller processing gains, ICA performs better than the other two linear receivers. We consider a synchronous five-user Gaussian channel. All users have equal energy, the correlation coefficient is 0.2, and the spreading gain is 5. Figure 1 shows that ICA performs better than the linear MMSE and the decorrelating receiver. Since Gassian noise is independent of all user signals and it is symmetric in all directions, ICA can mitigate the noise by extracting user signals first and leaving noise behind.

References

[1] A. Hyvarinen and E. Oja. Independent component analysis:A tutorial, *http://www.cis.hut.fi/ aapo/papers*, 1999.

[2] S. Verdu. *Multiuser Detection*. Cambridge University Press, Cambridge, United Kingdom, 1998.

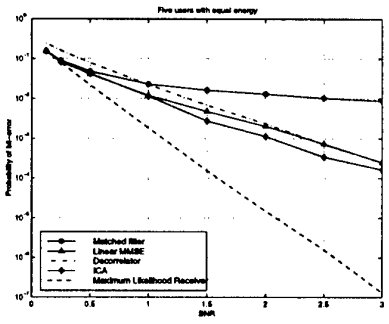


Figure 1: Linear CDMA receiver performance

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Blind Adaptive Multiuser Detection with Averaging for Cellular Systems [1]

Deepak Das and Mahesh K. Varanasi
Department of Electrical and Computer Engineering
University of Colorado, Boulder, CO 80309-0425, USA
e-mail: dasd@ucsu.colorado.edu varanasi@schof.colorado.edu

Abstract — **We consider blind adaptive multiuser detection in Correlated Waveform Multiple Access (CWMA)-based cellular radio networks. A common stochastic approximation (SA) based framework is proposed from which three blind adaptive algorithms for linear MMSE detection are obtained. Two of them coincide with previously proposed algorithms and the third is shown to be best suited for implementation at a base station. Improvement in terms of convergence properties of these SA-based adaptation algorithms is sought by using the more recent results on the SA technique with *averaging*.**

I. System Model

We consider a cellular network model in which there are B base stations with K_j users assigned to base j. While the transmissions of out-of-cell users are received symbol-asynchronously at a base station, it is assumed, for the sake of simplicity, that in-cell users are symbol-synchronous. A base station is assumed to have knowledge of the (common) timing of the received signals of only the users in its own cell. For simplicity, we assume binary antipodal signalling.

The discrete-time model for the N_j matched filter outputs at base j can be expressed as

$$\mathbf{y}_j = \sum_{i=1}^{K_j} \sqrt{w_{ij} g_{ijj}}\, \mathbf{s}_{ij} b_{ij} + \sum_{l \neq j}^{B} \sum_{i=1}^{K_l} \sqrt{w_{il} g_{ilj}} \left(\mathbf{s}^-_{ilj} b^-_{il} + \mathbf{s}^+_{ilj} b^+_{il} \right) + \chi_j, \quad (1)$$

where the channel gain to base j, the transmit power and the transmitted symbol of the i^{th} user of base l are denoted by g_{ilj}, w_{il} and b_{il}, respectively. $\mathbf{s}_{ij}$ denotes the vector representation (the "signature sequence") of the signal of user i of base j with respect to a set of orthonormal basis functions that spans at least the in-cell signal subspace. For the same basis functions, the vectors $\mathbf{s}^-_{ilj}$ and $\mathbf{s}^+_{ilj}$ denote the segments of the signals associated with the two symbols of user i of base l, b^-_{il} and b^+_{il}, respectively, that overlap with the symbol of interest at base j. χ_j is an N_j-dimensional zero-mean Gaussian random vector with a covariance matrix equal to $\sigma_j^2\mathbf{I}$. For base j, let us denote the signal matrix for in-cell users as $\mathbf{S}_j = [\mathbf{s}_{1j}\mathbf{s}_{2j}\cdots\mathbf{s}_{K_jj}]$ and the diagonal matrix of in-cell user energies as $\mathbf{W}_j = \mathrm{diag}\,[w_{1j}g_{1jj}, \cdots, w_{K_jj}g_{K_jjj}]$. With $i = 1, \cdots, K_l$ and $l \neq j$, the out-of-cell signal and user energy matrices will be denoted as $\mathbf{S}^-_j = \left[\left\{\mathbf{s}^-_{ilj}\right\}\right]$, $\mathbf{S}^+_j = \left[\left\{\mathbf{s}^+_{ilj}\right\}\right]$ and $\tilde{\mathbf{W}}_j = \mathrm{diag}\,[\{w_{il}g_{ilj}\}]$, respectively.

II. Blind Multiuser Detection with Averaging

We will consider detection at base station 1. The linear MMSE multiuser detector for user k is given (with suitable scaling) as the unique solution to the equation: $\mathbf{A}\mathbf{c}_{k1} = \mathbf{s}_{k1}$, where $\mathbf{A} \triangleq \mathbf{S}_1\mathbf{W}_1\mathbf{S}_1^T + \bar{\mathbf{S}}_1^-\bar{\mathbf{W}}_1(\bar{\mathbf{S}}_1^-)^T + \bar{\mathbf{S}}_1^+\bar{\mathbf{W}}_1(\bar{\mathbf{S}}_1^+)^T + \sigma_1^2\mathbf{I}$.

From the theory of iterative methods to solve linear equations, we can form the following general deterministic iteration

$$\mathbf{c}_{k1}(n) = (\mathbf{I} - \mu_n\mathbf{Q}\mathbf{A})\mathbf{c}_{k1}(n-1) + \mu_n\mathbf{Q}\mathbf{s}_{k1}, \quad (2)$$

that converges to the desired $\mathbf{c}_{k1}$. $\mathbf{Q}$ is a nonsingular matrix, whose inverse is called the splitting matrix. Replacing $\mathbf{Q}$ by the identity matrix and $\mathbf{A}$ by its instantaneous stochastic estimate $\mathbf{y}_1(n)\mathbf{y}_1(n)^T$, leads to the stochastic approximation based algorithm in [1]. Further, using the canonical representation for the (scaled) MMSE linear detector, $\frac{1}{\mathbf{s}_{k1}^T\mathbf{A}^{-1}\mathbf{s}_{k1}}\mathbf{c}_{k1} = \mathbf{s}_{k1} + \mathbf{p}_{k1}$, $\mathbf{p}_{k1} \perp \mathbf{s}_{k1}$, we can replace $\mathbf{Q}$ by $\mathbf{P}^{\perp}_{\mathbf{s}_{k1}} = \mathbf{I} - \mathbf{s}_{k1}(\mathbf{s}_{k1}^T\mathbf{s}_{k1})^{-1}\mathbf{s}_{k1}^T$ (note that in this case, $\mathbf{Q}$ is singular) to adaptively estimate $\mathbf{p}_{k1}$:

$$\mathbf{s}_{k1} + \mathbf{p}_{k1}(n) = (\mathbf{I} - \mu_n\mathbf{P}^{\perp}_{\mathbf{s}_{k1}}\mathbf{y}_1(n)\mathbf{y}_1^T(n))(\mathbf{s}_{k1} + \mathbf{p}_{k1}(n-1)). \quad (3)$$

$\mu_n > 0$ is a suitably chosen fixed or decreasing step-size sequence. The rule in (3) can be shown to be identical to the one in [2], where it was derived differently by minimizing the output energy. Both the recursions mentioned above are based on the knowledge of only each user's own signal, i. e., $\mathbf{s}_{k1}$.

Defining $\mathbf{B} \triangleq \mathbf{S}_1\mathbf{W}_1\mathbf{S}_1^T + \sigma_1^2\mathbf{I}$, we observe that in a cellular system where the out-of-cell interferers are typically weak, $\mathbf{B}$ can be considered as a course approximation of $\mathbf{A}$. Therefore, with the knowledge of the signals of the in-cell users, their energies, and the noise variance, we replace $\mathbf{Q}$ by $\mathbf{B}^{-1}$ to obtain:

$$\mathbf{c}_{k1}(n) = (\mathbf{I} - \mu_n\mathbf{B}^{-1}\mathbf{y}_1(n)\mathbf{y}_1(n)^T)\mathbf{c}_{k1}(n-1) + \mu_n\mathbf{B}^{-1}\mathbf{s}_{k1}. \quad (4)$$

This algorithm is seen to converge more quickly to the MMSE solution than its single-signal based counterparts.

A recent fundamental development in stochastic approximation is the idea of averaging as introduced for multidimensional problems in [3]. The stochastic version of the general deterministic rule in (2) can be modified to include an averaging step after the "basic" recursion:

$$\mathbf{c}_{k1}(n) = (\mathbf{I} - \mu_n\mathbf{Q}\mathbf{y}_1(n)\mathbf{y}_1(n)^T)\mathbf{c}_{k1}(n-1) + \mu\mathbf{Q}\mathbf{s}_{k1}, \quad (5)$$

$$\tilde{\mathbf{c}}_{k1}(n) = \frac{1}{n}\sum_{i=1}^{n}\mathbf{c}_{k1}(i). \quad (6)$$

The "smoothing" effect of the averaging allows the basic recursion step to use "larger" step-sizes than would be feasible for the non-averaged adaptive rule leading to an improvement in convergence. Analytical convergence for (3) is shown in a manner different than in [2]. The adapatations with averaging are shown to converge with zero asymptotic mean squared error under the assumption of a completely synchronous system and almost surely for the asynchronous model.

[1] This work was supported in part by NSF Grant NCR-9725778 and ARO grant DADD 19-99-1-0291.

References

[1] S. Ulukus and R. D. Yates, "A Blind Adaptive Decorrelating Detector for CDMA Systems", *IEEE Journal on Selected Areas of Communications*, Vol. 16, No. 8, pp. 1530-1541, October 1998.

[2] M. L. Honig, U. Madhow and S. Verdu, "Blind Adaptive Multiuser Detection", *IEEE Transcations on Information Theory*, Vol. 41, pp. 994-960, July 1995.

[3] B. T. Polyak, "New Stochastic Approximation Type Procedures", *Automat. i Telemekh.*, N7, pp. 98-107, 1990. (In Russian); translated in *Automatic Remote Control* Vol. 51, 1991.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Iterative Multistage Decoding of BCM Codes

Diana Stojanović
Department of Electrical Eng.
University of Hawaii
Honolulu, HI 96822
e-mail:
dixi@spectra.eng.hawaii.edu

Shu Lin
Department of Electrical and Computer Engineering
University of California, Davis
One Shields Avenue
Davis, CA 95616
e-mail: slin@ece.ucdavis.edu

Marc P.C. Fossorier
Department of Electrical Eng.
University of Hawaii
Honolulu, HI 96822
e-mail:
marc@spectra.eng.hawaii.edu

Abstract — **In this paper, we investigate a suboptimum version of the iterative multistage maximum likelihood algorithm presented in [2]. Application to Block Coded Modulation is considered. Conditions are introduced which reduce the computational complexity and decoding delay. Simulation results support the claims.**

I. Summary

Decomposable and multilevel codes [1], such as block coded modulation (BCM) codes, can be efficiently decoded by multistage decoding(MSD) algorithm. In the conventional MSD, the reduction of complexity, as compared to maximum likelihood decoding (MLD) algorithms, is achieved at the expense of increased error rate. For short codes, the performance degradation is small. The discrepancy between the optimum and MSD algorithms becomes apparent when long codes are used.

The iterative multistage (IMS) MLD [2] can be used to obtain the optimum performance for a given code. This algorithm achieves MLD through iterations with optimality tests at each decoding stage. In [3], another MSD algorithm for decoding multilevel codes based on list decoding of the outer codes was presented. The improvement is achieved by passing additional estimates from the first to the second decoding stage when the distance of the decoded codeword from the received sequence is larger than a given threshold.

The algorithms presented here combine those in [2] and [3]. Let $\mathrm{ED}^{(i),iter}$ denote the squared Euclidean distance between the received sequence $(r_{xl}, r_{yl})_{l=1,2,\ldots N}$ and the estimate at i-th decoding stage of iteration $iter$. The optimum version of IMS-MLD is based on two simple facts: 1) $\mathrm{ED}^{(i),iter} \leq \mathrm{ED}^{(i+j),iter}$ and $\mathrm{ED}^{(i),iter} \leq \mathrm{ED}^{(i),iter+j}$ for $j > 0$; 2) if the **constellation label sequence** at the first stage, $\mathrm{CLS}^{(1)}$, is a codeword in the BCM code, then no further estimate will be closer to received sequence than $\mathrm{CLS}^{(1)}$ is.

In the suboptimum version, threshold decoding is used to reduce the number of iterations. Due to new criteria introduced as a modification of [2], optimality is not claimed. However, the simulations show that properly chosen values of thresholds can lead to good error performances. This algorithm is particularly useful when long codes are used as outer codes in BCM schemes. Both algorithms are given in Figure 1, where dashed lines denote modifications that lead to suboptimum version.

Examples of several codes will be presented to show the performance vs. decoding complexity.

[1]This research was supported by the National Science Foundation under Grants No. NCR-94-15374 and NCR-97-32959, and NASA under Grant NAG 5-931.

References

[1] H. Imai and S. Hirakawa, "A new multilevel coding method using error correcting codes." *IEEE Transactions on Information Theory*, vol. IT-23, no. 3, pp. 371-376, May 1977.

[2] D. Stojanovic, M.P.C. Fossorier and S. Lin "Iterative Multistage Maximum Likelihood Decoding of Multi-Level Codes" *Proceedings of the 1999 Conference on Coding and Cryptography*, Paris, France January 10-14, 1999.

[3] U. Dettmar, J. Portugheis and H. Hentsch "New Multistage Decoding Algorithm" *Electronic Letters*, vol. 28 No. 7 pp. 635-636, 1992.

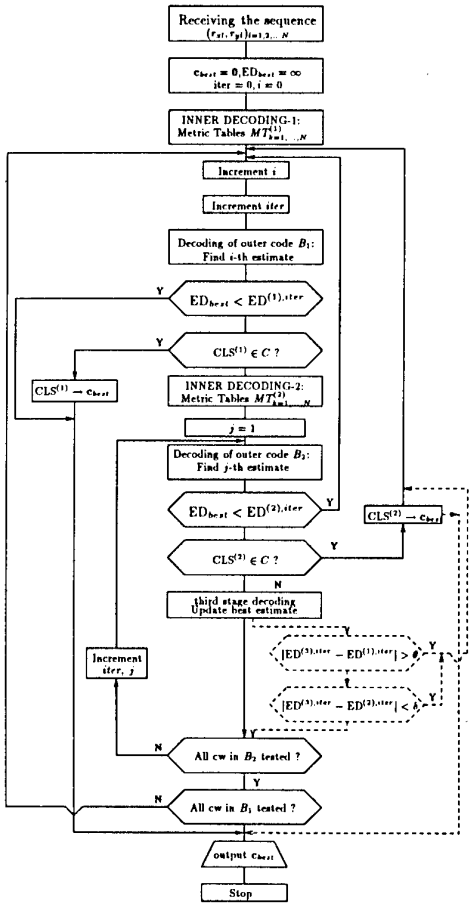


Fig. 1: Flowchart of the Iterative Decoding Algorithm for 3-level code

0-7803-5857-0/00/$10.00 ©2000 IEEE.

A New Block-Coded Modulation Scheme for Rayleigh Fading Channel, Soft Output Decoding Issues

Shahram Yousefi[1], Erik S. Hons[2], and Amir K. Khandani
Dept. of Elec. and Comp. Eng.
University of Waterloo
Waterloo, ON, Canada N2L 3G1
shahram,eshons,khandani@shannon.uwaterloo.ca

Brendan J. Frey
Dept. of Comp. Science
University of Waterloo
Waterloo, ON, Canada N2L 3G1
frey@dendrite.uwaterloo.ca

Abstract — **We investigate the application of the sum-product algorithm to the decoding of a q-ary Block-Coded Modulation (BCM) scheme which is based on extending the parity check equations of a binary block code to q-ary symbols. This is achieved by decomposing the code into a sub-code with an acyclic Tanner graph and its cosets which are represented by a trellis diagram. The combination of these two cycle-free graphs are used to develop an efficient soft output decoding algorithm for the given code.**

I. Introduction

Our objective has been to develop a soft output decoding method for the BCM codes proposed in [1]. The corresponding construction is based on extending good binary block codes from $GF(2)$ to Z_q. They assume a q-PSK signal constellation where the components of the q-ary code are directly mapped to the q-PSK points using an appropriate labeling. The extension of the binary linear code to a q-ary linear code is based on extending the parity check equations to $\{0, 1, ..., q-1\}$, mod q constraints. In this case, the encoder inputs $\log(q^k) = k \cdot \log(q)$ bits and outputs a length n codeword of elements of $Z_q = \{0, 1, ..., q-1\}$ which are each mapped to the points of a q-PSK constellation. The resulting scheme is $2n$-dimensional with a minimum time diversity of MTD= d, and Band-Width-Efficiency (BWE) of $\eta = k \cdot \log(q)/n = R \cdot \log(q)$ bits/2-D symbol ($R = k/n$ is the binary code rate). Therefore the optimality of these codes for a Rayleigh fading channel in terms of MTD and BWE is tantamount to that of the underlying binary block code. These schemes fall into the category of codes over rings and groups which recently have received a lot of attention among coding theorists [2].

II. Decoding

Consider the communication system in Figure 1 where k information bits $\vec{u} = (u_1, u_2, ..., u_k)$ are first encoded to n channel symbols $\vec{x} = (x_1, x_2, ..., x_n)$ and then transmitted through the channel which outputs $\vec{y} = (y_1, y_2, ..., y_n)$. Channel is memoryless such that each channel output y_i is only related to the channel input at the same time, namely, x_i, by, $y_i = \alpha_i \cdot x_i + n_i$, where α_i is 1 for an AWGN channel and Rayleigh-distributed for a Rayleigh fading channel. For a probability propagation decoding, one can construct a probabilistic model for the system by examining the encoding process and the channel. Then, a soft output decoding method

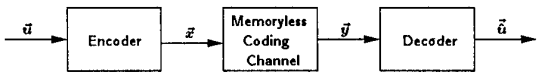


Figure 1: General Memoryless Coding Channel.

that maximizes $\Pr(x_i \mid \vec{y})$, $i = 1, 2, \ldots, n$, will minimize the symbol (q-ary) error probability. The sum-product algorithm provides an efficient way for calculating such marginals using a graphical representation of the code [3, 4].

In [1], a 2-level decoding method based on a generalization of the method discussed in [5] is proposed. To decode the constructed BCM scheme, the codebook which has a cyclic Tanner graph (TG) is decomposed to a sub-code with an Acyclic Tanner Graph (ATG), and its cosets. The significance of representing the code by an ATG is that, one can use a generalization of the well-known *Wagner* rule for their decoding. A composite Tanner graph-Trellis (TG-T) is used to represent the code structure.

On the other hand, it is well known that the probability propagation algorithms for soft output decoding, e.g., BCJR algorithm, can be used on a cycle-free graph to produce an exact probability calculation of code symbols. Examples of such cycle free graphs include a trellis representation and a cycle-free Tanner graph. The focus of the current article is to use the TG-T representation of the code (which is based on the combination of two cycle free graphical representations) to produce an efficient soft output decoding method.

The bit error performance of the resulting code construction will depend on the method used for the bit labeling of the underlying q-PSK constellation. We will present a discrete optimization method to optimize such labeling to minimize the resulting bit error probability.

[1] This work was supported by Natural Sciences and Engineering Research Council of Canada (NSERC).

[2] This work was supported by Communications and Information Technology Ontario (CITO).

References

[1] S. Yousefi and A. K. Khandani, "Codes over rings for Rayleigh fading channel," In *Proc. 34th Annu. Conf. on Inform. Sci. and Sys. CISS 2000*, Princeton, NJ, USA, vol. 1, WP7-23-27, March 15-17, 2000.

[2] G. Caire and E. Biglieri, "Linear block codes over cyclic groups," *IEEE Trans. Inform. Theory*, vol. IT-41, Sept. 1995, pp. 1246-1256.

[3] B. J. Frey, *Graphical Models for Machine Learning and Digital Communications*, MIT Press, Cambridge MA, 1998.

[4] F. R. Kschischang, B. J. Frey, and H.-A. Loeliger, "Factor graphs and the sum-product algorithm," preprint, 1998.

[5] M. Esmaeili and A. K. Khandani, "Acyclic Tanner graphs and two-level decoding of linear block codes," Proc. of *IEEE Int. Symp. Inform. Theory*, Cambridge, MA, USA, pp. 91, Aug. 16-21 1998.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Iterative Viterbi Algorithm for Concatenated Multidimensional TCM

Qi Wang and Lei Wei
Department of Engineering
The Australian National University
ACT 0200, AUSTRALIA

Abstract — **In this paper, we apply the iterative Viterbi algorithm (IVA) to decode a concatenated multidimensional TCM in which a trellis code is used as the inner code and a simple even parity code is used as the outer code.**

I. Introduction

In this work, we extend the iterative Viterbi algorithm (IVA) [2][3] for concatenated multidimensional (MD) trellis codes. With a simple BCH code, at $BER = 4.4 \times 10^{-6}$ about 2.2 dB additional net gain can be achieved using the IVA for the 4D 16-state Wei's code [1] at a spectral efficiency of 7 bits/T.

II. Encoding the Concatenated MD TCM

In Fig. 1, there are $(m-1)$ information streams organized into a block of $(m-1)$ rows. The m^{th} stream called the parity-check (PC) stream is then generated in such way that the trellis-encoded bits in the m^{th} stream will be the parity of the trellis-encoded bits of the $(m-1)$ information streams, i.e., $I^t_{m,c} = \sum_{i=1}^{m-1} \oplus I^t_{i,c}$. The non-trellis-encoded bits in the m^{th} stream are intact.

We noted that the operation of differential encoder in Wei's code design is a nonlinear operation. Therefore, to prevent the PC property being violated after the differential encoding, we impose the PC condition on the trellis-encoded bits of all the m streams only after the differential encoding.

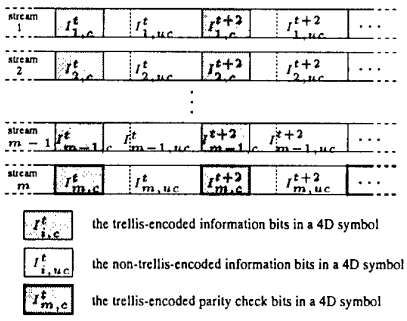


Figure 1: 1D structure consisting of the m streams

III. Decoding the Concatenated MD TCM Using the IVA

Let R^t_i $(i = 1,2,\cdots,m)$ denote the received 4D signals of the m streams at time t. Let Z^t_i and Z^{t+1}_i denote the 2D encoded codewords of the i^{th} stream in the first and second 2D sub-constellations at time t, respectively.

In the IVA, the likelihood function of the 4D type in the $(m-1)^{th}$ stream at time t is

$$\begin{aligned} \lambda^t_{m-1} &= -\log\left[P(R^t_1, R^t_2, \cdots, R^t_m | Z^t_{m-1}, Z^{t+1}_{m-1})\right] \quad (1) \\ &\approx \lambda^{t(v)}_{m-1} + \lambda^{t(p)}_{m-1}. \end{aligned}$$

where $\lambda^{t(v)}_{m-1}$ denotes the branch metric value, which is identical to the metric used in the VA, and $\lambda^{t(p)}_{m-1}$ denotes the *extrinsic* metric value introduced by the PC condition from the other streams. The metric function $\lambda^{t(p)}_{m-1}$ is equal to the metric used in the VA for the m^{th} stream, but it is "controlled" by the estimated PC condition $\widehat{W}^t_{m-2} = \sum_{i=1}^{m-2} \oplus \hat{I}^t_i$, where $\hat{I}^t_i$ is the decision of I^t_i in the previous iteration.

IV. Numerical Results

Figure 2 presents the performance of the 4D 16-state Wei's code using the 2D IVA with and without BCH code at a spectral efficiency of 7 bits/T. It is shown that at $BER = 4.4 \times 10^{-6}$ level about 2.7 dB gross gain or 2.2 dB net gain is achieved.

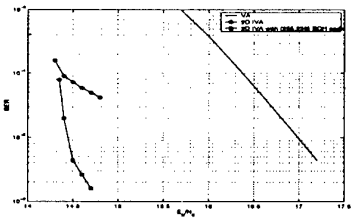


Figure 2: Performance of the 4D 16-state Wei's codes using the VA and 2D IVA at a spectral efficiency of 7 bits/T

V. Conclusions

Significant gains for concatenated 4D trellis codes using the IVA over the use of the VA can be obtained with low complexity and reasonable computation. The cases of the 8D and higher dimensional concatenated TCM can be obtained through the similar way. More results about the performance of other decoding algorithms can be found in [4].

References

[1] L. F. Wei, "Trellis coded Modulation with multidimensional constellations", *IEEE Trans. on Inform. Theory*, Vol. IT-33, pp. 483-501, July 1987.

[2] Q. Wang, L. Wei and R. A. Kennedy, "Iterative Viterbi decoding, trellis shaping and multilevel structure for high-rate concatenated TCM", submitted to *IEEE Trans. on Comm.*

[3] L. Wei, "Near shannon limit iterative Viterbi algorithm for Forney concatenated systems," submitted to *IEEE Trans. on Inform. Theory.*

[4] Q. Wang and L. Wei, "Complexity and Performance Comparison of Graph-Based Iterative Decoding Algorithms for Parity-Concatenated Trellis Codes", submitted to *IEEE Trans. on Inform. Theory.*

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Trellis Coded Modulation with More Than One Redundancy Bit

The Cuong Dinh and Takeshi Hashimoto
Dept. of Electron. Eng., The Univ. of Electro-Communications
Chofu, Tokyo, 182-8585 Japan. Email dinh@chopin.ee.uec.ac.jp

Abstract — **A multilevel coding approach to the construction of multidimensional (MD) GU trellis codes is considered. We present a family of GU trellis codes with good trade-off between SNR, decoding complexity with stage decoding, and coding rate near the cut-off rate.**

I. Introduction

For a transmission rate of hn bits per h channel symbols over an AWGN channel employing 2D QAM signals, almost all TCM schemes known in the literature assume that the modulator has twice more signal h-tuples than strictly needed. The redundancy of the trellis code is then 1 bit per h symbols and it has been shown by Ungerboeck that very litle increamental gain can be achieved by further increasing the modulator alphabet redundancy. It seems that the only way to make the trellis code more powerful is to increase the number of encoder states. The problems are the maximum likely-hood decoding complexity and the lack of algebraic methods to synthesize good codes with many states: the only practical way is to generate a large number of codes in a small class where one expects to find the best codes, followed by their performance evaluation. However, an exhaustive search for good codes with many states still remains difficult even for the class of Geometrically Uniform (GU) codes [1] whose symmetry properties and algebraic structure permit an efficient search for good codes.

In this paper, we show that a possible way to solve the problem is to allow the code to have more redundancy than one bit so that a stage construction [2] can be used to simplify the search for good codes with many states in connection with reduced decoding complexity, using stage decoding.

II. Multilevel Code Construction

A 2^{n+1}-point QAM signal constellation S is partitioned in two steps according to the GU partition chain $\mathbf{Z}^2/R\mathbf{Z}^2/2R\mathbf{Z}^2$ using a reflection v about the vertical axis, a reflection g about the origin, and a translation τ by $(0,2)$. This gives a 8-way GU partition of S isomorphic to $\mathbf{Z}_2^3$. For a positive integer $h \geq 2$, the encoder structure for $2h$-D GU trellis codes is shown in Fig. 1. As a multilevel code, one bit of the code C_1, which is the best 2^{ν_1}-state rate-$1/h$ binary convolutional codes, identifies a coset in $\mathbf{Z}^2/R\mathbf{Z}^2$ and a pair of bits of the code C_2, which is the 2^{ν_2}-state rate-$(2h-1)/2h$ binary convolutional code taken from the best $2h$-D trellis codes employing 4-way partition of the QAM constellation, selects a coset in $R\mathbf{Z}^2/2R\mathbf{Z}^2$ each time. The third level is uncoded. As an encoder for an MD trellis code, the scheme generates a $2h$-D GU trellis code $\mathbf{C}$ with $2^{\nu_1+\nu_2}$ states and a transmission rate of n bit/sym. For $h = 2, 3, 4$, we have found codes with good performance/complexity trade-off with stage decoding. Table 1 shows the search result for $h = 2$. The encoder's generators are given in octal. Effective coding gain is in decibels.

III. Performance Analysis

Figure 2 shows cut-off rates of two-step partition of the 64QAM constellation. The code design region for transmission of 5 bit/sym is shadowed. For $h = 2, 3, 4$, rates of component codes are shown together with required SNR for stage decoding to perform well [3]. In this region, the rate and decoding complexity are traded-off by the SNR.

References

[1] G. David Forney, Jr., "Geometrically uniform codes", *IEEE Trans. Inform. Theory*, vol. 37, pp. 1241–1260, Sept. 1991.

[2] R. Garello and S. Benedetto, "Multilevel construction of block and trellis group codes", *IEEE Trans. Inform. Theory*, vol. 41, pp. 1257–1264, Sept. 1995.

[3] U. Wachsmann, Robert F. H. Fischer, and Johannes B. Huber, "Multilevel codes: theoretical concepts and practical design rules", *IEEE Trans. Inform. Theory*, vol. 45, pp. 1361–1391, July 1999.

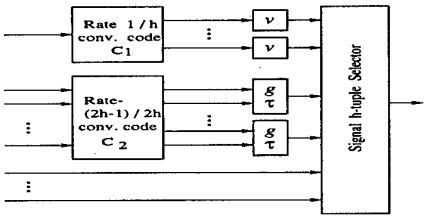


Fig. 1: The encoder structure

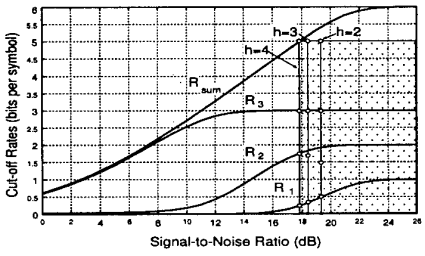


Fig. 2: Cut-off rates of the partition of 64QAM. Design rates for constituent codes ($h = 2, 3, 4$).

Tab. 1: 4D GU trellis codes ($h = 2$).

C_1			C_2		$\mathbf{C}$	
ν_1	generators		ν_2	taken from	γ_{eff}	$\tilde{N}_D$
4	23	35	3	Wei's 4D code	4.84	88
5	53	75	3	Wei's 4D code	5.17	104
6	133	171	3	Wei's 4D code	5.33	136
6	133	171	4	Wei's 4D code	5.70	152
6	133	171	5	Wei's 4D code	6.02	248

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Hardness of Approximating the Minimum Distance of a Linear Code

Daniele Micciancio
Dept. of Computer Science and Engineering
University of California at San Diego
La Jolla, CA 92093-0114, USA

Ilya Dumer[1]
College of Engineering
University of California at Riverside
Riverside, CA 92521, USA

Madhu Sudan[2]
Dept. of Electrical Engineering and Computer Science
Massachusetts Institute of Technology
Cambridge, MA 02139, USA

Abstract — **We show that the minimum distance d of a linear code is not approximable to within any constant factor in random polynomial time (RP), unless NP equals RP. In the process we show that it is hard to find the nearest codeword even if the number of errors exceeds $d/2$ by an arbitrarily small fraction ϵd.**

I. Introduction

Consider a linear code $\mathcal{A}[n,k,d]_q$ with generator matrix $\mathbf{A} \in \mathbb{F}_q^{k\times n}$. We study complexity of the following problems:

- *Approximate* the Minimum Distance d of a linear code $\mathcal{A}$;
- Find the Nearest Codeword $\mathbf{y}$ for the received vector $\mathbf{x}$.

Vardy [5] proved that it is NP-hard to compute d *explicitly*. The (second) Nearest Codeword Problem (NCP) was proven to be NP-hard in [3]. More generally, we can consider decoding complexity given relatively low error weight. For real ρ, this gives the *Relatively Near Codeword Problem* $\mathrm{RNC}^{(\rho)}$:

Given a generator matrix $\mathbf{A} \in \mathbb{F}_q^{k\times n}$ of a linear code $\mathcal{A}$ of minimum distance d, an integer t with the promise that $t < \rho \cdot d$, and a received word $\mathbf{x} \in \mathbb{F}_q^n$, find a codeword within distance t from $\mathbf{x}$. (The algorithm may fail if the promise is violated, or if no such codeword exists.)

In particular, $\rho = 1/2$ in the "Bounded distance decoding problem". Till recently, not much was known about $\mathrm{RNC}^{(\rho)}$ for constants $\rho < \infty$, let alone $\rho = 1/2$. Now we show that $\mathrm{RNC}^{(\rho)}$ is NP-hard (under random reductions) for every $\rho > 1/2$. This result brings us closer to an eventual (negative?) resolution of the bounded distance decoding problem.

We also show that the minimum distance is hard to *approximate within any constant factor*, unless NP = RP (i.e., every problem in NP has a polynomial time probabilistic algorithm that always rejects No instances and accepts Yes instances with high probability). In our work, we adapt the proofs of results for integer lattices obtained in [2] and [4], by using linear codes that surpass random codes.

II. Approximation Problems

A *promise* problem is a generalization of decision problem when some strings are not required to be either a Yes or a No instance. However, given a string with the promise that it is either a Yes or No instance, one has to decide which of the two sets it belongs to. Below we use $\mathbf{A} \in \mathbb{F}_q^{k\times n}$, $\mathbf{v} \in \mathbb{F}_q^n$, and $t \in \mathbb{Z}^+$. Also, q is a prime power, $\gamma \geq 1$, and $\rho > 0$.

Definition 1 (Minimum Distance Problem)
An instance of $\mathrm{GapDist}_{\gamma,q}$ *is a pair* $(\mathbf{A}, d)$, *such that:*
$(\mathbf{A}, d)$ *is a* Yes *instance if* $\mathrm{d}(\mathcal{A}) \leq d$;
$(\mathbf{A}, d)$ *is a* No *instance if* $\mathrm{d}(\mathcal{A}) > \gamma \cdot d$.

Definition 2 (Nearest Codeword Problem)
An instance of $\mathrm{GapNCP}_{\gamma,q}$ *is a triple* $(\mathbf{A}, \mathbf{v}, t)$, *such that:*
$(\mathbf{A}, \mathbf{v}, t)$ *is a* Yes *instance if* $\mathrm{d}(\mathbf{v}, \mathcal{A}) \leq t$;
$(\mathbf{A}, \mathbf{v}, t)$ *is a* No *instance if* $\mathrm{d}(\mathbf{v}, \mathcal{A}) > \gamma \cdot t$.

Definition 3 (Relatively Near Codeword Problem)
An instance of $\mathrm{GapRNC}^{(\rho)}_{\gamma,q}$ *is a triple* $(\mathbf{A}, \mathbf{v}, t)$, *such that:*
$t < \rho \cdot \mathrm{d}(\mathcal{A})$;
$(\mathbf{A}, \mathbf{v}, t)$ *is a* Yes *instance if* $\mathrm{d}(\mathbf{v}, \mathcal{A}) \leq t$;
$(\mathbf{A}, \mathbf{v}, t)$ *is a* No *instance if* $\mathrm{d}(\mathbf{v}, \mathcal{A}) > \gamma t$.

Our reduction uses the promise problem $\mathrm{GapNCP}_{\gamma,q}$ that is proved to be NP-hard [1] for every constant $\gamma \geq 1$. It is also hard [1] to approximate $\mathrm{d}(\mathbf{v}, \mathcal{A})$ to within a factor of $2^{\log^{(1-\epsilon)} n}$ for any $\epsilon > 0$, unless NP $\subseteq$ QP (deterministic quasi-polynomial time).

We also use polynomial *reverse unfaithful random* reductions (RUR-reductions). Given a security parameter s, these probabilistic algorithms require $\mathrm{poly}(s)$ time to *necessarily* map No instances to No instances and Yes instances to Yes instances *with high probability* $1 - q^{-s}$.

Theorem 4 *For any* $\rho > 1/2$, $\gamma \geq 1$ *and any finite field* $\mathbb{F}_q$:
$\mathrm{GapRNC}^{(\rho)}_{\gamma,q}$ *is* NP*-hard under polynomial RUR-reductions;*
$\mathrm{GapDist}_{\gamma,q}$ *is* NP*-hard under polynomial RUR-reductions;*
$\mathrm{GapDist}_{\gamma,q}$ *is* NP*-hard under quasi-polynomial RUR-reductions for* $\gamma(n) = 2^{\log^{(1-\epsilon)} n}$.

For further details, see [6].

References

[1] S. Arora, L. Babai, J. Stern, Z. Sweedyk, "The Hardness of Approximate Optima in Lattices, Codes, and Systems of Linear Equations", *J. of Comp. and System Sci.*, Vol. 54, 1997, pp. 317–331.

[2] M. Ajtai, "The Shortest Vector Problem is NP-Hard for Randomized Reductions", *Proc. 30th Symposium on Theory of Computing*, 1998, pp. 10–19.

[3] E.R. Berlekamp, R.J. McEliece, H.C.A. van Tilborg, "On the Inherent Intractability of Certain Coding Problems", *IEEE Trans. Inform. Theory*, Vol. 24, 1978, pp. 384–386.

[4] D. Micciancio, "The Shortest Vector in a Lattice is Hard to Approximate to within Some Constant", in *Proc. 39th Symp. Foundations of Comp. Sci.* 1998, pp. 92–98.

[5] A. Vardy, "The Intractability of Computing the Minimum Distance of a Code," *IEEE Trans. Inform. Theory*, Vol. 43, 1997, pp. 1757–1766.

[6] I. Dumer, D. Micciancio, M. Sudan, "Hardness of approximating the minimum distance of a linear code," ECCC Technical Report TR99-029 (available from `http:\\www.eccc.uni-trier.de/eccc`), 1999.

[1]This work was supported by the NSF grant NCR-9703844.
[2]This work was supported by a Sloan Foundation Fellowship, an MIT-NEC Research Initiation Grant and NSF Career Award CCR-9875511.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On the Minimum Distance of some Quadratic-Residue Codes

Markus Grassl
Institut für Algorithmen und Kognitive Systeme (IAKS)
Am Fasanengarten 5, 76 128 Karlsruhe, Germany
e-mail: grassl@ira.uka.de

Abstract — **An updated table of parameters for binary and ternary quadratic-residue codes of length up to 200 resp. 100 is presented. In particular, we find that the minimum distance of the binary $[167, 83]$ quadratic-residue code is 24.**

I. Preliminaries

More than twenty years ago, MacWilliams and Sloane posed the computation of the minimum distance of binary and ternary quadratic-residue (QR) codes as a research problem (Research Problem (16.1) in [1]). Some of the missing minimum distances were presented in [2]. The increase of computing power in the last decades made it possible to find the minimum distances of the $[137, 69]$ binary QR code [3] and the minimum distance of the $[83, 42]$ ternary QR code [4]. The problem was solved by the built-in algorithm of the computer algebra system MAGMA [5]. Using some theoretical results, we were able to determine the minimum distance of the $[167, 83]$ binary QR code and to improve some of the bounds on the minimum distance presented in [1, Fig. 16.1].

II. Quadratic-Residue Codes

Let p and l be prime integers such that l is a quadratic residue modulo p. Furthermore, let Q denote the set of quadratic residues modulo p. Then the polynomial x^p-1 can be factored over $GF(l)$ as $x^p-1 = (x-1)q(x)n(x)$, where the roots of $q(x)$ are α^r for all non-zero quadratic residues $r \in Q$ and α is a primitive p^{th} root of unity in an extension field of $GF(l)$. The quadratic-residue (QR) codes $\mathcal{Q}$, $\overline{\mathcal{Q}}$, $\mathcal{N}$, and $\overline{\mathcal{N}}$ are the cyclic codes of length p over $GF(l)$ generated by $q(x)$, $(x-1)q(x)$, $n(x)$, and $(x-1)n(x)$, resp. The extended quadratic-residue codes $\hat{\mathcal{Q}}$ and $\hat{\mathcal{N}}$ are obtained by adding an overall parity check to $\mathcal{Q}$ and $\mathcal{N}$, resp. A lower bound on the minimum distance d_p of the quadratic-residue code $\mathcal{Q}_p$ of length p is given by $d_p \geq \sqrt{p}$. The minimum distance of the extended code $\hat{\mathcal{Q}}_p$ and of the expurgated code $\overline{\mathcal{Q}}_p$ is $\hat{d}_p = d_p+1$. For $p \equiv 3 \pmod 4$, $\hat{\mathcal{Q}}$ is self-dual. Hence l must be 2 or 3 (see Theorem 1 in [1, Ch. 19, §1]). Then, for $l = 2$, $\hat{\mathcal{Q}}$ is doubly-even, and for $l = 3$, all weights are multiples of 3 (see Theorem 8 in [1, Ch. 16, §4][1]).

III. Results

In Table 1, parameters of binary and ternary extended QR codes of length up to 200 resp. 100 are presented. Differences to the original version [1, Fig. 16.2] are marked and references are given. Here we briefly discuss our results:

For the $[167, 84]$ binary code $\mathcal{Q}_{167}$, the lower bound in [1] is $d_{167} \geq 15$, the upper bound is $d_{167} \leq 23$. As $\hat{\mathcal{Q}}_{167}$ is doubly even, candidates for the minimum distance are 16, 20, and 24. To show that the true minimum is 24, it is sufficient to show $\hat{d}_{167} \geq 21$ resp. $d_{167} \geq 20$. The lower bound $d_{167} \geq 20$ was established using MAGMA V2.5-1 in about 8 days on a SUN Ultra 5 running at 360 MHz.

For the $[192, 96]$ binary code $\hat{\mathcal{Q}}_{191}$, we have enumerated all approx. 2^{40} vectors of information weight $r \leq 9$. The lowest weight encountered was 28, showing $d_{191} \geq 20$ and $\hat{d}_{191} \geq 21$. Again, $\hat{\mathcal{Q}}_{191}$ is doubly even, hence $\hat{d}_{191} = 24$ or $\hat{d}_{191} = 28$. The lower bounds for $\hat{d}_{194}$ and $\hat{d}_{200}$ were obtained similarly.

The only ternary code of [1, Fig 16.2] whose minimum distance remains unknown is $\hat{\mathcal{Q}}_{97}$. Enumeration revealed $21 \leq \hat{d}_{98} \leq 24$. Additionally, we considered the $[108, 54]$ ternary code $\hat{\mathcal{Q}}_{107}$. This code is self-dual, hence $\hat{d}_{107} \equiv 0 \pmod 3$. Enumeration showed $d_{107} \geq 19$, hence $\hat{d}_{107} \geq 21$. The other possible values are 24 and 27.

Tab. 1: Parameters of extended quadratic-residue codes $\hat{\mathcal{Q}}$ (updated version of [1, Fig. 16.2, p. 483]).

(a) Over GF(2)

n	k	d	n	k	d	n	k	d
8	4	4	74	37	14	138	69	22[c]
18	9	6	80	40	16	152	76	20
24	12	8	90	45	18	168	84	24[e]
32	16	8	98	49	16	192	96	24[e]–28
42	21	10	104	52	20	194	97	22[f]–28
48	24	12	114	57	16[a]	200	100	24[g]–32
72	36	12	128	64	20			

(b) Over GF(3)

n	k	d	n	k	d	n	k	d
12	6	6	48	24	15	74	37	18[a]
14	7	6	60	30	18	84	42	20[d]
24	12	9	62	31	12[a]	98	49	21[h]–24
38	19	11[b]	72	36	18[a]	108	54	21[i]–27

New entries: [a]see [2], [b]see [2, 6], [c]see [3], [d]see [4], [e]$d \geq 21$ and doubly-even, [f]$d \geq 22$ and even, [g]$d \geq 22$ and doubly-even, [h]$d \geq 21$, [i]$d \geq 19$ and $d \equiv 0 \pmod 3$

References

[1] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

[2] D. Coppersmith and G. Seroussi, "On the minimum distance of some quadratic residue codes," *IEEE Trans. Inform. Theory*, vol. IT-30, no. 2, pp. 407–411, Mar. 1984.

[3] N. Boston, "The Minimum Distance of the $[137, 69]$ Binary Quadratic Residue Code," *IEEE Trans. Inform. Theory*, vol. IT-45, no. 1, p. 282, Jan. 1999.

[4] D. Kuhlmann, "The Minimum Distance of the $[83, 42]$ Ternary Quadratic Residue Code," *IEEE Trans. Inform. Theory*, vol. IT-45, no. 1, p. 282, Jan. 1999.

[5] W. Bosma, J. J. Cannon, and C. Playoust, "The Magma Algebra System I: The User Language," *Journal of Symbolic Computation*, vol. 24, no. 3–4, pp. 235–266, 1997.

[6] J. C. C. M. Remijn and C. de Vroedt, "The Minimum Distance of the $[38, 19]$ Ternary Extended QR-Code is 11," *IEEE Trans. Inform. Theory*, vol. IT-30, no. 1, pp. 405–407, Jan. 1984.

[1] Note that in Theorem 8 (ii) in [1] no restriction on p is made, but the proof uses Theorem 7 which requires $p \equiv 3 \pmod 4$.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On the probability of undetected error

Iiro Honkala
Department of Mathematics
University of Turku
FIN-20014 Turku, Finland
e-mail: honkala@utu.fi

Tero Laihonen[1]
Department of Mathematics
University of Turku
FIN-20014 Turku, Finland
e-mail: terolai@utu.fi

Abstract — **We show that for a code used for error detection or combined error correction and detection in the binary symmetric channel, the probability of an undetected error can have several local maxima.**

In particular, we construct a code with three local maxima in $(0,1/2)$, a code with five local maxima in $(0,1)$; and a linear code with two local maxima in $(0,1/2)$ and a linear code with three local maxima in $(0,1)$.

I. Introduction

Let t be a given non-negative integer and C a binary (n,M,d) code with $d \geq 2t+1$. Denote by $B_r(\mathbf{x})$ the Hamming sphere of radius r centered at $\mathbf{x}$ and $B_i = 1/M \cdot |\{(\mathbf{a},\mathbf{b}) \in C \times C \mid d(\mathbf{a},\mathbf{b}) = i\}|$. Assume that $\mathbf{x}$ and $\mathbf{y}$ are given, and $d(\mathbf{x},\mathbf{y}) = i$. We denote by $P_i^{(t)}(p)$ the probability that $\mathbf{x}$ changes to a vector in $B_t(\mathbf{y})$ in the binary symmetric channel with transition probability p. The probability of undetected error after using C to correct t or less errors is given by

$$P_{ue}^{(t)}(C,p) = \sum_{i=1}^{n} B_i P_i^{(t)}(p). \tag{1}$$

Kløve and Korzhik [3] give an excellent account of error detecting codes. They have studied a large number of codes, and ask [3, p. 227] whether it is true that for every code (or for every linear code) the function $P_{ue}^{(t)}(C,p)$ has at most one maximum in the interval $(0,1/2)$ and at most two maxima in $[0,1]$. We answer this question in the negative.

II. The approach

When we are only interested in the number of local maxima, we can multiply the polynomial (1) by the constant $M/2$, and instead consider the polynomial

$$Q^{(t)}(C,p) = \sum_{i=1}^{n} q_i P_i^{(t)}(p),$$

where now q_i tells how many of the $\binom{M}{2}$ pairwise distances between the codewords are equal to i. Consequently,

$$\sum_i q_i = \binom{M}{2}. \tag{2}$$

Since the distance between two codewords is even if and only if both of them have even weight or both of them have odd weight, we know that

$$\sum_{i \text{ odd}} q_i = K(M-K), \tag{3}$$

where K denotes the number of codewords of odd weight.

Our approach consists of two steps. We first try to find a polynomial $R(p) = \sum_{i=1}^{n} r_i P_i^{(t)}(p)$ with non-negative integer coefficients which has a prescribed number of local maxima and which satisfies (2) and (3) for some M and K. On the other hand, we have the goal of making M as small as possible.

The second step then consists of constructing a code C such that the $\binom{M}{2}$ pairwise distances between the codewords have the required distribution, i.e., the coefficients q_i of $Q^{(t)}(C,p)$ equal the r_i's. Such a code cannot of course exist unless the required distance distribution satisfies the Delsarte inequalities.

Using this method we are able to construct the following nonlinear and linear codes.

Theorem 1 *Let $t = 0,1$. There exists a code C such that the function $P_{ue}^{(t)}(C,p)$ has three local maxima in the interval $(0,1/2)$ and a code C' such that the function has five maxima in $(0,1)$.*

Theorem 2 *Let $t = 0,1$. There exists a linear code C_l such that the function $P_{ue}^{(t)}(C_l,p)$ has two maxima in $(0,1/2)$ and a code C_l' such that the function has three maxima in $(0,1)$.*

Example 1 We consider now the case $t = 2$. Let us extend twice the [31,5] simplex code. We furthermore take the vector 1111100...0 of length 33 as a codeword to obtain a $(33,33)$ code. The code gives $q_5 = 1$, $q_{13} = 4$, $q_{15} = 16$, $q_{16} = 496$, $q_{17} = 8$ and $q_{21} = 3$ (other q_i's equal zero). This code yields two maxima for $P_{ue}^{(2)}(C,p)$ in $(0,1/2)$. The first one is at $p \approx 0.10$ and the second at $p \approx 0.48$.

References

[1] I. Honkala and T. Laihonen, "The probability of undetected error can have several local maxima," *IEEE Trans. Inform. Theory*, vol. 45, pp. 2537–2539, 1999.

[2] I. Honkala and T. Laihonen, " On the probability of undetected error for binary codes used for combined correction and detection," *J. Discrete Math. Sci. Cryptography*, to appear.

[3] T. Kløve and V. I. Korzhik, *Error Detecting Codes.* Boston, Kluwer, 1995.

[1]This work was supported by the Academy of Finland under grant #46186.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Projective Systems and Higher Weights

Hans Georg Schaathun
Department of Informatics
University of Bergen
Høyteknologisenteret
N-5020 Bergen, Norway
e-mail: georg@ii.uib.no

Abstract — **We use projective multisets (projective systems) to find upper bounds on the weight hierarchies for a special class of codes, namely the extremal non-chain codes. Several code constructions exist meeting the bounds with equality.**

I. Introduction

Let C be a linear q-ary code of dimension k and length n. The weight $w(S)$ of a subcode $S \subseteq C$, is the number of positions where at least one word in S differs from zero. The rth generalised Hamming weight d_r of C is the least weight of an r-dimensional subcode of C. The sequence $(d_1, d_2, \ldots, d_k)$ is called the weight hierarchy of C [6].

II. Extremal Non-Chain Codes

The chain condition was introduced in [7], and states that there is a chain $D_0 \subset \ldots \subset D_k$ of subcodes, where D_i has dimension i and weight d_i.

The opposite extreme are the extremal non-chain codes, defined as follows. For each pair (i,j) where $1 \leq i < j < k$, there are no subcodes $D_i \subseteq D_j$ of dimensions i and j respectively such that $w(D_i) = d_i$ and $w(D_j) = d_j$. The extremal non-chain codes were introduced by Chen and Kløve [1], and this study continues their work.

III. Projective Multisets

Let G be a $k \times n$ generator matrix of C. By permuting columns of G or by multiplying certain columns by non-zero scalars, we get an equivalent code. Equivalent codes have the same weight hierarchy.

Let $\mathsf{PG}(k-1,q)$ be the projective $(k-1)$-space over the finite field with q elements. The code C is determined up to equivalence by giving the map $\gamma : \mathsf{PG}(k-1,q) \to \{0,1,\ldots\}$, saying how many times each projective point occurs as a column in G. Such a map is called a projective multiset [2], a projective system [5], or a value assignment [1, 4]. The definition of γ is extended by $\gamma(S) = \sum_{x \in S} \gamma(x)$ for all $S \subseteq \mathsf{PG}(k-1,q)$. The number $\gamma(S)$ is called the value of S.

We know [3, 5] that a subcode D_r of dimension r and weight w, corresponds to a subspace $S_r \subseteq \mathsf{PG}(k-1,q)$ of dimension $k-r-1$ and value $\gamma(S_r) = n - w$. Hence a subcode D_r of minimum value corresponds to a projective subspace S_r of maximum value. Also if $D_r \subseteq D_{r'}$, then $S_r \supseteq S_{r'}$.

The difference sequence $(\delta_0, \delta_1, \ldots, \delta_{k-1})$ is defined by $\delta_i = d_{k-1} - d_{k-1-i}$. The difference sequence is easily computed from the weight hierarchy and vice versa. If S is an i-space of maximum value, then $\gamma(S) = \delta_0 + \delta_1 + \ldots + \delta_i$. A difference sequence corresponding to an extremal non-chain code is called an ENDS (Extremal Nonchain Difference Sequence).

IV. Results

Theorem 1 (General Bound) *If $(\delta_0, \delta_1, \ldots, \delta_{k-1})$ is an ENDS, $1 \leq m \leq k-2$, then*

$$\delta_m \leq q^m \delta_0 - \frac{q^{m+1}-1}{q-1}.$$

If equality holds for $m = \bar{m}$, then equality holds for all $m < \bar{m}$.

Theorem 2 (Binary Codes) *If $(\delta_0, \delta_1, \ldots, \delta_{k-1})$, $k \geq 4$ is a binary ENDS, then*

$$\delta_{k-2} \leq 2^{k-3}\delta_1 - 2 - 2^{k-3}.$$

Theorem 3 (Total Value) *If $(\delta_0, \delta_1, \ldots, \delta_{k-1})$, $k \geq 3$ is an ENDS, then*

$$\gamma(\mathsf{PG}(k-1,q)) \leq \sum_{i=0}^{m-1} \delta_i + (\delta_m - 1)\frac{q^{k-m}-1}{q-1},$$

for all m such that $1 \leq m \leq k-2$.

Explicit constructions meeting the bounds with equality exist in dimension 5 and less, provided δ_0 is sufficiently large; $\delta_0 \geq 5$ is sufficient in all cases.

Acknowledgments

Most of this work is part of my graduate thesis. I am grateful to prof. Torleiv Kløve for all his help as a superviser in all stages of the work.

References

[1] Wende Chen and Torleiv Kløve. Bounds on the weight hierarchies of extremal non-chain codes of dimension 4. *Applicable Algebra in Engineering, Communication and Computing*, 8:379–386, 1997.

[2] S. Dodunekov and J. Simonis. Codes and projective multisets. *Electron. J. Combin.*, 5(1), 1998. Research Paper 37.

[3] Tor Helleseth, Torleiv Kløve, and Øyvind Ytrehus. Generalized Hamming weights of linear codes. *IEEE Trans. Inform. Theory*, 38(3):1133–1140, 1992.

[4] Hans Georg Schaathun. Upper bounds on weight hierarchies of extremal non-chain codes. Technical Report 171, Department of Informatics, University of Bergen, 1999. Also available at http://www.ii.uib.no/~georg/sci/inf/coding/public/.

[5] Michael A. Tsfasman and Serge G. Vlăduţ. Geometric approach to higher weights. *IEEE Trans. Inform. Theory*, 41(6, part 1):1564–1588, 1995. Special issue on algebraic geometry codes.

[6] Victor K. Wei. Generalized Hamming weights for linear codes. *IEEE Trans. Inform. Theory*, 37(5):1412–1418, 1991.

[7] Victor K. Wei and Kyeongcheol Yang. On the generalized Hamming weights of product codes. *IEEE Trans. Inform. Theory*, 39(5):1709–1713, 1993.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Nonquasicatastrophic Maximum Transition Run Codes

Roy D. Cideciyan and Evangelos Eleftheriou
IBM Research, Zurich Research Laboratory
Säumerstrasse 4, 8803 Rüschlikon
Switzerland

Abstract - **Nonquasicatastrophic maximum transition run (MTR) codes are introduced by defining a new *t*-constraint. Finite state transition diagrams (FSTD) exhaustively characterizing MTR (*j,k,t*) constraints for detector trellises that are unconstrained or incorporate the *j*-constraint are presented and their capacity is computed. It is shown that (*G,I*) constrained systems are a subclass of (*j,k,t*) MTR constrained systems.**

I. Introduction

Consider a recording channel consisting of a modulation encoder, precoder, generalized partial response channel, Viterbi detector, inverse precoder and modulation decoder. Let $\{b_i\} \in B$ denote the input of the modulation encoder, where $b_i \in \{0, 1\}$ and B is the set of all binary sequences. The modulation encoder generates binary sequences $\{x_i\} \in X$ that satisfy a desired constraint, such as a (G,I) constraint or a maximum transition run constraint. The precoder is usually of the form $1/(1 \oplus D)$ or $1/(1 \oplus D^2)$ and its output is denoted by $\{y_i\} \in Y$, where Y denotes the set of all possible channel input sequences.

The class of generalized partial-response channel polynomials of the form $F(D) = (1 - D^2)(1 - P(D))$ is studied, where the whitening filter $1 - P(D)$ has no roots on the unit circle. The Viterbi detector provides an estimate of the channel input sequence $\{\hat{y}_i\} \in \hat{Y}$, where Y is usually a proper subset of $\hat{Y}$. The output sequences of the inverse precoder are denoted by $\{\hat{x}_i\} \in \hat{X}$.

II. Characterization of MTR Constraints

We define the maximum run of accumulated zero-distance as the maximum number of branches associated with two distinct trellis paths that have the same output labels, i.e.,

$$r \triangleq \max \{ n : \sum_{i=1}^{n} \varepsilon_i^2 = 0 \}, \qquad (1)$$

where $\{\varepsilon_i\}$ is the channel-output error sequence with D-transform $\varepsilon(D) = (y(D) - \hat{y}(D))F(D)$. Clearly, the sequence detector suffers from quasicatastrophic error propagation [1] if $r = \infty$.

It can be verified that traditional MTR(*j,k*) codes [2] do not avoid quasicatastrophic error propagation in sequence detectors for generalized partial-response channels that have spectral nulls both at dc and the Nyquist frequency, i.e., $r = \infty$. A new constraint is thus necessary to ensure that MTR codes are nonquasicatastrophic. We say that the output sequence $\{x_i\}$ of an encoder satisfies a "twins" constraint, or *t*-constraint, if it does not allow t+1 consecutive pairs of 0's or 1's ("twins") that are the complement of an allowable string $\hat{x}_i, \hat{x}_{i+1}, \ldots, \hat{x}_{i+2t+1}$ at the inverse precoder output. The *t*-constraint can be characterized by a finite set of forbidden strings and is therefore a shift of finite type. A special case of the twins constraint was introduced in [3]. Traditional MTR codes that also satisfy a twins constraint are referred to as MTR(*j,k,t*) codes. It can be shown that for the new class of MTR(*j,k,t*) codes it holds that $r = \max(j + 1, k + 1, 2t + 3) - L$. Hence, MTR(*j,k,t*) codes are nonquasicatastrophic if and only if j, k, and t are finite.

Let $P_c(G, I)$ be the set of all allowable sequences at the output of a $1/(1 \oplus D^2)$ precoder following a (G,I) modulation encoder. Similarly, let $M(j,k,t)$ and $M_c(j,k,t)$ be the sets of all allowable sequences at the $1/(1 \oplus D)$ precoder input and output, respectively, where the MTR constrained system corresponds to the case of an unconstrained detector trellis, i.e., $\hat{X} = \hat{Y} = B$.

Proposition 1 $\quad P_c(G, I) = M_c(j = G + 1, k = G + 1, t = I)$

The above proposition states that (G,I) constraints are a subclass of the (j,k,t) MTR constraints.

For channels with memory $L \geq j + 1$ the *j*-constraint can readily be incorporated into the detector trellis to reduce the number of states and/or branches, and to increase the capacity of the constrained system $M(j,k,t)$ by adding new potential code sequences that were not allowed before. The new expanded constrained system is denoted by $M'(j,k,t)$,where the prime indicates that the generalized partial-response detector trellis is *j*-constrained. For j=2 and j=3, FSTDs have been constructed by tracking the run length of all four phases of the patterns (0011) arriving at a state. Tables 1 and 2 list the capacity of MTR constraints $M'(j,k,t)$ for j=2 and 3 by truncating the numbers after the fourth digit following the decimal point.

References

[1] G. D. Forney and A. R. Calderbank, "Coset codes for partial-response channels; or, coset codes with spectral nulls," *IEEE Trans. Inform. Theory*, vol. 35, pp. 925-943, Sept. 1989.

[2] J. Moon and B. Brickner, "Maximum transition run codes for data storage systems," *IEEE Trans. Magn.*, vol. 32, pp. 3992-3994, Sept. 1996.

[3] W. G. Bliss, "An 8/9 rate time-varying trellis code for high density magnetic recording," *IEEE Trans. Magn.*, vol. 33, pp. 2746-2748, Sept. 1997.

TABLE 1. Capacity of MTR constraints $M'(j = 2, k, t)$

	k							
t	2	3	4	5	6	7	8	9
1	0.5514	0.6370	0.6819	0.7057	0.7189	0.7263	0.7305	0.7330
2	0.6508	0.7472	0.7888	0.8090	0.8193	0.8248	0.8278	0.8294
3	0.6792	0.7819	0.8264	0.8475	0.8581	0.8636	0.8664	0.8680
4	0.6887	0.7900	0.8334	0.8538	0.8641	0.8694	0.8722	0.8737
5	0.6922	0.7933	0.8365	0.8569	0.8671	0.8724	0.8751	0.8766
6	0.6934	0.7941	0.8372	0.8575	0.8671	0.8728	0.8756	0.8771
7	0.6939	0.7945	0.8375	0.8578	0.8679	0.8731	0.8759	0.8773
8	0.6941	0.7946	0.8375	0.8578	0.8679	0.8732	0.8759	0.8774

TABLE 2. Capacity of MTR constraints $M'(j = 3, k, t)$

	k							
t	2	3	4	5	6	7	8	9
1	0.6370	0.6942	0.7266	0.7444	0.7544	0.7599	0.7631	0.7650
2	0.7472	0.8345	0.8707	0.8876	0.8960	0.9002	0.9024	0.9036
3	0.7819	0.8670	0.9034	0.9203	0.9285	0.9326	0.9346	0.9357
4	0.7900	0.8756	0.9115	0.9280	0.9359	0.9399	0.9419	0.9429
5	0.7933	0.8781	0.9137	0.9301	0.9380	0.9419	0.9439	0.9450
6	0.7941	0.8788	0.9143	0.9306	0.9385	0.9425	0.9444	0.9455
7	0.7945	0.8790	0.9145	0.9308	0.9387	0.9426	0.9446	0.9456
8	0.7946	0.8791	0.9145	0.9308	0.9387	0.9426	0.9446	0.9456

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Simple Soft-Output Detection for Magnetic Recording Channels

Emina Soljanin
Bell Labs, Lucent Technologies
Murray Hill, NJ 07974, USA
e-mail: emina@lucent.com

Abstract — **Recent success of turbo-like coding schemes on memoryless channels has sparked interest in using them on intersymbol-interference (ISI) channels. Decoders for turbo and low density parity check (LDPC) codes perform much better with soft input information which has to be supplied by the channel detector as its soft output. We consider a class of ISI channels commonly used to model magnetic recording channels in a wide range of linear recording densities, and show that simple soft output detectors are possible, since the channel transfer functions belong to a family of special polynomials.**

I. Introduction

Let $\{x_n\}$, $x_n \in \mathsf{GF}(2)$, be the possibly coded user data sequence. We consider a discrete-time model for the magnetic recording channel with input $\{a_n\}$, $a_n = 2x_n - 1$, impulse response $\{h_n\}$, and output $\{y_n\}$ given by

$$y_n = \sum_m a_{n-m} h_m + \eta_n, \qquad (1)$$

where η_n are independent, zero-mean, Gaussian random variables. We separately consider the PR4 channel with the transfer function $\boldsymbol{h}(D) = \sum_n h_n D^n = 1 - D^2$, and *higher order* partial response (PR) channels with $\boldsymbol{h}(D) = (1-D)(1+D)^N$, $N \geq 2$.

The optimal receiver for magnetic recording channel model performs maximum likelihood sequence estimation (MLSE) *i.e.*, it determines an $\{\hat{a}_n\}$ satisfying

$$\min_{\{a_n\} \in \mathcal{C}} \Omega(\{a_n\}) = \Omega(\{\hat{a}_n\}),$$

where $\Omega(\{a_n\})$ is the well known log-likelihood function for channels with inter-symbol interference:

$$\Omega(\{a_n\}) = \sum_n \Big(y_n - \sum_m a_m h_{n-m}\Big)^2. \qquad (2)$$

A general soft-output sequence estimation was introduced in [1], and it is of course possible to get information on symbol reliabilities by using techniques presented there. However, the transfer functions of magnetic recording channels belong to a family of special polynomials. We exploit that fact to derive simple soft output detectors for these channels. We propose two types of soft output channel detectors: one based on a sequence detector for the PR4 channel, the other based on a symbol-by-symbol detector enabled by special precoding for higher order PR channels.

II. The PR4 Channel

The maximum likelihood sequence detector for the $1 - D^2$ channel is realized by two interleaved Viterbi detectors corresponding to the two constituent $1 - D$ channels whose log-likelihood function is given by

$$\Omega(\{a_n\}) = \sum_k \big[y_k - (a_k - a_{k-1})\big]^2.$$

Common implementations of the MLSE use the recursive *difference metric algorithm* of [2]. It was recognized in [2] that the decision about extensions to both states at time n can be made based on single variable

$$\delta_n = \Delta J_{n-1} - y_n, \quad \text{where } \Delta J_n = [J_n(1) - J_n(-1)]/2$$

and $J_n(s)$ is the minimum cost up to time n and state s, $s \in \{-1, 1\}$:

$$J_n(s) = \min_{\{a_n\} \in \mathcal{C}} \sum_{k=-\infty, a_n = s}^{n} [(a_k - a_{k-1}) y_k + a_k a_{k-1}].$$

It can be easily shown that the difference in cost of the surviving and discarded extension to state $s \in \{-1, 1\}$ at time n is equal to $|\delta_n + s|$. Therefore, once the most likely symbol at time n, $\hat{a}_n$, is known, the soft information about $\hat{a}_{n-1}$ (its reliability) can be computed as $|\delta_n + \hat{a}_n|$. Under the assumption that either the most likely path or the second best path is the correct path and the assumption that only minimum distance error events are possible, the two most likely paths can differ in a string of consecutive 1s or a string of consecutive -1s. Therefore the possible error event may have originated at any time $k \leq n - 1$ such that $\hat{a}_k = \hat{a}_{k+1} = \cdots = \hat{a}_{n-1}$. All these symbols are assigned the reliability of $\hat{a}_{n-1}$.

III. Higher Order PR Channels

Let $\{w_n\}$, $w_n \in \mathsf{GF}(2)$, be a sequence obtained from $\{x_n\}$ by special processing known as *precoding*, and $\{a_n\}$ the channel sequence in (1) obtained from $\{w_n\}$ as $a_n = 2w_n - 1$. For channel with the transfer function $\boldsymbol{h}(D) = (1 - D)(1 + D)^N$, we choose the precoder transfer function to be $1/(1 \oplus D)^{N+1}$, as proposed in [3]. This gives

$$W(D) = \frac{1}{(1 \oplus D)^{N+1}} X(D),$$

where $\oplus$ denotes the addition in $GF(2)$. Such precoding gives the following relation between the user data $\{x_n\}$ and the channel noiseless output $r_n = \sum_m a_{n-m} h_m$:

$$x_n = \left| \frac{r_n}{2} \right| \mod 2, \qquad (3)$$

which makes symbol-by-symbol channel detection possible. The soft-output channel detection we propose relays on (3) and some other features of these special ISI channel.

References

[1] J. Hagenauer and P. Hoeher, "A Viterbi algorithm with soft-decision outputs and its applications," *Proc. 1989 IEEE Global Telecommun. Conf. (GLOBECOM '89)*, Dallas, TX, Nov. 1989, pp. 1680–16867.

[2] M. M. Ferguson, "Optimal reception for binary partial-response channels," *Bell Syst. Techn. J., vol. 51*, no. 2, pp. 493–505, Feb. 1972.

[3] B. F. Uchôa Filho and M. A. Herro, "Good Convolutional Codes for the precoded $(1 - D)(1 + D)^N$ partial-response channels," *IEEE Trans. Inform. Theory*, vol. 43, pp. 441-453, Mar. 1997.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Performance Bounds for High Rate Linear Codes over Partial Response Channels

Tolga M. Duman
Electrical Engineering Dept.
Arizona State University
Tempe, AZ 85201-7206, USA
duman@asu.edu

Erozan Kurtas
Seagate Technology
2403 Sidney St.
Pittsburgh, PA 15203-2116, USA
Erozan_M_Kurtas@notes.segate.com

Abstract — **We develop union bounds for high rate linear codes used for partial response equalized channels with additive white Gaussian noise. One particular application of the present setting is the computation of bounds for magnetic recording systems using turbo codes.**

I. Summary

A recent application of turbo codes is in digital magnetic recording [1]. So far, all of the studies on the subject, with the exception of one [2], use Monte Carlo simulation using a sub-optimal decoding algorithm to evaluate the performance of system. There clearly is a need to analyze the system performance from a theoretical perspective. In [2], the authors develop performance bounds for the turbo equalized dicode $(1-D)$ channel assuming maximum likelihood decoding by using the union bounding technique. However, their result cannot be used to predict the performance of a general partial response (PR) equalized magnetic recording channel, such as PR4 or EPR4.

In this paper, we develop the union bound for an arbitrary partial response equalized channel when maximum likelihood decoding is employed. The resulting bound is a generalization of the results of [2], however, our approach is totally different.

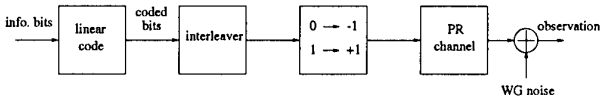


Figure 1: System block diagram.

The block diagram of the system is presented in Figure 1. Consider the transmission of a block of N_u information bits. The information bits are first encoded by a high rate linear code to obtain a coded sequence. The coded sequence is then interleaved, and then may or may not be precoded. The (precoded) bit sequence is then modulated ("1"s are mapped to "+1" and "0"s are mapped to "−1"s) to obtain the channel input. The channel is a partial response channel, which can be described by a certain trellis.

In order to make the derivation of the bounds tractable, we assume that the interleaver is uniform. Furthermore, we assume that for any error event $\boldsymbol{e}$, the squared Euclidean distance between two codewords, $\boldsymbol{b_1}$ and $\boldsymbol{b_2}$ with $\boldsymbol{b_1} \oplus \boldsymbol{b_2} = \boldsymbol{e}$, is approximately equal to the squared Euclidean distance produced when these two codewords are not restricted to lie within the code. This approximation is valid for high-rate linear codes only, and it is the same approximation used in [2] to find performance bounds for the dicode channel.

We assume that $\frac{N_0}{2}$ is the two sided power spectral density of the noise, and we define the signal to noise ratio per information bit as $SNR = \frac{1}{R_c}\frac{E}{N_0}$, where R_c is the underlying code rate, and E is the energy of the PR channel. Let us denote the number of codewords of the underlying code with information weight i and total weight d by $c(i,d)$. We show that

$$P_b \leq 2^{-N} \sum_{i=1}^{N_u} \sum_{d=0}^{N} \sum_{d_E^2} \frac{i}{N_u} c(i,d) \frac{1}{\binom{N}{i}} t(d,d_E^2) Q\left(\sqrt{\frac{d_E^2}{2N_0}}\right)$$

where P_b is the bit error probability, and $t(d,d_E^2)$ is the number of different pairs of sequences with a Hamming distance d and a squared Euclidean distance d_E^2. This quantity can be computed using an extended state diagram of the partial response target which lists the possible squared Euclidean distances and the number of information bit differences between any two pairs of sequences, that is, any two uncoded sequences.

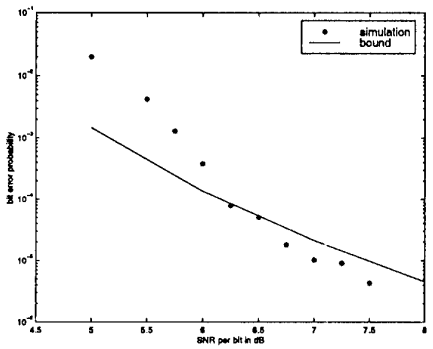


Figure 2: Bound and simulation results for the example.

In Figure 2 we present the union bound for the rate 16/17 $(5,7)$ (in octal notation) convolutional code with an interleaver length of $N = 2048$ for EPR4 $(1 + D - D^2 - D^3)$ channel.

II. Conclusions

We developed the union bound for a high rate linear code used over a partial response equalized additive white Gaussian noise channel. The bound is applicable for a general partial response equalized channel with or without precoding. Therefore, we now have a way of predicting the performance of a coded magnetic recording system, or any other partial response equalized system, with maximum likelihood decoding.

References

[1] W. E. Ryan, "Performance of High Rate Turbo Codes on a PR4 Equalized Magnetic Recording Channel", in *Proceedings of IEEE ICC*, June 1998.

[2] M. Oberg and P. H. Siegel, "Performance Analysis of the Turbo-Equalized Dicode Partial-Response Channel", in *Proceedings of Allerton Conference on Communications, Control and Computing*, Sept. 1998.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Concatenated Runlength Limited Codes with Soft-Decision Decoding

Evelio Martín García Fernández
Departamento de Comunicações
FEEC/UNICAMP
P.O. Box 6101
13083-970 Campinas, SP, Brazil
e-mail:
evelio@decom.fee.unicamp.br

Renato Baldini Filho
Departamento de Comunicações
FEEC/UNICAMP
P.O. Box 6101
13083-970 Campinas, SP, Brazil
e-mail:
baldini@decom.fee.unicamp.br

Abstract — **This paper presents a concatenated coding scheme for error correction in (0, k) constraint channels with hard and soft decision decoding.**

I. Introduction

In magnetic recording systems, constraints on the number of consecutive like symbols sent on the channel are imposed in order to maintain the clock synchronization at the receiver. The use of runlength limited (RLL) sequences have found almost universal application in optical and magnetic disk recording practice [1]. Ref. [2] has shown a method to find combined codes by modifying a known error control code into a runlength limited code. The best codes obtained are of short length because the lower bounds obtained for the k constraint are prohibitively large for long codes. This paper presents a concatenated coding scheme for error correction in channels with (0, k) constraint based on a Reed-Solomon code as an outer code and a runlength limited code obtained by modifying a binary linear transparent block code [2] as an inner code.

II. Code Construction

The inner code C_1 is a (n_1, k_1) modified version of a linear transparent binary block code [2]. The outer code C_2 is a non-binary Reed-Solomon code with symbols of k_1 bits. The encoding process is done in three steps. Firstly, k_2 information symbols are encoded by a conventional Reed-Solomon encoder to form an n_2 coding vector. In the next step, each k_1-binary sequence is encoded into a code vector by C_1. Finally, a modification vector is added to each C_1 codeword to obtain a string of n_2 runlength limited code vectors of C_1. Thus, the resulting code is a (n_1n_2, k_1k_2) binary code. The decoding process may be performed either by hard or soft decision. Hard decision decoding is performed firstly removing the modification vector from each modified C_1 codeword as it arrives at the receiver. Then, a conventional decoder for the C_1 parent code is used to decode the n_1 codewords, producing sequences of k_1 bits. Sequences of n_2 symbols are then decoded by a conventional Reed-Solomon decoder to obtain an estimate of the original message. Soft decision decoding may be performed by using a minimal trellis representation of the inner code. The branch labelling of the trellis must be modified according to the corresponding modification vector [3]. Then, the Viterbi algorithm may be used to decode the inner code. The RLL code is obtained from the method presented in ref. [2]. The runlength constraint of this code is reached by modifying the systematic generator matrix of a binary linear transparent block error control code and then adding a suitable coset leader that provide the best performance in terms of runlength. The modification is made by means of column permutations of the generator matrix of the parent code C_1 to obtain a lower bound for the k constraint. Because of the linearity of the original code, the Hamming distance and the correction capacity of the code are preserved.

III. Results

The proposed scheme is best explained by examples, which are going to be shown in the presentation. Soft decision decoding of the concatenated codes presents a coding gain of about 3dB over hard decision decoding.

IV. Conclusion

This paper presented a construction of a concatenated coding scheme for error correction in channels with (0, k) constraint. The parent binary codes and the bounds for the k constraint may be selected from ref. [2]. Because of transparency, all the code vectors (and any concatenation of them) of the runlength limited-inner code of the scheme satisfy the k constraint. Hence, both the number of "zeros" and the number of "ones" of any encoded sequence are bounded by k without loss in coding rate. The proposed scheme allows to construct long error control codes with the same runlength constraints of a small runlength limited code. The error correction capacity of the inner code may be utilized for correcting random errors. Burst of errors affecting symbols can be corrected by the outer code. Hence, the codes are effective against a mixture of random and burst errors. An increase in the length of the correctable burst can be obtained by interleaving the symbols of the outer Reed-Solomon code.

Acknowledgments

The authors would like to thank the Brazilian Agency FAPESP for supporting this research under grant 97/009266.

References

[1] K. A. S. Immink, "Runlength-limited sequences", *Proc. of the IEEE*, vol. 28, No. 11, pp. 1744–1759, Nov. 1990.

[2] E. M. García F. and R. Baldini F., "A method to find runlength limited block error control codes", *Proc. of ISIT97*, Ulm, Germany, p. 220, 1997.

[3] B. Honary and G. Markarian, *Trellis Decoding of Block Codes: A Practical Approach*, Kluwer Academic Publisher, 1997.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Pruned Convolutional Codes for Flexible Unequal Error Protection Against Insertion/Deletion/Reversal Errors

B. Brink
Department Electrical and Electronic Engineering
Rand Afrikaans University
PO Box 524
Auckland Park, 2006
South Africa
e-mail: brybⓐeng.rau.ac.za

H.C. Ferreira
Department Electrical and Electronic Engineering
Rand Afrikaans University
PO Box 524
Auckland Park, 2006
South Africa
e-mail: hcfⓐing1.rau.ac.za

W.A. Clarke
Department Electrical and Electronic Engineering
Rand Afrikaans University
PO Box 524
Auckland Park, 2006
South Africa
e-mail: waclⓐing1.rau.ac.za

Abstract — **The class of punctured convolutional codes were first constructed by starting with low rate convolutional codes, and by periodically puncturing single bits out of some code symbols in a time varying trellis diagram. Thus, simplified Viterbi decoders could decode the resulting codes, with only two branches entering each state in the trellis diagram [1]. This concept was ingeniously extended in [2], to construct incrementally variable rate codes for unequal error protection. Here we somewhat reverse the above procedure, and name the resulting codes "pruned codes". We now start with optimal high rate convolutional codes, and periodically delete complete code symbols and branches to obtain a time varying trellis diagram. Hence, lower rate codes capable also of correcting insertions and deletions can be constructed.**

I. Pruned Convolutional Codes

The sequences of high rate convolutional codes offer many degrees of freedom for pruning. We show that, by judiciously pruning these codes, lower rate codes can be obtained, capable of correcting insertions/deletions, and also with an increased free distance at the corresponding stages in the trellis diagram, thus making possible unequal error protection.

It should be noted that the pruned codes are subcodes of known good convolutional codes, hence complicating issues such as catastrophic error propagation are avoided. In some of our code constructions, the original punctured code implementation advantage of a simplified Viterbi decoder with only two branches remerging in each state can be retained. This is possible if we start with a high rate base code, which is a punctured convolutional code.

II. Example

Our code construction procedure can perhaps be best explained by an example.

The time varying trellis diagram of a $R = \frac{3}{4}$, $d_{min} = 3$ (i.e. reversal error correction, $t = 1$) punctured convolutional code, with octal generators $5, 7, 5, 7$ from [1], can be depicted with a $R = \frac{1}{n}, \dot{n} = 1, 2$ trellis diagram.

The $R = \frac{3}{4}$ code is selectively pruned to obtain a rate of $R = \frac{1}{4}$. This code now has $d_{min} = 8, t = 3$, and the remaining code symbols represent a single insertion/deletion correcting code (i.e. $s = 1$) since each $n = 4$ bit symbol complies with the condition in [3]:

$$\sum ix_i \equiv a(modm), i = 1 \ldots 4. \quad (1)$$

for some fixed integers a and m, where $m \geq n + 1$. Here $a = 0$ and $m = 5$.

In general, before affecting single insertion/deletion correction with codes complying with (1), the boundaries of the code word need to be known. This can be affected with marker sequences, or more productively with the remaining code symbols forming marker code books [4], which enable the simultaneous transmission of data.

An alternative pruning of the $R = \frac{3}{4}$ code can then be done. The resulting $R = \frac{1}{4}$ code also has $d_{min} = 8$, and $t = 3$. Each pair of code symbols, exiting a state, now form a marker code book from [4]. This alleviates the boundary problem. Furthermore, each pair of $n = 4$ bit symbols also form an $s = 1$ insertion/deletion correcting code, due to the repetition of 3 bits within the symbol.

These flexible codes can be used as building blocks, which can be concatenated in many different ways, to protect sensitive data files, such as multimedia, with unequal error protection against reversal (i.e. additive) errors, or against insertion/deletions during synchronization failures.

It should be noted that there is a trade off. Although the lower rate codes may have a suboptimum d_{min}, the advantage of correcting insertions/deletions is obtained.

References

[1] J. B. Cain, G. C. Clark & J. M. Geist, "Punctured convolutional codes of rate (n-1)/n and simplified maximum likelihood decoding," IEEE Transactions on Information Theory, vol. IT-25, no 1, January 1979, pp 97 - 100.

[2] J. Hagenhauer, "Rate-compatible punctured convolutional codes and their applications," IEEE Transactions on Communications, vol 36, no 4, April 1988, pp 389-400.

[3] V. I. Levenshtein, "Binary codes capable of correcting deletions, insertions and reversals," Sov. Phys - Dokl, vol 10, no 8, February 1966, pp 707-710.

[4] H.C. Ferreria, W. A. Clarke, A. S. J. Helberg, K. A. S. Abdel-Ghaffer & A. J. Vinck, "Insertion/Deletion correction with spectral nulls," IEEE Transactions on Information Theory, vol 43, no 2, March 1997, pp 722-732.

[5] T. Mori & H. Imai, "Viterbi decoding considering synchronization errors," IEICE Trans. Fundamentals, vol E-1, no 1, January 1995, pp 1-6.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Free distance lower bounds for unequal error-protection convolutional codes

Tamar Danon
BreezeCom
Tel-Aviv, ISRAEL
e-mail: tamard@breezecom.co.il

Shraga I. Bross
Dept. of Electrical Engineering
Technion, Haifa 32000, ISRAEL
e-mail:
shraga@ee.technion.ac.il

Abstract — **Convolutional codes with unequal information protection are investigated. Lower bounds on the free distance of time-varying codes are derived and compared to previous bounds. The asymptotic behavior of these bounds leads to the conclusion that significant gains for the important data are attainable by enlarging the corresponding constraint length. This comes at the cost of reduced performance for the less significant data.**

We consider codes with two importance levels wherein each message block is divided into two significance levels : $m = (m_1, m_2)$, $m_i \in \mathcal{M}_i = (GF(2))^{k_i}$ [1]. Consequently, the data portion at the encoder input corresponding to m_1 is represented by a binary k_1-tuple, that corresponding to m_2 is represented by a binary k_2-tuple, and the concatenated binary $k = k_1 + k_2$ vector comprises the encoder input in result to $m = (m_1, m_2)$. Suppose that a block code is used with the encoding function $c : m \rightarrow c(m)$ then the *separation* of the code – $s = (s_1, s_2)$ – is defined as

$$s_i \triangleq \min_{(m,m') \,:\, m_i \neq m'_i} d(c(m), c(m')) \ , \quad i = 1, 2 \ ,$$

where $d(\cdot, \cdot)$ is any metric defined on the set $\{c(m)\}$.

Herein as we deal with convolutional codes the separation definition extends to free distances or active row distances [2] evaluated on output sequences generated while the input sequences are constrained to $m_i \neq m'_i$.

For the class of time varying convolutional codes with period T we seek to answer the following. Given that the encoder input is a binary k-tuple, the code complexity is fixed at $k\nu = k_1\nu_1 + k_2\nu_2$ and the branch length equals N, what is the set of attainable separation vectors.

Let $\mathbf{u}_t, t \in \{-\infty, +\infty\}$, denote the encoder input k-tuple at time t and let $\mathcal{U}_{[t-\nu, t+j+\nu]}$ denote the set of information sequences $\mathbf{u}_{t-\nu}\mathbf{u}_{t-\nu+1} \ldots \mathbf{u}_{t+j+\nu}$ such that the first ν and last ν subblocks (k-tuples) are zero and such that they do not contain $\nu + 1$ consecutive zero subblocks. Further, let S^h denote the set of information sequences $\mathcal{U}_{[t-\nu, t+h+\nu]}, 0 \leq h \leq T$ and let $S^h_{k_1}$ denote the set of information sequences in S^h which differ from the all zero sequence *at least* on the k_1 data section. Furthermore, let $S^h_{k_2}(k_1)$ denote the set of information sequences in S^h which differ from the all zero sequence *only* on the k_2 section while the k_1 section identifies to that of the all zero sequence (alternatively, to the k_1 section of the correct sequence).

Let $F(h, d_1)$ denote the fraction of codes with a nonzero codeword of weight less than d_1 produced by an information sequence from the set $S^h_{k_1}$. Similarly let $F(h, d_2|k_1)$ denote the fraction of codes with a nonzero codeword of weight less than d_2 produced by an information sequence in $S^h_{k_2}(k_1)$. With these definitions we have the following

Lemma 1: A sufficient condition for the existence of a code that has minimum codeword weight not smaller than d_2, and codeword weight of at least d_1 for information sequences differing on k_1, where $d_1 > d_2$ is

$$\sum_{h=1}^{T} \Big[F(h, d_1) + F(h, d_2|k_1) \Big] < 1 \ . \qquad (1)$$

Using this result Costello's [3] technique is extended to the ensemble of unequal error-protection time varying codes.

Lemma 2: Consider the ensemble $\mathcal{E}(k, N, \nu, T)$ of binary, rate $R = (k_1 + k_2)/N$, periodically time-varying convolutional codes encoded by polynomial generator matrices of memory length ν_1 for the k_1 important bits and ν_2 for the k_2 less important bits where $k\nu = k_1\nu_1 + k_2\nu_2$. The fraction of codes whose jth order active row distances $a_j(2)$, $a_j(1)$, $a_j(1) > a_j(2)$, $0 \leq j \leq T$, satisfy respectively
$a_j(2) \leq \hat{a}_j(2) < (j + \nu_2 + 1)N/2$ or
$a_j(1) \leq \hat{a}_j(1) < (j + \nu_1 + 1)N/2$
does not exceed

$$T2^{(j+\nu_1+1)N\left(\frac{j+1}{j+\nu_1+1}R + H\left(\frac{\hat{a}_j(1)}{(j+\nu_1+1)N}\right) - 1\right)}\left(1 - 2^{-(j+1)k_1}\right)$$
$$+ T2^{(j+\nu_2+1)N\left(\frac{j+1}{j+\nu_2+1}R_2 + H\left(\frac{\hat{a}_j(2)}{(j+\nu_2+1)N}\right) - 1\right)} \ ,$$

where $H(\cdot)$ denotes the binary entropy function.

As a corollary to Lemma 2 we derive a lower bound on the corresponding active row distances.

Our main conclusion is that, in the asymptotic case of large ν, non-uniform error protection is feasible by splitting the memory unevenly between m_i.

References

[1] E. K. Englund, "Nonlinear unequal error-protection codes are sometimes better than linear ones," *IEEE Trans. Inform. Theory*, vol. IT-37, No. 5, pp. 1418-1420, September 1991.

[2] S. Host , R. Johannesson , K. Zigangirov and V. Zyablov , "Active distances for convolutional codes," *IEEE Trans. Inform. Theory*, vol. IT-45, pp. 658-669, March 1999.

[3] D. J. Costello, "Free distance bounds for convolutional codes," *IEEE Trans. Inform. Theory*, vol. IT-20, pp. 356-365, May 1974.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Dc-Free Error-Correcting Codes Based on Convolutional Codes

Mao-Ching Chiu[1]
Dept. of Electrical Engineering
National Chi Nan University
Puli, Nantou, Taiwan 545, R.O.C.
e-mail: mcchiu@ncnu.edu.tw

Abstract — **A new construction of dc-free error-correcting codes based on convolutional codes is proposed. The encoder employs a Viterbi algorithm as the codeword selector so that the selected code sequences satisfy the dc constraint. Some important parameters, including the free distance, the running digital sum (RDS), and the sum variance are investigated.**

I. Construction and Free Distance

Our construction of dc-free error-correcting codes can be described by the encoder shown in Figure 1. Codes C_1 and C_2 are (n, k_1) and (n, k_2) binary linear convolutional codes, respectively, with $C_1 \cap C_2 = \{0\}$. The information sequence $a(D)$ is first encoded to a code sequence $x(D)$. The code sequence $x(D)$ is then used by the codeword selector which produces a code sequence $b(D) \in C_2$ so that the final modified sequence $y(D) = x(D) \oplus b(D)$ satisfies the dc constraint. To ensure dc-free transmission, two codeword selection criteria are proposed, the minimum absolute RDS (MRDS) criterion [1] and the minimum squared weight (MSW) criterion [2]. The codeword selector, based on the MRDS or MSW criterion, is implemented by a Viterbi algorithm (VA) with proper metric assignment. To reduce the decoding complexity, a suboptimal decoder is proposed that is implemented by a VA decoder operating over the minimum trellis of the convolutional code $C_{12} = C_1 \oplus C_2$. The free distance d_b of the new constructed code C_b is obviously bounded by $d_b \geq d_{12}$, where d_{12} is the free distance of C_{12}. Define $w[H]$ as the nonzero minimum weight of codewords in $H \subseteq C_{12}$. A tighter bound is given in the following theorem.

Theorem 1 *Let d_b be the free distance of C_b; then $d_b \geq w[C_{12} \backslash C_2]$.*

Define $d_{\text{eff}} = w[C_{12} \backslash C_2]$. For a Viterbi decoder operating on the trellis of C_{12}, d_{eff} is exactly the free distance attained by this suboptimal decoding scheme. A procedure is proposed for determining d_{eff} based on a minimum-weight codeword search over C_{12}.

II. Running Digital Sum and Sum Variance

We present a sufficient condition for the codes to have bounded RDS. Define $D(P)$ as a set of disparities of all binary vector in P. The polynomial generator matrix $G_2(D)$ of C_2 can be expressed as $G_2(D) = G_2^{(0)} \oplus G_2^{(1)} D \oplus \ldots \oplus G_2^{(\alpha)} D^\alpha$. Define the binary generator matrices $G_{2,\tau}$ for $\tau = 1, \ldots, \alpha+1$ as $G_{2,\tau} = [[G_2^{(0)}, \ldots, G_2^{(\tau-1)}]^T, [0, G_2^{(0)}, \ldots, G_2^{(\tau-2)}]^T, \ldots, [0, \ldots, 0, G_2^{(0)}]^T]^T$. Define Σ as the set of all possible states in the trellis of C_2, $\Lambda^{(\tau)}$ as the set of all possible τn-tuple binary outputs from

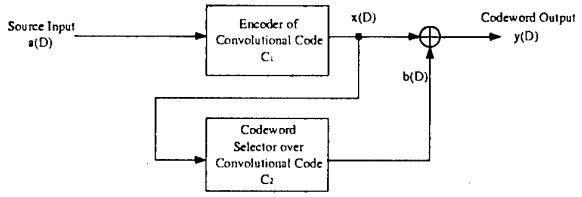


Figure 1: Dc-free encoder.

C_1, and $\beta(\sigma)$ is a τn-tuple binary output of the encoder of C_2 with the initial state σ and with an all-zero input.

Theorem 2 *The RDS of C_b are bounded if there exists some τ, $\tau = 1, 2, \cdots, \alpha+1$, such that, for arbitrary $x \in \Lambda^{(\tau)}$ and $\sigma \in \Sigma$, the set $D(\langle G_{2,\tau} \rangle_b \oplus \beta(\sigma) \oplus x)$ contains opposite polarities or a zero.*

Let t be the smallest integer of τ that satisfies Theorem 2. By a simplified codeword selection algorithm, the sum variance of the new code can be shown to be

$$s^2 = A - B \tag{1}$$

$$A = \frac{1}{n'} \sum_{j=1}^{n'} \sum_{\substack{z \in \Omega \\ \sigma \in \Sigma}} P(Z_m = z, S_m = \sigma) \sum_{x \in \Lambda} P(X_m = x) \left(z + \gamma_j(b_{z,\sigma}(x) \oplus x)\right)^2$$

$$B = \frac{1}{n'} \sum_{j=1}^{n'} \left[\sum_{\substack{z \in \Omega \\ \sigma \in \Sigma}} P(Z_m = z, S_m = \sigma) \sum_{x \in \Lambda} P(X_m = x) \left(z + \gamma_j(b_{z,\sigma}(x) \oplus x)\right)\right]^2,$$

where $n' = tn$, Λ is the set of all the possible outputs of length n' of C_1, $\gamma_j(b_{z,\sigma}(x) \oplus x)$, $j = 1, 2, \ldots, n'$, are the disparities among $b_{z,\sigma}(x) \oplus x$, Ω is the set of all the possible RDS, Σ is the set of all possible states in the trellis of C_2, and $b_{z,\sigma}(x)$ is the n'-tuple binary output of C_2 that corresponds to the path beginning at state (z, σ) and minimizing the absolute value of $z + \gamma_{n'}(b_{z,\sigma}(x) \oplus x)$. The state (Z_m, S_m) can be cast into a Markov chain model and the stationary probabilities $P(Z_m = z, S_m = \sigma)$ can be evaluated by a simple matrix inverse. The results are then substituted into (1) to obtain the sum variance.

[1]This work was supported by the National Science Council of Republic of China under Grant NSC 88-2218-E-260-004.

References

[1] R. H. Deng and M. A. Herro, "DC-free coset codes," *IEEE Trans. Inform. Theory*, vol. 34, pp. 786–792, July 1988.

[2] K. A. S. Immink and L. Pátrovics, "Performance assessment of dc-free multimode codes," *IEEE Trans. Commun.*, vol. 45, pp. 293–299, Mar. 1997.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

DC-Free Binary Convolutional Coding

Tadashi Wadayama
Okayama Prefectural University
wadayama@c.oka-pu.ac.jp

A.J. Han Vinck
Essen University
vinck@exp-math.uni-essen.de

Abstract — **A novel DC-free binary convolutional coding scheme is presented. The proposed scheme achieves DC-free and error correcting capability simultaneously. The scheme has a simple cascaded structure of the RDS(running digital sum) control encoder and the conventional convolutional encoder. The scheme provides wide varieties of reasonable tradeoffs between the coding gain, the RDS constraint, and decoding complexity.**

I. Introduction

The DC-free coding is widely used in digital communication and magnetic/optical recording areas. We here present a DC-free convolutional coding scheme with error correcting capability. Figure 1 illustrates the configuration of the proposed coding scheme. First, the user message sequence is encoded to the *intermediate sequence* by a *RDS control encoder*. The convolutional encoder then converts an intermediate sequence to the coded sequence. After the binary-bipolar conversion, the coded sequence is transmitted to the channel. The scheme

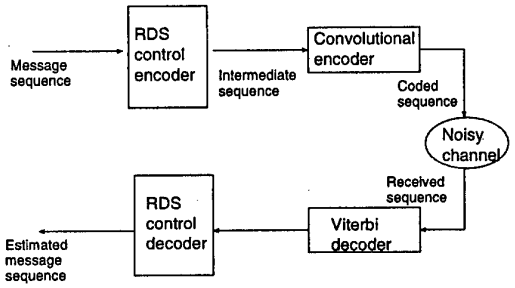


Figure 1: DC-free convolutional coding scheme

is suitable for a power limited noisy channel. Availability of soft decision decoding is one of the major advantages of the proposed scheme. By using the RDS bound which have been derived in this research, we can guarantee that the RDS values obtained from the proposed scheme belong to a certain bounded range. The proposed scheme is based on the following three major ideas: (1)*additive encoding* using a binary linear block code, (2) upper and lower bound on the RDS for an additive encoder, and (3) splitting a convolutional code into infinite sequences of a linear binary block code, which is called a *window code*.

II. Additive encoder

Assume an infinite length binary message sequence $\{\boldsymbol{a}_0, \boldsymbol{a}_1, \ldots\}$. Each vector $\boldsymbol{a}_i (i = 0, 1, 2, \ldots)$ belongs to $F_2^{k_1}$. An additive encoder encodes a message block $\boldsymbol{a}_i$ to $\boldsymbol{c}_i \in C$ for each block index i. The code C is a binary linear code of length n. The resulting sequence $\{\boldsymbol{c}_0, \boldsymbol{c}_1, \ldots\}$ is called a coded sequence. The additive encoder appends redundancy $k_0 = n - k_1$ bits per block and thus the coding rate becomes k_1/n. After the binary-bipolar conversion, the bipolar sequence $\{f(\boldsymbol{c}_0), f(\boldsymbol{c}_1), \ldots\}$ is transmitted over the noisy channel, where f is the binary to bipolar conversion map. For achieving DC-free transmission, the additive encoder has to generate the coded sequence with a RDS constraint. An additive encoder encodes a message block $\boldsymbol{a}_i$ into $\boldsymbol{c}_i$ in such a way:

$$\boldsymbol{c}_i = \boldsymbol{b}_i G_0 \oplus \boldsymbol{a}_i G_1,$$

where $\boldsymbol{b}_i \in F_2^{k_0}$ is selected by the additive encoder according to the value of the RDS and a *selection rule*. The matrices G_0 and G_1 span sub-spaces of C. We call the vector $\boldsymbol{b}_i$ the *control vector*. In other words, the additive encoder has freedom to select a control vector and should specify a control vector so as to obtain a code sequence which keeps the RDS value bounded. In this setting, upper and lower bounds on the RDS for the additive encoder have been derived.

III. DC-free convolutional code

The idea of the additive encoding can be applied to binary convolutional codes. The main idea is to apply the additive encoding method to window codes obtained from a convolutional code. A window code is a binary linear block code obtained by splitting a convolutional code into an infinite series of blocks. Thus, the RDS bound for block codes can be extended to the case of convolutional codes. For a given window code, we need a good decomposition of the window code for achieving a tight RDS constraint. We have performed exhaustive computer searches. Table 1 presents the results for the case where the base convolutional code is rate 1/2 64-state convolutional code with $d_{free} = 10$. For example, a 64-state DC-free coding scheme with the overall rate 6/16 satisfies a bounded RDS condition(from $\mathcal{L} = -18$ to $\mathcal{U} = +18$) and it yields the asymptotic coding gain(ACG) of 5.7 dB. We have performed encoding simulations as well. In Table 1, the results of encoding simulations are also shown.

Table 1: Results on searches and simulations

R	$\mathcal{L}$	$\mathcal{U}$	L	U	ACG(dB)
5/14	−13	+13	−11	+13	5.53
4/14	−8	+8	−6	+8	4.56
3/14	−7	+7	−7	+5	3.31
6/16	−18	+18	−12	+13	5.74
5/16	−9	+9	−7	+9	4.95
4/16	−7	+7	−5	+7	3.98

R:overall coding rate,
$\mathcal{L}$ and $\mathcal{U}$:theoritical lower and upper bounds on RDS
L and U:observed RDS's in encoding simulation
$ACG \triangleq 10\log_{10}(Rd_{free})$

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Improving the Performance of Variable-Length Encoded Systems Through Cooperation Between Source and Channel Decoders

Ahsun H. Murad
COMSAT Laboratories
22300 COMSAT Drive
Clarksburg, MD 20871–9475, USA
email: ahsun.murad@comsat.com

Thomas E. Fuja[1]
University of Notre Dame
Department of Electrical Engineering
Notre Dame, IN 46556, USA
email: tfuja@nd.edu

Abstract — **Systems employing variable-length source codes are prone to error propagation. Several techniques that involve varying levels of cooperation between the channel decoder and source decoder are considered for improving performance. At one extreme, conventional tandem decoding performs channel decoding and source decoding independently; at the other extreme, joint source-channel MAP decoding combines the two into a single decoder. Simulation results indicate that joint source-channel list decoding with "trellis pruning" can result in significant improvement over conventional tandem decoding.**

I. Introduction

Most efficient data communication systems employ source coding (compression) and channel coding (error-control). Variable-length source codes (VLCs, e.g., Huffman codes) and convolutional channel codes are commonly employed in such systems, and the receiver typically uses a tandem decoding scheme – i.e., a maximum-likelihood (ML) Viterbi decoder for the channel code followed by an independent source decoder. When transmitted over a noisy channel, error propagation results if a bit error causes the source decoder to incorrectly interpret a source codeword as a codeword of a different length. While VLCs exhibit an impressive ability to resynchronize, the resulting shift in the decoded sequence (relative to the transmitted sequence) is often considered catastrophic.

II. Methods for Mitigating Error Propagation

Since error propagation is associated with symbol additions/deletions, one approach to limiting propagation is to packetize the data and convey to the decoder the bit-size and symbol-size of each packet. (Typically, one of these would be a (fixed) parameter of the protocol and the other is reliably conveyed to the decoder, e.g., as part of the packet header, protected with a powerful block code.) Several methods for exploiting this *side information* to improve the probability-of-symbol-error performance of the system are discussed below.

Tandem Decoding: The conventional scheme consisting of a channel decoder and a source decoder operating independently *in tandem* is used as the baseline for comparison. The channel decoder performs maximum likelihood (ML) Viterbi decoding, and "tosses" its estimated sequence "over a wall" to the source decoder, which maps it onto the corresponding source-symbol sequence. If too many symbols are generated, the extra ones are discarded; if too few symbols are generated, the sequence is padded.

List Decoding: In list decoding [1], the channel decoder is modified so that, at each decoding stage, the decoder retains the L most likely paths among those paths merging at a given state. After decoding a block, the L best paths among the survivors are selected and provided to the source decoder. The source decoder decodes each of the L sequences and selects from the resulting sequences the most likely path that maps to the correct number of symbols.

[1]Supported in part by NSF grant CCR-99-96222.

Source Decoder Assisted List Decoding: This is a modification of the above list-decoding scheme; with this strategy, the channel decoder is provided with information about the length (in source symbols) of each path through the trellis. The list decoder, when selecting the survivors into a state, selects the L best paths with *distinct symbol lengths*.

Trellis Pruning: Here, the channel decoder is provided at each decoding stage with an indication whether the path has a valid extension with the correct symbol length. Any path with no valid extension is eliminated from consideration.

Hybrid Schemes: List decoding and trellis pruning can be combined in a straight forward manner and result in a further improvement in performance. Combining source-assisted list decoding with trellis pruning is expected to result in further improvement in performance.

Example: Consider a memoryless source with alphabet $\{a, b, c, d, e, f, g, h\}$ and probabilities $\{0.75, 0.15, 0.07, 0.02, 0.007, 0.002, 0.0007, 0.0003\}$. The source code is a Huffman code; the channel code is the convolutional code with generator $G(D) = \left(1 + D^2, 1 + D + D^2\right)$ followed by BPSK modulation. Simulation results illustrating the performances of the above schemes are shown in Figure 1. Increasing cooperation results in improved performance, and list decoding with trellis pruning provides the best performance for this example. Note that increasing the list size from $L = 2$ to $L = 3$ yields only a small improvement.

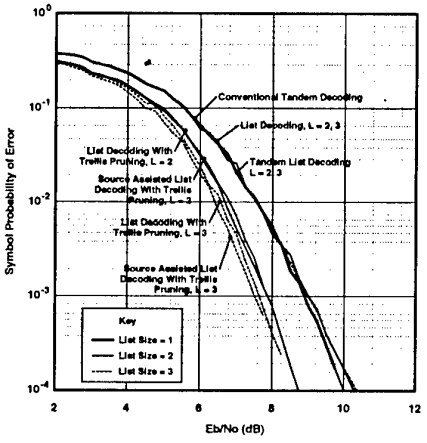


Fig. 1. Performance of various decoding schemes discussed in the text for the system outlined in the example.

References

[1] A. H. Murad and T. E. Fuja, "Joint Source-Channel Decoding of Variable Length Coded Sources," Information Theory Workshop, June 22–26, 1998, Killarney, Ireland.

[2] N. Seshadri and C.-E. Sundberg, "List Viterbi Decoding Algorithms with Applications," *IEEE Transactions on Communications*, vol. 42, no. 2/3/4, pp. 313-323, February/March/April 1994.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Source Optimized Channel Codes (SOCCs) for Parameter Protection

S. Heinen, P. Vary
Institute of Communications Systems and Data Processing (ind)
Aachen University of Technology, Muffeter Weg 3, 52056 Aachen, Germany
e-mail: heinen@ind.rwth-aachen.de, vary@ind.rwth-aachen.de

Abstract — **We present a new class of channel codes, which we call *Source Optimized Channel Codes* (SOCCs). These non-linear codes are designed to maximize a given analogue quality measure in consideration of source and channel statistics.**

I. Introduction

Unlike conventional channel coding which usually minimizes the residual bit or sequence error rate, we design a new class of non-linear block codes which minimizes a given quality measure in the domain of continuous-valued source encoder symbols, e.g. parameters of a speech encoder. These codes are called *Source Optimized Channel Codes* (SOCCs) [1, 2]. At the receiver, we do not exploit the code redundancy for error correction, but for parameter estimation [3]. The performance of SOCCs is compared to that of a reference system which was developed at the Institute for Communications Engineering at Munich University of Technology [6] This reference employs rate compatible convolutional codes [4] for *Unequal Error Protection* (UEP) and *Source Controlled Channel Decoding* (SCCD) [5].

II. Communication Model

By the model shown in Figure 1, we simulate a block-oriented speech transmission. The source encoder is represented by a vector source producing L-dimensional real valued parameter vectors $\mathbf{u} = (u_1, .., u_L)$. To mimic residual inter-frame correlation each component u_i is independently modeled by a Gaussian low-pass source with $\varphi_{u_i u_i}(1) = \rho$. Each vector component is quantized independently. Instead of conventional linear channel encoding as used e.g. in mobile telecommunications, we apply non-linear *Source Optimized Channel Codes* (SOCCs) to encode the quantized parameter vectors $\bar{\mathbf{u}}$ to a binary channel sequence $\mathbf{x}$. At the receiver, parameter estimates $\hat{\mathbf{u}}$ are extracted from the observed soft bit sequence $\hat{\mathbf{y}}$ by *Softbit Source Decoding* (SBSD) [3].

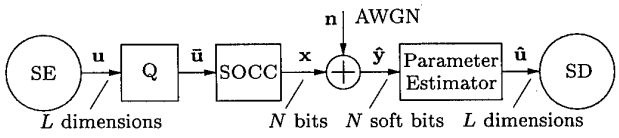


Fig. 1: Communication model
SE: parameter source (model of the source encoder),
Q: quantizer, SD: parameter sink (source decoder)

III. Source Optimized Channel Codes

We assume a given quality measure $\mathcal{D}(\bar{\mathbf{u}}, \hat{\mathbf{u}})$ and a statistical model of the transmission channel $\hat{\mathbf{y}} \mp t(\mathbf{x})$ which is described by $p_{\hat{\mathbf{y}}|\mathbf{x}}(\hat{\mathbf{y}}|\mathbf{x})$. The optimal decoder (estimator) with respect to $\mathcal{D}$ and t is denoted by $\hat{\mathbf{u}} = f_{\mathcal{D},t}(\hat{\mathbf{y}})$. Then we define a SOCC as a set of channel symbols

$$\mathbb{C} = \{\, \mathbf{x} \,|\, \mathbf{x} = \Phi[\bar{\mathbf{u}}],\ \bar{\mathbf{u}} \in \mathbb{U} \,\}\ , \qquad (1)$$

which results from solving the optimization problem

$$\mathbf{E}\,\{\mathcal{D}(\bar{\mathbf{u}}, f_{\mathcal{D},t}(\, t(\Phi[\bar{\mathbf{u}}])\,))\} = \min_{\Phi}\ , \qquad (2)$$

where $\mathbf{E}\{\cdot\}$ denotes expectation. Hence, SOCCs minimize the mean distortion $\mathcal{D}(\bar{\mathbf{u}}, \hat{\mathbf{u}})$ measured between quantized and estimated parameter vectors.

IV. SOCC Performance

Figure 2 depicts a performance comparison between SOCC/SBSD and UEP/SCCD at a transmission rate of 4 bits per vector dimension. Three values of residual inter-frame correlation are considered: $\rho = 0$, 0.75 and 0.9. SOCC/SBSD outperforms UEP/SCCD for all channel conditions if $\rho \geq 0.75$. For $\rho = 0.9$, a gain in parameter SNR of at least 1 dB and up to 3 dB can be observed. In addition, the SOCC/SBSD system exhibits a graceful analogue-type degradation, whereas UEP/SCCD shows the well known threshold effect.

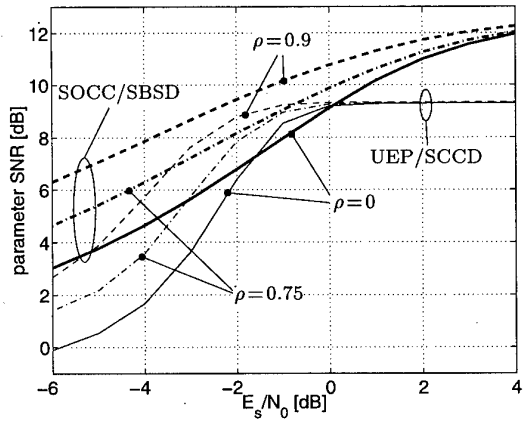


Fig. 2: SOCC/SBSD vs. UEP/SCCD, 4 bits per dim.

References

[1] S. Heinen, S. Bleck, and P. Vary, "Robust Speech Transmission Over Noisy Channels Employing Non-Linear Block Codes," in *Proceedings Speech Coding Workshop 1999*, (Porvoo, Finland), pp. 72–74, IEEE, June 1999.

[2] S. Heinen, T. Hindelang, and P. Vary, "Channel Codes for Softbit Source Decoding: Estimation of Correlated Parameters," in *3rd ITG Conference Source and Channel Coding*, (Munich, Germany), pp. 259–266, Jan. 2000.

[3] T. Fingscheidt and P. Vary, "Robust Speech Decoding: A Universal Approach to Bit Error Concealment," in *Proceedings ICASSP*, vol. 3, pp. 1667–1670, Apr. 1997.

[4] Joachim Hagenauer, "Rate-Compatible Punctured Convolutional Codes (RCPC Codes) and their Applications," *IEEE Trans. Communications*, vol. 36, pp. 389–400, Apr. 1988.

[5] J. Hagenauer, "Source-Controlled Channel Decoding," *IEEE Trans. Communications*, vol. 43, pp. 2449–2457, Sept. 1995.

[6] T. Hindelang, S. Heinen, and J. Hagenauer, "Source Controlled Channel Decoding: Estimation of Correlated Parameters," in *3rd ITG Conference Source and Channel Coding*, (Munich), ITG, Jan. 2000.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Combined Source/Channel (De-)Coding: Can A Priori Information Be Used Twice?

T. Hindelang, T. Fingscheidt, N. Seshadri, R.V. Cox*
AT&T Labs - Research, 180 Park Avenue, Florham Park, NJ 07932, USA
Email: T.Hindelang@ei.tum.de, Tim.Fingscheidt@mch.siemens.de, nambi@broadcom.com, rvc@research.att.com

Abstract — **In digital transmission of speech, audio, images and video signals residual redundancy is often left after source coding due to the complexity and delay constraints. This redundancy remains both inside one block or frame but also in a time correlation of subsequent frames. Both kinds of redundancy are used in an iterative process of source and channel decoding to improve the quality of transmitted parameters. For better understanding, Gaussian distributed and time correlated parameters are used.**

In [1] it is shown that a priori knowledge can be used either in channel or source decoding. In [2] an approach is shown which exploits a priori knowledge in channel and source decoding and an additional correction of the a priori probabilities leads to an improvement in the parameter SNR. Now this approach is extended to iterative source and channel coding.

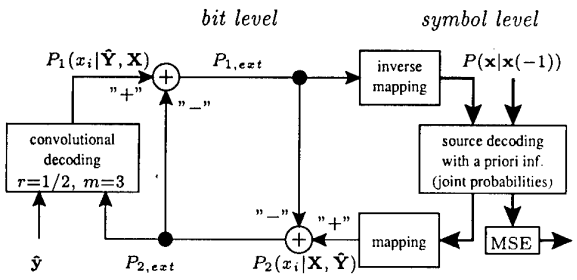


Fig. 1: Block diagram of iterative source/channel decoding.

In the following Fig. 1 is explained by an example. A Gaussian distributed parameter with time correlation $\rho = 0.8$ is Lloyd-Max quantized with 8 levels and these levels are assigned to 3 bits x_i with folded binary mapping. 20 parameters are then placed within one frame. They are not correlated to each other but in time from frame to frame. The interleaver orders the 20 MSBs of the correlated parameters in the mid of the frame; to the left and the right there are first placed the 20 mid bits (10 each side) and then the LSBs. Finally, 20 bits are put to the beginning and to the end of the block (dummy bits), so that the influence of the definite start and termination of the code can be neglected. This leads to a blocklength of 100 bits which are coded by a rate 1/2, constraint length 4 recursive systematic convolutional code and transmitted over an AWGN channel.

Through this mapping and interleaving a typical "Turbo" decoding system is designed. There, the extrinsic information was introduced. In the same manner we "subtract" (in the log domain) the a priori information $P_{2,ext}$ from $P_1(x_i|\hat{\mathbf{Y}},\mathbf{X})$ after channel decoding and the input into the source decoder $P_{1,ext}$ from its output $P_2(x_i|\mathbf{X},\hat{\mathbf{Y}})$. The capital $\hat{\mathbf{Y}},\mathbf{X}$ denote the dependence of the bit x_i from all channel values and parameters not only in the current frame but also in the previous frames. The channel values $\hat{\mathbf{y}}$ and the probabilities denoting the time correlation $P(\mathbf{x}|\mathbf{x}(-1))$ are the two inputs for the system. The output delivers a mean square estimation for the considered parameters.

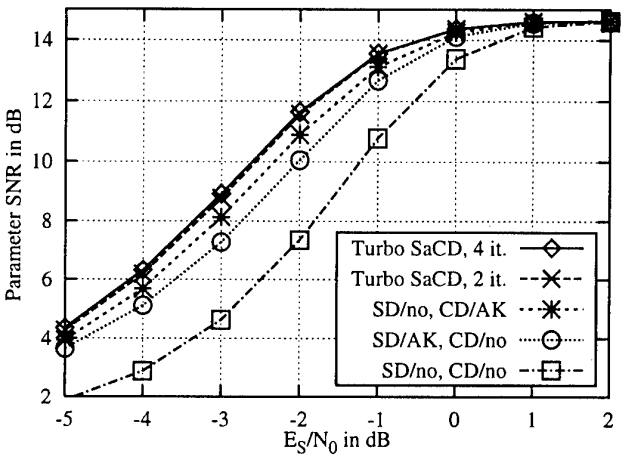


Fig. 2: Combined Source and Channel Decoding (SaCD) using a priori knowledge: Comparison of the iterative approach (4 and 2 iterations), decoding with a priori knowledge (AK) in channel (CD) or source decoding (SD), and neglected AK.

From Fig. 2 the answer to the title question can be seen: "A priori information can be used twice!" There's almost no further gain by doing more iterations. The reason is that in the source decoder we only have three bits denoting one symbol and the correlation of this symbol to the previous one is similar to a very short code. Maybe, the whole system could be improved if there is correlation between parameters within on frame. This approach can be implemented e.g., into a speech transmission standard. With some extension this is done for the ANSI-136 system [3].

References

[1] T. Fingscheidt, T. Hindelang, R. V. Cox, and N. Seshadri, "Combined Source/Channel Decoding: When Minimizing Bit Error Rate is Suboptimal," in *Proc. of 3. ITG Conference "Source and Channel Coding"*, Munich, Germany, Jan. 2000, pp. 273–277, VDE–Verlag.

[2] T. Hindelang, T. Fingscheidt, N. Seshadri, and R.V. Cox, "Combined Source/Channel (De)Coding: Can A Priori Information Be Used Twice?," in *Proc. of ICC'2000*, New Orleans, Lousiana, June 2000.

[3] T. Fingscheidt, T. Hindelang, R.V. Cox, and N. Seshadri, "Joint Source-Channel (De)Coding for Mobile Communications," *submitted to IEEE Trans. on Comm.*, Jan. 2000.

* This work was done while all authors were with AT&T Labs - Research.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Global Broadcast by Broadcasts Among Subsets of Players

Matthias Fitzi[1] Ueli Maurer[1]

Abstract — **In the standard model with only pairwise communication channels, unconditionally secure broadcast among n players is achievable if and only if the number t of corrupted players satisfies $t < \frac{n}{3}$. We show that, when additionally given broadcast among each subset of three players then global broadcast is achievable if $t < \frac{n}{2}$.**

I. Introduction

Given a set $P = \{p_1, \ldots, p_n\}$ of n players, the goal of *broadcast* is to let some distinct player $d \in P$ (called *dealer*) reliably distribute a value to all players in P, i.e., all correct (i.e. uncorrupted) players must receive the same value (*agreement*), and if the dealer is correct then this must be the value the dealer intended to distribute (*validity*).

In this paper we focus on broadcast protocols that are unconditionally secure against an adversary that may actively corrupt up to t of the n players. To actively corrupt a player means to make him deviate from the protocol in an arbitrarily malicious way. Unconditionally secure means that the correctness of the protocol does not rely on any further restriction on the power of the adversary than the threshold t of players he can corrupt during the protocol.

Since the network typically consists only of communication channels among subsets of players and some of the players, especially the dealer, may be corrupted by the adversary, broadcast is a non-trivial problem.

Pease, Shostak, and Lamport [2] proved that, according to the standard communication model of a complete synchronous network of pairwise authentic channels among each pair of players, unconditionally secure broadcast is achievable if and only if $t < \frac{n}{3}$. The communication model considered in this paper extends this standard model by a synchronous network of authentic broadcast for each subset $S \subseteq P$ of the players of cardinality $|S| = 3$, i.e.,

- for every subset of three players and for any selection of a dealer among them there is a broadcast channel, and
- for every such channel, all involved players are authentic, i.e., every correct player is able to assign a received message to its corresponding broadcast invocation.

A broadcast primitive or protocol for n players that is secure against t corrupted players is called *(n,t)-broadcast.*

II. Results

Theorem 1 *Given $(3,1)$-broadcast, $(n, \lfloor \frac{n-1}{2} \rfloor)$-broadcast is achievable for any $n \geq 3$.*

The basic idea is to take some known broadcast protocol (e.g [2]) for some *virtual* player set Q ($|Q| = n'$) in the standard model that tolerates $t' < \frac{n'}{3}$ corrupted players among Q — where, for the moment, n' can be supposed to arbitrary, i.e., not necessarily dependent on k. Instead of letting the virtual players directly participate in the protocol, every virtual player q_i is simulated by some specific collection $S_i \subseteq P$ of the *actual* players (according to player simulation in [1]). If it can be achieved that at most $t' < \frac{n'}{3}$ players q_i are incorrectly simulated then the protocol achieves broadcast among the players in Q (with respect to the players q_j that are correctly simulated). Finally, broadcast among the players in P can then easily be derived from broadcast among the players in Q.

The following proposition immediately follows from [1].

Proposition 1 *A player $q_i \in Q$ of any protocol among a player set Q can be simulated correctly by a collection of players S if broadcast among the players in S is possible and less than $\frac{|S|}{2}$ players in S are corrupted.*

Proof of Theorem 1: The proof of this theorem is based on a recursive construction that, for any $k > 0$, allows to achieve $(2k+3, k+1)$-broadcast from $(2k+1, k)$-broadcast. Finally, $(3,1)$-broadcast can then be used as a base for the recursive construction in order to achieve any $(n, \lfloor \frac{n-1}{2} \rfloor)$-broadcast.

Let P be a set of $2k+3$ players and assume $(2k+1, k)$-broadcast to be achievable among any $S \subset P$ with $|S| = 2k+1$. We define a set Q of $n' = \binom{2k+3}{2k+1}$ virtual players and involve them in some standard broadcast protocol that tolerates $t' < \frac{n'}{3}$ player corruptions. We now let every possible collection $S \subset P$ of $|S| = 2k+1$ players from P simulate exactly one player $q_i \in Q$. Such a player q_i is simulated correctly if at least $k+1$ of the simulating players are correct themselves (since $k+1$ constitutes a majority and hence broadcast among S works correctly and hence Proposition 1 applies), i.e., at least $k+1$ of the simulating players in S must be corrupted by the adversary in order to corrupt the corresponding virtual player. Hence at most $t' \leq \binom{k+1}{k+1}\binom{k+2}{k}$ players of the original protocol can be corrupted which are given by all simulating collections $S \subset P$ of cardinality $|S| = 2k+1$ including at least $k+1$ corrupted players. Since $k > 0$ we get

$$\frac{n'}{t'} = \frac{\binom{2k+3}{2k+1}}{\binom{k+2}{k}} = \frac{2(2k+3)}{k+2} = 4 - \frac{2}{k+2} > 3,$$

and hence strictly less than a third of the players in the original protocol is corrupted. Finally we can let every simulated player send his result to every simulating player who then can compute the outcome of the broadcast by a majority voting on all received values. ∎

References

[1] M. Hirt and U. Maurer, "Complete characterization of adversaries tolerable in secure multi-party computation," *Proc. 16th ACM Symposium on Principles of Distributed Computing (PODC)*, pp. 25–34, Aug. 1997.

[2] M. Pease, R. Shostak, and L. Lamport, "Reaching agreement in the presence of faults," *Journal of the ACM*, 27(2):228–234, Apr. 1980.

[1]Department of Computer Science, ETH Zürich, CH-8092 Zurich, Switzerland. E-mail: {fitzi,maurer}@inf.ethz.ch. Research supported by the Swiss National Science Foundation, SPP project no. 5003-045293.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Performance of a Secure Wireless Transmission Method

Havish Koorapaty
Ericsson Inc.
7001 Development Drive
RTP, NC 27709, USA
e-mail: havish@rtp.ericsson.se

Amer Hassan
Teledesic
1445 120th Ave NE,
Bellevue, WA 98005, USA
e-mail: amer@teledesic.com

Abstract — **A new technique for secure information transmission in a mobile environment using the short term reciprocity of the radio channel was described in [1]. This paper evaluates the performance and security aspects of the technique.**

I. System Model and Algorithm Review

Users $\mathcal{A}$ and $\mathcal{B}$, at least one of them being mobile, must communicate in a secure manner in the presence of an adversary $\mathcal{E}$ on a common wireless medium. Assuming that $\mathcal{B}$ is transmitting information to $\mathcal{A}$, the communication is achieved in two steps. The first step involves a transmission of M sinusoids at frequencies $f_1, f_2, \ldots, f_M$ with equal phases and equal energies from user $\mathcal{A}$ to user $\mathcal{B}$. The signal transmitted by $\mathcal{A}$ in the k^{th} signaling interval $(kT, (k+1)T]$ is given by $s_{\mathcal{A}}(t) = \sum_{i=1}^{M} \sqrt{\frac{2E}{T}} \cos(2\pi f_i t + \phi)$. The mobile channel is a time-varying fading channel with additive white Gaussian noise. The sinusoids $cos(2\pi f_i t)$ are separated by at least the coherence bandwidth of the channel. The receiver differentially estimates the $(M-1)$ received phase differences $(\Theta_2(k) - \Theta_1(k)), \ldots, (\Theta_M(k) - \Theta_1(k))$ between the various sinusoids. Now, $\mathcal{B}$ has probed the response of the channel to the transmission of these multiple sinusoids. In the next step, the knowledge of this response is used by user $\mathcal{B}$ to transmit information to user $\mathcal{A}$. This is done by transmitting a signal consisting of sinusoids of the same frequencies but with the phases of each of the sinusoids modified so as to control the phase differences received by user $\mathcal{A}$ to fall within one of R decision regions depending on the information symbols to be transmitted. The signal transmitted by $\mathcal{B}$ is given by $s_{\mathcal{B}}(t) = \sum_{i=1}^{M} \sqrt{\frac{2E}{T}} \cos(2\pi f_i t - (\Theta_i - \Theta_1) + \Psi_i)$, $\Psi_1 = 0$, $\Psi_i \in \{-\pi, -\pi + 2\pi/R, \ldots, -\pi + 2(R-1)\pi/R\}$, $i \in \{2 \ldots M\}$, where $\Theta_i - \Theta_1$ are the phase differences detected from $\mathcal{A}$'s transmission, and Ψ_i is determined by the information to be transmitted and the mapping between each decoding region and the information bits. The signal that is received by $\mathcal{A}$ is now given by $r_{\mathcal{A}}(t) = \sum_{i=1}^{M} \sqrt{\frac{2E}{T}} \cos(2\pi f_i t + \Psi_i) + n(t)$, $\Psi_1 = 0, \Psi_i \in \{-\pi, -\pi + 2\pi/R, \ldots, -\pi + 2(R-1)\pi/R\}$, $i \in \{2..M\}$. User $\mathcal{A}$ detects the $M-1$ phase differences, $(\Theta_i - \Theta_1) = \Psi_i$, $i = 2..M$, and for each phase difference it decodes the corresponding information symbols.

II. Performance and Security

A symbol error is made on reception by $\mathcal{A}$ if the total phase error $\Phi_e = \Phi_e^B + \Phi_e^A$ due to the phase errors Φ_e^B at $\mathcal{B}$ and the phase error Φ_e^A at $\mathcal{A}$ forces the i^{th} phase difference at $\mathcal{A}$ to fall within a region other than the desired region. It can be shown that the conditional probability density function of Φ_e^B and Φ_e^A is given by $p_\Phi(\phi|\Gamma) = \frac{1}{2\pi} \exp\{-\Gamma\} + \frac{1}{\sqrt{\pi}} \left(\sqrt{\Gamma}\cos\phi\right) \cdot \exp\left\{-\Gamma \sin^2\phi\right\} \left[1 - Q\left(\sqrt{2\Gamma}\cos\phi\right)\right]$, where $\Gamma = \frac{\Lambda_1^2 \Lambda_2^2}{\Lambda_1^2 + \Lambda_2^2} \frac{E}{N_o}$. The probability density function $P_\Gamma(\gamma)$ can be shown to be $P_\Gamma(\gamma) = \int_0^1 \frac{\gamma}{\overline{\gamma}^2} \frac{1}{x^2(1-x)^2} \exp\left\{-\frac{\gamma}{\overline{\gamma}} \frac{1}{x(1-x)}\right\} dx$, where $\overline{\gamma} = 4\sigma^2 E/N_o$ is the average signal to noise ratio. Now, the probability density function of $\Phi_e = \Phi_e^A + \Phi_e^B$ is obtained as $p_{\Phi_e}(\phi) = \int_0^\infty p_{\Phi_e}(\phi|\Gamma) P_\Gamma(\gamma) d\gamma$, where $p_{\Phi_e}(\phi|\Gamma)$ is the convolution of two identical density functions for Φ_e^A and Φ_e^B. Note that this sum can take values in $[-2\pi, 2\pi)$. The probability of symbol error may be obtained from the above density function after resolving the ambiguities of 2π. For $R = 2$, the performance is close to that of differential PSK in a flat Rayleigh fading channel.

The security of the proposed method depends completely on two basic assumptions: the reciprocity assumption and the spatial decorrelation assumption. If the phase differences at the intended users locations and adversary location are statistically independent, then the amount of work required to break the system approaches that of a simple exhaustion of trials of the cryptovariable. To inspire the reciprocity assumption with mobility, consider a mobile with a speed of 100 km/hr and using a carrier in the 900 MHz region; with a delay of 10 μsec, the distance moved by the mobile would be 0.00028 m, which is negligible compared to the wavelength 0.33 m. To motivate the assumption of phase independence, let the distance between the locations of $\mathcal{E}$ and $\mathcal{B}$ be many wavelengths, let Φ^E be $\mathcal{E}$'s estimate of $\Theta_i - \Theta_1$ and define $\Psi \triangleq \Phi^B - \Phi^E$. Then, Ψ is a random variable with a probability density function that is a function of $\alpha^2 = J_0^2(w_D\tau)/(1 + (w_1 - w_2)^2\sigma^2)$, where $J_0(.)$ is the Bessel function of order 0, $w_D\tau$ is the Doppler times delay between the received phases used in computing the phase differences, and σ is a time delay spread parameter that ranges between 1/4 micro-seconds for suburban areas to 5 micro-seconds for urban areas [2]. It was shown in [2] that for $\alpha^2 \leq 0.4$, ψ is almost uniformly distributed. That is, if the bandwidth and time delay between transmissions satisfy $\alpha^2 \leq 0.4$, the phases are independent when $\mathcal{E}$ and $\mathcal{B}$ are separated by many wavelengths. This value of $\alpha^2 = 0.4$ is achieved for $w_1 - w_2 = 240$ kHz, if $w_D = 200$ Hz, $\sigma = 5\mu s$ as is the case for a fast moving mobile terminal. Note that $\tau = 0$ is chosen in this computation since there is no delay between the received phases used in computing the phase differences. To compute the rate at which we may transmit information securely, we compute the value of τ for which $\alpha^2 \leq 0.4$ with the above parameters and with $w_1 - w_2 = 0$ since the phases at the same frequency must be sufficiently de-correlated in time. The rate then is calculated as $(M-1)/\tau$. For the above scenario, with two tones, a rate of 156 bits per second is possible.

References

[1] H. Koorapaty, A. A. Hassan, and S. Chennakeshu, "Secure Information Transmission for Mobile Radio," *Proc. IEEE Intl. Symp. Info. Th..*, 1998.

[2] W. C. Jakes, "Microwave Mobile Communications," *John Wiley and Sons, New York*, 1974.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

A New Identity-based Conference Key Distribution Scheme

Sheng-bo Xu [1]
Philips Components BV
Hurksestraat 19, P.O.Box 218
5600 MD Eindhoven
the Netherlands
E-mail: S.B.Xu@philips.com

Henk van Tilborg
Dept. of Math. & Comp. Sci.
TUE, P.O. Box 513
5600 MB Eindhoven
the Netherlands
E-mail: henkvt@win.tue.nl

Abstract — **A new identity-based conference key distribution scheme is presented using Harn-Yang's identity-based digital signature scheme.**

I. Introduction

In 1993, Harn and Yang proposed ID-based cryptographic schemes for user identification, digital signature, and key distribution [1]. Here we extend their key distribution scheme to a conference key distribution scheme using Harn-Yang's identity-based digital signature scheme.

II. New identity-based conference key distribution scheme

The new scheme consists of three phases: the initiation phase, the user registration phase, and the application phase.

Initiation phase: The key authentication center (KAC) selects a one-way function f, a large prime p, and a primitive element α of GF(p), which are made known to the public. A random number $x \in [1, p-1]$, with $gcd(x, p-1) = 1$, is selected as KAC's secret key. KAC calculates his public key as follows.

$$y = \alpha^x \pmod{p}. \tag{1}$$

User registration phase: When a user, say i, is registering in the KAC, he presents his identity ID_i to the KAC. The KAC computes for user i an extended identity $EID_i = f(ID_i)$ and the signature (r_i, s_i) of EID_i as

$$s_i = (EID_i - k_i r_i)x^{-1} \pmod{p-1} \tag{2}$$

where $r_i = \alpha^{k_i} \pmod{p}$ and k_i is chosen randomly from [1, p-1] such that $gcd(s_i, p-1) = 1$. Note that no k_i should be used repeatly. In the application phase, s_i is user i's secret key and r_i is user i's public key.

Application phase: Suppose all n users have registered in KAC, and they are connected in a star network. Without loss of generality, we assume user 1 is the chairman, and he collects and delivers messages between him and user j $(2 \le j \le n)$. In addition, all n users share a conventional encryption algorithm $E_K(\cdot)$, where K is their shared key.

- User 1 randomly chooses a random number $v_1 \in [1, p-1]$ such that $gcd(v_1, p-1) = 1$. So, there exists v_1^{-1} such that $v_1 v_1^{-1} = 1 \pmod{p-1}$. Then, user 1 calculates

$$\begin{array}{rcll} w_1 & = & y^{v_1} & (mod \quad p) \\ \eta_1 & = & (m - v_1 w_1)s_1^{-1} & (mod \quad p-1) \end{array} \tag{3}$$

  where $m = f(ID_1, time)$. User 1 sends (ID_1, r_1, w_1, η_1) to user j $(2 \le j \le n)$.

- Upon receiving (ID_1, r_1, w_1, η_1), user j checks whether the following congruence holds:

$$y^m = w_1^{w_1}(\alpha^{EID_1} r_1^{-r_1})^{\eta_1} \pmod{p}. \tag{4}$$

  If (4) holds, user j chooses a random number $v_j \in [1, p-1]$ such that $gcd(v_j, p-1) = 1$. So there exists v_j^{-1} such that $v_j v_j^{-1} = 1 \pmod{p-1}$. Then user j computes

$$\begin{array}{rcll} w_j & = & y^{v_j} & (mod \quad p) \\ n_j & = & w_1^{v_j} & (mod \quad p) \\ \eta_j & = & (n_j - v_j w_j)s_j^{-1} & (mod \quad p-1). \end{array} \tag{5}$$

  Next, user j sends $(ID_j, r_j, w_j, n_j, \eta_j)$ to user 1.

- Upon receiving $(ID_j, r_j, w_j, n_j, \eta_j)$, user 1 checks whether the following $(n-1)$ congruences hold:

$$y^{n_j} = w_j^{w_j}(\alpha^{EID_j} r_j^{-r_j})^{\eta_j} \pmod{p}. \tag{6}$$

  If all the congruences hold, user 1 generates a random number $r \in [1, p-1]$ and calculates the conference key Kc as follows.

$$Kc = y^r \pmod{p}. \tag{7}$$

  Also, user 1 computes

$$z_j = n_j^{v_1^{-1} r} \pmod{p}, \tag{8}$$

  and sends $(z_j, E_{Kc}(ID_1))$ to all other users, where $E_{Kc}(ID_1)$ denotes a conventional encryption of ID_1 using Kc.

- User j $(2 \le j \le n)$ computes the conference key

$$Kc = (z_j)^{v_j^{-1}} \pmod{p}, \tag{9}$$

  and verifies it through decryption of $E_{Kc}(ID_1)$.

Through the above scheme, each user can obtain the same conference key Kc. Since the conference key depends on the random number r, Kc will be different from one time to the next.

[1] This work was partially done when the author was visiting Eindhoven University of Technology.

References

[1] L. Harn and S. Yang, "ID-based cryptographic schemes for user identification, digital signature, and key distribution", *IEEE Journal on Selected Areas in Communication*, Vol.11, No.5, June 1993, pp.757-760.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

An Information Theoretic Model for Distributed Key Distribution

Carlo Blundo
Dipartimento di Informatica ed Applicazioni
Università di Salerno
84081 Baronissi (SA), Italy
e-mail: carblu@dia.unisa.it

Paolo D'Arco
Dipartimento di Informatica ed Applicazioni
Università di Salerno
84081 Baronissi (SA), Italy
e-mail: paodar@dia.unisa.it

Abstract — **A Distributed Key Distribution Scheme is a protocol enabling a set of n servers of a network to *jointly* realize a Key Distribution Center, a server which distributes cryptographic keys to users for secure group communications. We model Distributed Key Distribution Schemes within an information theoretic framework showing lower bounds on the size of the information sent and stored by the servers and on the number of random bits needed to set up such schemes. The bounds are tight as there exists a protocol which meets them.**

I. Introduction

Enabling groups of users in a network (*conferences*) to privately communicate using symmetric encryption algorithms requires an efficient protocol to give each conference a key.

Often, in a network, there exists a Key Distribution Center which is responsible of the management of the secret keys. If the center works on-line, then users must sent it requests to obtain the common key. If the center is off-line, then the common keys can be recovered by the conferences using some private information initially distributed by the center. The protocols implemented by the Key Distribution Center are called Key Distribution Schemes (KDSs).

All the previous KDSs, concern with a centralized environment. With a Distributed Key Distribution Scheme (DKDS), the secret keys are distributed between n servers and it can be recovered by a user only if he obtains answers to a *key-request message* sent to k out of the n servers. The distribution avoids the *concentration* of secret information in a single place of the network and increases the *availability* and *security* of the overall system. We are interested in unconditionally secure DKDSs.

II. The Model

Initially, a dealer distributes private information to each server of the network.

- Let $\mathcal{U} = \{1, \ldots, m\}$ be a set of users, let $S_1, \ldots, S_n$ be the servers of the network, and let $\mathcal{C}$ be the family of all conferences of $\mathcal{U}$ that need to communicate securely.
- Let K_h be the set of possible keys κ_h that can be computed by the users in $C_h \in \mathcal{C}$ (let $\mathbf{K}_h$ be the corresponding random variable).
- Let A_i be the set of values that the server S_i can obtain privately from the dealer during the initialization phase.
- Let $Y_{i,j}^h$ be the set of values that can be sent by the server S_i to user $j \in \mathcal{U}$ upon a key-request message for the conference C_h (let $\mathbf{A}_i$ and $\mathbf{Y}_{i,j}^h$ be the corresponding random variables). Let $\mathbf{Y}^s = \mathbf{Y}_{i,j}^1 \ldots \mathbf{Y}_{i,j}^{h-1}, \mathbf{Y}_{i,j}^{h+1} \ldots \mathbf{Y}_{i,j}^s$, for $s \neq h$, for $i = 1, \ldots, n$ and $j \in \mathcal{U}$, and let $\mathbf{Y} = \mathbf{Y}^1, \ldots, \mathbf{Y}^{h-1}, \mathbf{Y}^{h+1}, \ldots, \mathbf{Y}^{|\mathcal{C}|}$.

Definition II.1 *A $(k, n, \mathcal{C})$-DKDS is a protocol which enables each user of $C_h \in \mathcal{C}$ to compute a common key κ_h interacting with at least k of the n servers of the network. More precisely:*

- For each conference $C_h \in \mathcal{C}$, for each user $j \in C_h$, and for each subset of indices $\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, n\}$, it holds that
$$H(\mathbf{K}_h | \mathbf{Y}_{i_1,j}^h, \ldots, \mathbf{Y}_{i_k,j}^h) = 0.$$
- For each conference $C_h \in \mathcal{C}$ and for each subset of indices $\{i_1, \ldots, i_{k-1}\} \subseteq \{1, \ldots, n\}$, it holds that
$$H(\mathbf{K}_h | \mathbf{Y}, \mathbf{A}_{i_1}, \ldots, \mathbf{A}_{i_{k-1}}) = H(\mathbf{K}_h).$$

The first property of the above definition establishes that each user in a conference $C_h \in \mathcal{C}$ can univocally compute the key κ_h, after interacting with at least k servers of his choice. The second property formalizes the security condition. W.l.o.g, we assume that all the entropies on keys are equal, and we denote this common entropy by $H(\mathbf{K})$.

III. Our Results

Theorem III.1 *In a $(k, n, \mathcal{C})$-DKDS, for each $C_h \in \mathcal{C}$, and for $i = 1, \ldots, n$ and $j \in \mathcal{U}$, it holds that $H(\mathbf{Y}_{i,j}^h) \geq H(\mathbf{K})$.*

Theorem III.2 *Let $A_1, \ldots, A_n$ be the private information of $S_1, \ldots, S_n$. Then, $H(\mathbf{A}_i) \geq |\mathcal{C}| H(\mathbf{K})$, for each $i = 1, \ldots, n$.*

Theorem III.3 *Let $A_1, \ldots, A_n$ be the private information of $S_1, \ldots, S_n$. Then, $H(\mathbf{A}_1, \ldots, \mathbf{A}_n) \geq k|\mathcal{C}| H(\mathbf{K})$.*

All the previous bounds are tight. Indeed, using multiple copies of the Shamir's Secret Sharing Scheme [2], we can construct a protocol that meets the bounds. Moreover, also the scheme described in [1] is optimal with respect to the information distributed.

IV. Open Problems

Further researches can be done to model: DKDSs with an initialization performed by a subset of $S_1, \ldots, S_n$; DKDSs secure against coalitions of users *fixed* in size; DKDSs in which user's key-recovering is not based on a threshold structure but on a generic *access structure* on $S_1, \ldots, S_n$.

References

[1] M. Naor, B. Pinkas, and O. Reingold, "Distributed Pseudo-random Functions and KDCs", *Advances in Cryptology: Proceedings of Eurocrypt 99*, Lecture Notes in Computer Science, Vol. 1592, Springer-Verlag, 1999, 327-346.

[2] A. Shamir, "How to Share a Secret", *Communications of ACM*, Vol. 22, No. 11, Nov. 1979, 612-613.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Adaptive Joint Detection and Decoding in Flat-Fading Channels via Mixture Kalman Filtering [1]

Rong Chen
Dept. of Statistics
Texas A&M University
College Station, TX 77843-3128
e-mail: chen@stat.tamu.edu

Xiaodong Wang
Dept. of Electrical Engineering
Texas A&M University
College Station, TX 77843-3128
e-mail: wangx@ee.tamu.edu

Jun S. Liu
Dept. of Statistics
Stanford University
Stanford, CA 94305
email: jliu@stat.stanford.edu

Abstract — **A novel adaptive Bayesian receiver for signal detection in flat-fading channels is developed based on the sequential Monte Carlo methodology. The basic idea is to treat the transmitted signals as missing data and to sequentially impute multiple copies of them based on the observed signals. The imputed signal sequences, together with their importance weights, provide a way to approximate the Bayesian estimate of the transmitted signals and the channel states. It is shown through simulations that the proposed sequential Monte Carlo receivers achieve near-bound performance in fading channels without the aid of any training/pilot symbols or decision feedback. Moreover, the proposed receiver structure exhibits massive parallelism and is ideally suited for high-speed parallel implementation using the VLSI systolic array technology.**

I. System Description

We consider a communication system signaling through a flat-fading channel with additive ambient noise. The transmitted complex data symbol s_t takes values from a finite alphabet set $\mathcal{A} = \{a_1, \cdots, a_{|\mathcal{A}|}\}$. The input-output relationship of the flat-fading channel is described by

$$y_t = \alpha_t s_t + n_t, \qquad t = 0, 1, \cdots, \tag{1}$$

where y_t, α_t, s_t and n_t are the received signal, the fading channel coefficient, the transmitted symbol, and the ambient additive noise at time t, respectively. The processes $\{\alpha_t\}$, $\{s_t\}$, and $\{n_t\}$ are assumed to be mutually independent. It is assumed that the additive noise $\{n_t\}$ is a sequence of independent and identically distributed (i.i.d.) zero-mean complex Gaussian random variables: $n_t \sim \mathcal{N}(0, \sigma^2)$. It is further assumed that the channel-fading process is Rayleigh. That is, the fading coefficients $\{\alpha_t\}$ form a complex Gaussian process that can be modeled by the output of a lowpass Butterworth filter driven by white Gaussian noise. This fading channel can be described by the following state-space model

$$\boldsymbol{x}_t = \boldsymbol{F}\boldsymbol{x}_{t-1} + \boldsymbol{g}u_t, \tag{2}$$

$$y_t = s_t \boldsymbol{h}^H \boldsymbol{x}_t + \sigma v_t, \tag{3}$$

where $\{v_t\}$ in (3) is a white complex Gaussian noise sequence with unit variance and independent real and imaginary components.

[1]This work was supported in part by the Interdisciplinary Research Initiatives Program, Texas A&M University. R. Chen was supported in part by the U.S. National Science Foundation (NSF) under grant DMS-9626113 and grant DMS-9982846. X. Wang was supported in part by the NSF grant CAREER CCR-9875314. J.S. Liu was supported in part by the NSF grant DMS-9803649.

II. The Mixture Kalman Filter Receiver

Denote $\boldsymbol{Y}_t \triangleq (y_0, \cdots, y_t)$ and $\boldsymbol{S}_t \triangleq (s_0, \cdots, s_t)$. Assume that the transmitted symbols are independent and identically distributed uniformly *a priori*. We are interested in estimating the symbol s_t and the channel state $\alpha_t = \boldsymbol{h}^H \boldsymbol{x}_t$ at time t based on the observation $\boldsymbol{Y}_t$. Note that with a given $\boldsymbol{S}_t$, the state-space model (2)-(3) becomes a linear Gaussian system. Hence,

$$p(\boldsymbol{x}_t \mid \boldsymbol{S}_t, \boldsymbol{Y}_t) \sim \mathcal{N}\left(\mu_t(\boldsymbol{S}_t), \boldsymbol{\Sigma}_t(\boldsymbol{S}_t)\right), \tag{4}$$

where the mean $\mu_t(\boldsymbol{S}_t)$ and covariance matrix $\boldsymbol{\Sigma}_t(\boldsymbol{S}_t)$ can be obtained by a Kalman filter with the given $\boldsymbol{S}_t$. The adaptive receiver proposed in this paper is based on a recently proposed filtering method, the mixture Kalman filter (MKF). The basic idea is to obtain a set of Monte Carlo samples of the transmitted symbols, $\{(\boldsymbol{S}_t^{(j)}, w_t^{(j)})\}_{j=1}^m$, properly weighted with respect to the distribution $p(\boldsymbol{S}_t|\boldsymbol{Y}_t)$. Then for any integrable function $h(\boldsymbol{x}_t, s_t)$, we can approximate the quantity of interest $E\{h(\boldsymbol{x}_t, s_t)|\boldsymbol{Y}_t\}$ as follows:

$$\begin{aligned} & E\left\{h(\boldsymbol{x}_t, s_t) \mid \boldsymbol{Y}_t\right\} \\ = & \int \underbrace{\left[\int h(\boldsymbol{x}, s_t)\, \phi\left(\boldsymbol{x}; \mu_t(\boldsymbol{S}_t), \boldsymbol{\Sigma}_t(\boldsymbol{S}_t)\right) \mathrm{d}\boldsymbol{x}\right]}_{\xi(\boldsymbol{S}_t)} p(\boldsymbol{S}_t \mid \boldsymbol{Y}_t) \mathrm{d}\boldsymbol{S}_t \\ \cong & \frac{1}{W_t} \sum_{j=1}^{m} \xi\left(\boldsymbol{S}_t^{(j)}\right) w_t^{(j)}, \end{aligned} \tag{5}$$

where $W_t = \sum_{j=1}^m w_t^{(j)}$; and $\phi(\cdot; \mu, \Sigma)$ denotes a complex Gaussian density function with mean μ and covariance matrix Σ. In particular, *a posteriori* symbol probability can be estimated as

$$P(s_t = a_j) \cong \frac{1}{W_t} \sum_{j=1}^{m} 1(s_t^{(j)} = a_i)\, w_t^{(j)},$$

where $1(\cdot)$ is an indicator function. Denote $\mu_t^{(j)} \triangleq \mu_t(\boldsymbol{S}_t^{(j)})$, $\boldsymbol{\Sigma}_t^{(j)} \triangleq \boldsymbol{\Sigma}_t(\boldsymbol{S}_t^{(j)})$, and $\kappa_t^{(j)} \triangleq [\mu_t^{(j)}, \boldsymbol{\Sigma}_t^{(j)}]$. By exploiting the Markovian nature of the state-space model (2)-(3), we can derive a recursive procedure for generating a set of properly weighted Monte Carlo samples (i.e., $\{(\boldsymbol{S}_t^{(j)}, \kappa_t^{(j)}, w_t^{(j)})\}_{j=1}^m$) at time t, with respect to $p(\boldsymbol{S}_t|\boldsymbol{Y}_t)$, from a set of properly weighted Monte Carlo samples at time $(t-1)$, which leads to an adaptive receiver structure in fading channels based on Monte Carlo filtering. Moreover, if the transmitted symbols are convolutionally coded, then a similar Monte-Carlo-based adaptive receiver can be developed that directly samples the information bits based on the received signal. Simulation results indicate that a sample size of 50 suffices to obtain good receiver performance.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Adaptive Maximum Likelihood Multiuser Detection

Deva K. Borah[1]
Klipsch School of ECE
New Mexico State University
Las Cruces, NM 88003, USA
e-mail: dborah@nmsu.edu

Predrag B. Rapajic
School of EE and Telecomm
The University of New South Wales
Sydney, Australia
e-mail: P.Rapajic@unsw.edu.au

Abstract — **An optimal multiuser detector, in the weighted least squares (WLS) sense, is derived for Code Division Multiple Access (CDMA) and Space Division Multiple Access (SDMA) systems.**

I. Introduction

Optimal detectors, e.g., the maximum likelihood detector with a bank of matched filters (MF-ML) [1], require knowledge of many parameters such as the number of users, their signature sequences, and transmission delays. In this paper, we present an optimal WLS detector that can be implemented adaptively without the knowledge of these parameters. The WLS detector includes the MF-ML detector as a special case and it also optimally suppresses narrow band interference.

II. WLS Structure

Let $y(t)$ be a received CDMA or SDMA signal due to K_T users. Consider the fractionally chip spaced received vector, $\mathbf{y} = \mathbf{S}\mathbf{b} + \mathbf{n}$, where $\mathbf{y} = [y_0, \cdots, y_{N_t-1}]^T$, N_t is the total number of received samples, $y_l = y(lT_{cr})$, $T_{cr} = T_c/r$, T_c is the chip period, and r is chosen to satisfy the Nyquist sampling criterion. The matrix $\mathbf{S}$ equals $[\mathbf{s}_{1,0}, \cdots, \mathbf{s}_{K_T,N_b-1}]$, where $\mathbf{s}_{k,i} = E[b_{k,i}\mathbf{y}]$ is the signature vector for the i-th bit of the k-th user, $b_{k,i}$, and N_b is the total number of bits transmitted by each user. $\mathbf{S}$ also includes the effects of multipath channel. The vector $\mathbf{b}$ equals $[b_{1,0}, \cdots, b_{K_T,N_b-1}]^T$. The covariance matrix of the noise vector $\mathbf{n}$, which may also contain narrow band interference, is $\mathbf{R}_n$. Consider the problem of joint detection of K users, where $K = K_T - K_I$, K_I being the number of unknown CDMA/SDMA interferers. We rewrite $\mathbf{S}\mathbf{b} = \mathbf{S}_D\mathbf{b}_D + \mathbf{S}_U\mathbf{b}_U$, where $\mathbf{b}_D$ contains symbols of the K users and S_D contains the corresponding signature vectors. Similarly, $\mathbf{S}_U$ and $\mathbf{b}_U$ correspond to the K_I users.

Proposition 1 *The output samples of a bank of KN_b minimum mean squared error (MMSE) filters corresponding to each symbol of each of the K users contain a set of sufficient statistics for WLS detection.*

The proof follows from the WLS detection criterion,

$$\hat{\mathbf{b}}_D = \arg\min_{\tilde{\mathbf{b}}_D}(\mathbf{y} - \mathbf{S}_D\tilde{\mathbf{b}}_D)^H\mathbf{R}_U^{-1}(\mathbf{y} - \mathbf{S}_D\tilde{\mathbf{b}}_D)$$

where $\mathbf{R}_U = \mathbf{S}_U\mathbf{S}_U^H + \mathbf{R}_n$. The MMSE filter $\mathbf{p}_{k,i}$ corresponding to $b_{k,i}$ is of the form $\mathbf{p}_{k,i} = \mathbf{R}_U^{-1}\mathbf{s}_{k,i}$.

Corollary 1.1 *If the interfering users' symbols are Gaussian distributed, and $\mathbf{n}$ is Gaussian, then the MMSE filter output samples are also a set of sufficient statistics for ML detection.*

Corollary 1.2 *Only a bank of $K + \sum_{k=1}^{K}(N_k' + (N_b - N_k''))$ MMSE filters is required for generating sufficient statistics, if the MMSE filter corresponding to $b_{k,i}$ is of the form $\mathbf{p}_{k,i} = [\mathbf{0}_{1,\xi}, \mathbf{p}_k^T, \mathbf{0}_{1,\eta}]^T$ for $N_k' \le i < N_k''$, where N_k' and N_k'' are integers, $\xi = l_0 + (i-1)rN$, $\eta = N_t - (rN_f + l_0 + (i-1)rN)$ for some integer l_0, $\mathbf{0}_{m,n}$ is an $m \times n$ zero matrix, and $\mathbf{p}_k$ is a vector of length rN_f. In practice, only K filters are needed.*

Each user repeats its signature sequence for consecutively transmitted symbols. Therefore, instead of considering the whole received vector, a sliding windowed received signal vector $\mathbf{y}(i)$ of length rN_f samples may be considered so that $\mathbf{y}(i) = \mathbf{S}(i)\mathbf{b}(i) + \mathbf{n}(i)$, where the argument i implies that it corresponds to the i-th symbol of all users. This sliding window moves at steps of rN samples, where N is the spreading gain. Then the WLS metric, to be minimized, becomes $\Lambda(\mathbf{b}_D) = \sum_{k=1}^{K}\sum_{i=0}^{N_b-1}[-2\mathrm{Re}[b_{k,i}^*\mathbf{p}_k^H\mathbf{y}(i)] + b_{k,i}^*\mathbf{q}_{dd,k}^H\mathbf{b}_{dd}(i)]$, where $\mathbf{q}_{dd,k}$ represents interference contributions to $\mathbf{y}(i)$, in MMSE sense, from symbols of the K users except $b_{k,i}$ and the vector $\mathbf{b}_{dd}(i)$ contains these symbols. Re[·] denotes real part.

III. Adaptive Implementation

Consider a centralized decision feedback detector, with feedforward filter(FFF) tap vector $\mathbf{w}_{dfe,k}$, and feedback filter (FBF)vector $\mathbf{d}_{dfe,k}$ for the k-th user. We write $\mathbf{S}(i)\mathbf{b}(i) = \mathbf{S}_{ud}(i)\mathbf{b}_{ud}(i) + \mathbf{S}_{dd}(i)\mathbf{b}_{dd}(i)$, where $\mathbf{S}_{dd}(i)$ contains windowed signature vectors corresponding to symbols in $\mathbf{b}_{dd}(i)$, and the remaining signature vectors and symbols are contained in $\mathbf{S}_{ud}$ and $\mathbf{b}_{ud}$ respectively.

Proposition 2 *The MMSE solution for the FFF and FBF taps is [2]:* $\mathbf{w}_{dfe,k} = \mathbf{F}_u^{-1}\mathbf{s}_{k,i}(i)$, $\mathbf{d}_{dfe,k} = \mathbf{S}_{dd}^H(i)\mathbf{w}_{dfe,k}$, *where* $\mathbf{F}_u = \mathbf{S}_{ud}(i)\mathbf{S}_{ud}^H(i) + \mathbf{R}_n'$, $\mathbf{R}_n' = E[\mathbf{n}(i)\mathbf{n}^H(i)]$.

This solution can be adaptively obtained using training symbols from the K users. The FFF/FBFs are normalized with respect to one of the users, say user 1. Define $\beta_k = d_{dfe,1}^*(k,i)/d_{dfe,k}(1,i)$ for $1 < k \le K$, where $d_{dfe,k}(m,i)$ denotes the effect due to the m-th user's i-th bit. 'Scaled' FFFs and FBFs are defined for $1 < k \le K$ as $\tilde{\mathbf{w}}_{dfe,k} = \beta_k\mathbf{w}_{dfe,k}$ and $\tilde{\mathbf{d}}_{dfe,k} = \beta_k\mathbf{d}_{dfe,k}$. The WLS metric becomes $\Lambda(\mathbf{b}_D) = \sum_{k=1}^{K}\sum_{i=0}^{N_b-1}[-2\mathrm{Re}[b_{k,i}^*\tilde{\mathbf{w}}_{dfe,k}^H\mathbf{y}(i)] + b_{k,i}^*\tilde{\mathbf{d}}_{dfe,k}^H\mathbf{b}_{dd}(i)]$.

Ignoring the scaling factor β_k, when users have different power levels, results in performance loss [3]. The WLS data detection is now performed by using the Viterbi algorithm [3].

IV. Conclusions

A more general optimal detector, compared to the ML detector, is presented and its adaptive version is realized.

References

[1] S. Verdu, "Minimum Probability of Error for Asynchronous Gaussian Multiple-Access Channels," *IEEE Trans. Info. Theory*, vol. IT-32, pp. 85-96, Jan. 1986.

[2] P. B. Rapajic and D. K. Borah, "Adaptive MMSE Maximum Likelihood CDMA Multiuser Detection," *IEEE J. Select. Areas Commun.*, vol. 17, pp. 2110-2122, Dec. 1999.

[3] D. K. Borah and P. B. Rapajic, "Adaptive Maximum Likelihood Multiuser Detection," submitted to *IEEE Trans. Info. Theory*.

[1]Part of the work was done at RSISE, Australian National University, Canberra, Australia.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Adaptive Bayesian Multiuser Detection [1]

Xiaodong Wang
Dept. of Electrical Engineering
Texas A&M University
College Station, TX 77843-3128
e-mail: wangx@ee.tamu.edu

Rong Chen
Dept. of Statistics
Texas A&M University
College Station, TX 77843-3128
e-mail: chen@stat.tamu.edu

Abstract — **We consider the problem of simultaneous parameter estimation and data restoration in a synchronous CDMA system. Bayesian inference of all unknown quantities is made from the superimposed and noisy received signals. The Gibbs sampler, a Markov Chain Monte Carlo procedure, is employed to calculate the Bayesian estimates. The basic idea is to generate ergodic random samples from the joint posterior distribution of all unknowns, and then to average the appropriate samples to obtain the estimates of the unknown quantities. Being "soft-input soft-output" in nature, this technique is well suited for iterative processing in a coded system, which allows the adaptive Bayesian multiuser detector to refine its processing based on the information from the decoding stage, and vice versa – a receiver structure termed as *adaptive Turbo multiuser detector.***

I. System Description

We consider a synchronous CDMA system with K users, employing normalized modulation waveforms $s_1, s_2, \cdots, s_K$, and signaling through a channel with additive white Gaussian noise. The received signal is given by

$$r(i) \;=\; \sum_{k=1}^{K} A_k\, x_k(i)\, s_k + n(i), \quad i = 0, \cdots, M-1. \quad (1)$$

In (1), M is the number of data symbols per user per frame; A_k, $x_k(i)$ and s_k denote respectively the amplitude, the i-th symbol and the normalized spreading waveform of the k-th user; $n(i) = [n_0(i)\ n_1(i)\ \cdots\ n_{P-1}(i)]^T$ is a zero-mean white Gaussian noise vector, i.e., $n_j(i) \sim \mathcal{N}(0, \sigma^2)$, where σ^2 is the variance of the noise. Define the following *a priori* symbol probabilities

$$\rho_k(i) \;\triangleq\; P[x_k(i) = +1], \quad i = 0, \cdots, M-1;\ k = 1, \cdots, K.$$

Note that when no prior information is available, then $\rho_k(i) = 1/2$, i.e., all symbols are equally likely.

Denote $\boldsymbol{Y} \triangleq \{r(0), r(1), \cdots, r(M-1)\}$. We consider the problem of estimating the *a posteriori* probabilities of the transmitted symbols

$$P[x_k(i) = +1 \mid \boldsymbol{Y}], \quad i = 0, \cdots, M-1;\ k = 1, \cdots, K,$$

based on the received signals $\boldsymbol{Y}$ and the prior information $\{\rho_k(i)\}_{k=1;\,i=0}^{K;\,M-1}$, without knowing the channel amplitudes $\{A_k\}_{k=1}^{K}$ and the noise variance σ^2.

[1]This work was supported in part by the Interdisciplinary Research Initiatives Program, Texas A&M University. X. Wang was supported in part by the NSF grant CAREER CCR-9875314. R. Chen was supported in part by the U.S. National Science Foundation under grant DMS 9626113 and grant DMS-9982846.

II. The Gibbs Multiuser Detector

We choose the following conjugate prior distributions for the unknown parameters $p(\boldsymbol{a})$, $p\left(\sigma^2\right)$ and $p(\boldsymbol{X})$. For the unknown amplitude vector $\boldsymbol{a}$, a truncated Gaussian prior distribution is assumed,

$$p(\boldsymbol{a}) \;\propto\; \mathcal{N}(\boldsymbol{a}_0, \boldsymbol{\Sigma}_0)\ I_{\{\boldsymbol{a}>0\}}.$$

For the noise variance σ^2, an inverse chi-square prior distribution is assumed,

$$p\left(\sigma^2\right) \;\sim\; \chi^{-2}(\nu_0, \lambda_0).$$

Finally, the prior distribution $p(\boldsymbol{X})$ can be expressed as

$$p(\boldsymbol{X}) \;=\; \prod_{i=0}^{M-1} \prod_{k=1}^{K} \rho_k(i)^{\delta_{ki}} [1 - \rho_k(i)]^{1-\delta_{ki}},$$

where δ_{ki} is the indicator such that $\delta_{ki} = 1$ if $x_k(i) = +1$ and $\delta_{ki} = 0$ if $x_k(i) = -1$.

The Gibbs sampling implementation of the adaptive Bayesian multiuser detector in Gaussian noise proceeds iteratively as follows. Given the initial values of the unknown quantities $\{\boldsymbol{a}^{(0)}, \sigma^{2(0)}, \boldsymbol{X}^{(0)}\}$ drawn from the above prior distributions, and for $n = 1, 2, \cdots$

1. Draw $\boldsymbol{a}^{(n)}$ from $p(\boldsymbol{a} \mid \sigma^{2(n-1)}, \boldsymbol{X}^{(n-1)}, \boldsymbol{Y})$.
2. Draw $\sigma^{2(n)}$ from $p(\sigma^2 \mid \boldsymbol{a}^{(n)}, \boldsymbol{X}^{(n-1)}, \boldsymbol{Y})$.
3. For $i = 0,\ 1,\ \cdots,\ M-1$
   For $k = 1,\ 2,\ \cdots,\ K$
   Draw $x_k(i)^{(n)}$ from $P[x_k(i) \mid \boldsymbol{a}^{(n)}, \sigma^{2(n)}, \boldsymbol{X}_{ki}^{(n)}, \boldsymbol{Y}]$,

where $\boldsymbol{X}_{ki}^{(n)} \triangleq \{\boldsymbol{x}(0)^{(n)}, \cdots, \boldsymbol{x}(i-1)^{(n)}, x_1(i)^{(n)}, \cdots x_{k-1}(i)^{(n)}, x_{k+1}(i)^{(n-1)}, \cdots, x_K(i)^{(n-1)}, \boldsymbol{x}(i+1)^{(n-1)}, \cdots, \boldsymbol{x}(M-1)^{(n-1)}\}$. The conditional distributions in the above algorithm can be found in closed forms.

To ensure convergence, the above procedure is usually carried out for $(n_0 + N)$ iterations and samples from the last N iterations are used to calculate the Bayesian estimates of the unknown quantities. In particular, the *a posteriori* symbol probabilities in are approximated as

$$\hat{P}[x_k(i) = +1 \mid \boldsymbol{Y}] \;\cong\; \frac{1}{N} \sum_{n=n_0+1}^{n_0+N} \delta_{ki}^{(n)}.$$

The above Bayesian multiuser detector can incorporate the *a priori* symbol probabilities, and it produces as output the *a posteriori* symbol probabilities. Hence it is very well suited for iterative processing in a coded system, which allows the adaptive Bayesian multiuser detector to refine its processing based on the information from the decoding stage, and vice versa – a receiver structure termed as *adaptive Turbo multiuser detector.*

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Joint Detection in Multi-User Systems via Iterative Processing[1]

Christian Schlegel[1]
Dept. of Electrical Engineering
University of Utah
Salt Lake City, UT 84112
email: schlegel@ee.utah.edu

Abstract — **Multi-user detection of CDMA signals is studied in the light of iterative processing. The complete factor graph of a coded CDMA system is used to develop several successively less complex joint detection algorithms whose performance is related to the computational complexity of the algorithm.**

Introduction

We study the general structure of coded CDMA systems from an iterative processing point of view, illuminating how the different parts, in particular the FEC codec and the CDMA receiver have to interact with each other. We apply a series of simplifications to the basic (graphical) structure of the receiver which result in simpler algorithms with reduced performance. In the course of these simplifications we rederive a number of previously proposed receivers, such as the iterative receivers and linear metric generation receivers. We show that if the receiver for a given user does not know the code (FEC) of the other users, its code network breaks into subnetworks, specifically, into a FEC decoder network, and a number of metric generation networks.

The optimal metric generator can easily be formulated, but is in general too complex for most practical considerations. Hence, we simplify this metric generation, which leads to a family of low-complexity interference cancellers. In particular linear metric generation can be performed at the cost of further loss in performance. There exist efficient methods for generating these metrics iteratively [2].

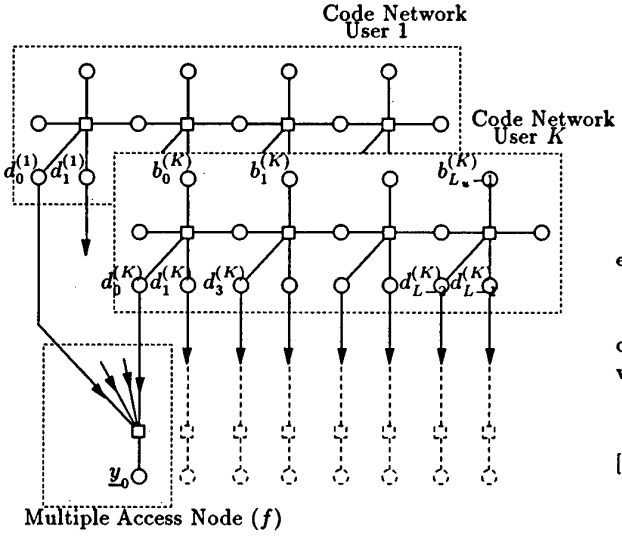


Fig. 1: Factor Graph of a complete coded CDMA system.

[1]Supported in part by NSF Grant No. CCR-9732962.

For illustration, assume that the encoders are (rate $R = 1/2$) convolutional encoders. Using the factor graph representation for a convolutional code [1], a factor graph for the complete decoder can be drawn and is shown in Figure 1: (Note that there are other ways of drawing the code network graph, in particular, the multiple-access node can be expanded into a complete trellis diagram describing the multiple access interference between the symbols d).

We refer to detection in an interference limited environment as *interference cancellation* whenever full joint detection is not possible. That is, we assume that the receiver for the target user, say user K, has no knowledge about the FEC system of the interfering users and can therefore not decode their data streams. Since knowledge of the code of the interfering users is not available, the network structure of their coding system is also unknown, and we have to truncate the receiver network at the transmitted symbol nodes of the interferers, using the a priori distributions for them. The resulting network structure is shown below:

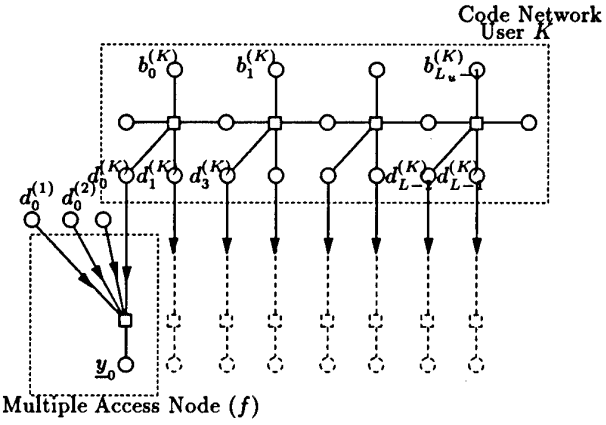


Fig. 2: Factor Graph of the coded CDMA system without knowledge of the FEC networks of the interfering users.

While the algorithm now no longer has to visit the FEC code networks for the $K-1$ (interfering) users, the problem with the large multiple-access node arc incidence persists.

References

[1] F.r. Kschischang, B.J. Frey, and H-A. Loeliger, "Factor graphs and the sum-product algorithm," submitted to *IEEE Trans. Inform. Theory*, July 1998, available at http://www.com.utoronto.ca/frank/factor/.

[2] A. Grant and C. Schlegel, "Iterative implementations for linear multiuser detectors", submitted to *IEEE Trans. Commun.*, February 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Quantum Error Detection

A. Ashikhmin A. Barg
Bell Labs, Lucent Technologies
{aea,abarg}@research.bell-labs.com

E. Knill
Los Alamos Natl. Lab.
knill@lanl.gov

S. Litsyn
Tel Aviv University
litsyn@eng.tau.ac.il

Abstract — **We show that the probability of undetected error for a quantum code on the depolarizing channel can be expressed via code's weight enumerators. We prove that there exist quantum codes whose probability of undetected error falls exponentially with the length of the code and derive a lower bound on this exponent. To derive upper bounds we formulate a linear programming problem and present two feasible programs for it. The asymptotic upper and lower bounds coincide in a certain interval of code rates close to 1.**

I. Introduction

A quantum code $Q((n,K))$ is a $K-$dimensional linear subspace of the space $H=\mathbf{C}^{2^n}$ [2]. The number $R=(\log_2 K)/n$ is called the rate of Q. During transmission over the channel a quantum state $\mathbf{v}\in H$ can be altered by an error operator

$$E=\tau_1\otimes\tau_2\otimes\ldots\otimes\tau_n, \qquad (1)$$

where $\tau_i\in\{\pm iI_2,\pm i\sigma_x,\pm i\sigma_z,\pm i\sigma_y\}$, and $\sigma_x,\sigma_y,\sigma_z$ are the Pauli matrices. Under the action of E the "tramsmitted" state is transformed to $E\mathbf{v}$. The number of nonidentity matrices in (1) is called the weight of of error, $\mathrm{wt}(E)$. By the definition of the channel, the probability of an error operator E equals $(p/3)^{\mathrm{wt}(E)}(1-p)^{n-\mathrm{wt}(E)}$.

Let P be the orthogonal projection on the code Q. "Weight enumerators" associated with Q have the form $B(x,y)=\sum B_i x^{n-i}y^i$ and $B^\perp(x,y)=\sum B_i^\perp x^{n-i}y^i$, where [3]

$$B_i=\sum_{\mathrm{wt}(E)=i}\mathrm{Tr}^2(EP) \text{ and } B_i^\perp=\sum_{\mathrm{wt}(E)=i}\mathrm{Tr}(PEPE).$$

II. Error Detection

It is possible to define error detection for quantum codes in several ways. If the measurement of the received state produces a vector in the subspace orthogonal to Q, this indicates a detectable error. If this measurement gives a vector in Q, the error is not detected. However, in a general situation, we assume that if the received state is very close to the transmitted state, no error has occurred.

Calculating the probability $P_{ue}(Q,p)$ of undetected error under these assumptions, we obtain

Theorem 1

$$P_{ue}(Q,p)=\frac{K}{K+1}\sum_{i=0}^{n}(B_i^\perp-B_i)\left(\frac{p^i}{3}\right)(1-p)^{n-i}.$$

We also consider some other possible definitions of undetected error that arise under natural physical assumptions. In all the cases the expressions obtained are the same as in the theorem (up to a constant factor).

To describe the behavior of the probability P_{ue} for best possible codes, we define the exponent

$$E(R,p) = \limsup_{n\to\infty}(-1/n\log_2 P_{ue}(n,R,p)).$$

where $P_{ue}(n,R,p)$ is the minimal attainable probability for codes of rate R.

III. Lower Bound

Let $T_4(x,y)=x\log_4 3-x\log_4 y-(1-x)\log_4(1-y)$ and $H_4(x)=T_4(x,x)$. Let $\delta(R)=H_4^{-1}((1+R)/2)$.

Lemma 1 *There exists a sequence of stabilizer codes of rate R such that $B_i=0$ for $1\le i\le n\delta(R)$ and $B_i^\perp\le n\binom{n}{i}3^i 2^{k-n}$ for $n\delta(R)\le i\le n$.*

Computing $P_{ue}(Q,p)$ for a sequence of codes Q from this lemma, we obtain the following lower bound on $E(R,p)$.

Theorem 2

$$E(R,p)\ge\begin{cases}T_4(H_4^{-1}((1-R)/2),p), & 0\le R\le 2(1-H_4(p))-1,\\ (1-R)/2, & \text{otherwise.}\end{cases}$$

IV. Upper Bounds

Theorem 3 *Let $Z(x)=\sum_{i=0}^n z_i K_i(n,4,x)$ be a polynomial expanded in the basis of the Krawtchouk polynomials. Suppose that*

$$Z(i)\le(p/3)^i(1-p)^{n-i}$$

and

$$(1/2)(1+R)nz_i-Z(i)\ge 0 \quad (1\le i\le n).$$

Then $P_{ue}(R,n)\ge z_0(1/2+R/2)n-Z(0)$.

By an appropriate choice of polynomials we derive two asymptotic upper bounds on $E(R,p)$. We cite the first one. Denote by $R_{lp}(\delta)$ the upper bound [1] on the asymptotic rate of quaternary codes with distance δ and by $\delta_{lp}(R)$ its inverse function.

Theorem 4

$$E(R,p)\le\begin{cases}\frac{1-R}{2}-H_4(\delta_{lp}(\frac{1+R}{2}))+T_4(\delta_{lp}(\frac{1+R}{2}),p), & R\le 2R_{lp}(p)-1,\\ \frac{1-R}{2}, & \text{otherwise.}\end{cases}$$

The second bound derived in the work improves this theorem for medium code rates. The journal version of this talk is published in IEEE Trans. Inform. Theory, May 2000.

References

[1] M. Aaltonen, "Linear programming bounds for tree codes," *IEEE Trans. Inform. Theory*, vol. 25, no. 1, pp. 85–90, 1979.

[2] A.R. Calderbank, E.M. Rains, P.W. Shor and N.J.A. Sloane, "Quantum error correction and orthogonal geometry," *Phys. Rev. Lett.*, vol. 78, pp. 405-409, 1997.

[3] P.W. Shor and R. Laflamme, "Quantum analog of the MacWilliams identities in classical coding theory," *Phys. Rev. Lett.*, vol. 78, pp. 1600-1602, 1997.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Multiuser detection in a quantum channel

Julio Concha[1] and H. V. Poor[1]
Department of Electrical Engineering
Princeton University
Princeton, NJ 08544, USA
e-mail: {jiconcha,poor}@princeton.edu

I. Introduction

The use of multiuser detection techniques in multiple access optical channels has been studied in the literature, with emphasis on optical CDMA [2]. In general, it has been assumed that the optical detection is carried out by PIN diodes, which count the photons present in the field. However, the theory of quantum detection [1] indicates that other measurements might yield significantly smaller error probabilities.

In this paper, we show by example that this can happen in the multiple-access case. We also note that the quantum multiuser detection problem differs from the classical one, in that quantum measurement precludes the use of matched filter banks for non-orthogonal signals.

II. Channel model

We assume that K users transmit information via the electromagnetic field with OOK modulation. Specifically, user k sends a bandpass signal $s_k(t)$ to indicate a "1" and no signal to indicate a "0". s_k can be conveniently described by its lowpass equivalent S_k, where $s_k(t) = \text{Re}\ S_k(t)\ e^{i2\pi f_c t}$ and f_c is the carrier frequency. We will take these signals to represent the electric field in a quasi-monochromatic linearly polarized coherent light beam.

Since we want to study the effect of multiple-access interference, we ignore the effects of noise and assume that the different users transmit synchronously. Thus, the detector receives the linear superposition of the S_k's, which excite various modes of the detector aperture field. The resulting quantum state, described by a density operator ρ, contains the transmitted information. The receiver then has to decide which one of the several possible ρ's is present, using a *probability operator-valued measure* (POVM). This is a collection of Hermitian positive-definite operators Π_k, which must be chosen so that the probability of detection error is minimized.

In the single-user case, we can consider a "matched filter" detector, such that $S_1(t)$ coincides with one of the temporal modes of the field. Then the hypotheses to be tested are $|\psi\rangle = |\alpha\rangle$ vs. $|\psi\rangle = |0\rangle$, where $|\alpha\rangle$ is a coherent state and $|\psi\rangle\langle\psi|$ is the received density operator. It is shown in [1] that in this case an optimally-designed POVM achieves a lower probability of error than a detector based on photon counting.

III. Multiuser detection

Now consider the case $K = 2$. If S_1 and S_2 are orthogonal, they can again be aligned with two temporal modes of the field, so that the hypotheses to test are $|\psi\rangle = |0\rangle\,|0\rangle$ vs. $|\psi\rangle = |\alpha\rangle\,|0\rangle$ vs. $|\psi\rangle = |0\rangle\,|\alpha\rangle$ vs. $|\psi\rangle = |\alpha\rangle\,|\alpha\rangle$. We assume that both users transmit the same average number of photons, $N(=\alpha^2)$. It can be shown that in this case the optimal quantum detector is equivalent to two matched filters acting independently on each mode. In general this is true if the received density operator when user 1 sends symbol i and user 2 sends symbol j is of the form $\rho_{i,j} = \rho_i \otimes \rho_j$.

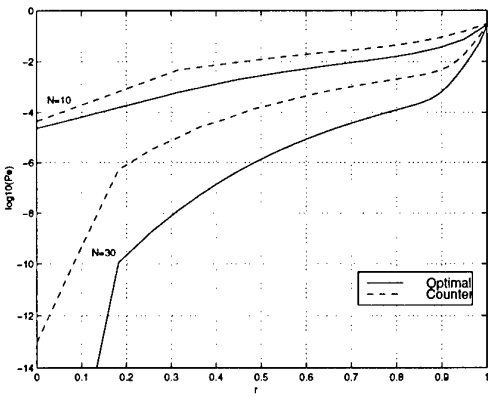


Figure 1: Probability of symbol error for the ML photon counter and the optimal quantum detector.

If S_1 and S_2 are not orthogonal, we can no longer assign separate modes to the different users, so that independent matched filtering is not only not optimal, but actually not possible. As an alternative we can take

$$g_1 = S_1/\|S_1\| \quad (1)$$

$$g_2 \propto S_2/\|S_2\| - r g_1, \quad (2)$$

where r is the correlation coefficient between S_1 and S_2.

Hence, the 4 hypotheses are $|\psi\rangle = |0\rangle\,|0\rangle$ vs. $|\psi\rangle = |\beta_1\rangle\,|\beta_2\rangle$ vs. $|\psi\rangle = |\alpha\rangle\,|0\rangle$ vs. $|\psi\rangle = \left|\sqrt{\alpha^2+\beta_1^2}\right\rangle|\beta_2\rangle$, where $r = \beta_1/\alpha$ and the two user powers are equal, i.e. $N = \alpha^2 = \beta_1^2 + \beta_2^2$.

Fig. 1 shows the probability of (symbol) error of the optimal quantum detector as the correlation coefficient varies between 0 and 1, for $N = 10$ and $N = 30$. The dashed line corresponds to a maximum-likelihood multiuser detector based on the number of photon counts in each of the modes. It can be seen that the optimal quantum detector outperforms the ML photon counter by 3 orders of magnitude for $r \approx 0.3$.

References

[1] C. W. Helstrom. *Quantum detection and estimation theory.* Academic Press, 1976.

[2] L. Nelson and H. V. Poor. Performance of multiuser detection for optical CDMA—Part I: error probabilities. *IEEE Trans. Communications*, 43:2803, 1995.

[1]This work was supported by the National Science Foundation under Grant CCR-99-80590.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Quantum Gaussian Channels

A.S.Holevo
Steklov Mathematical Institute
Gubkina 8
117966 Moscow, Russia
e-mail: holevo@mi.ras.ru

O.Hirota
Research Center for Quantum Communications
Tamagawa University
194-8610 Tokyo, Japan
e-mail:
hirota@lab.tamagawa.ac.jp

Abstract — **The aim of this paper is explicit calculation of the classical capacity of quantum Gaussian channels, in particular, of those using squeezed states. The calculation is based on a general formula for the entropy of quantum Gaussian state, which is of independent interest, and on the recently proved coding theorem for quantum communication channels.**

I. Introduction

One of the recent achievements of the quantum information theory is the direct coding theorem for transmission of classical information through quantum communication channels, which provides an explicit formula for the capacity of the channel as supremum of the quantum entropy bound with respect to input probability distributions. This result was extended to channels with constrained inputs [2] among which channels with additive quantum Gaussian noise and the constrained power of the signal are most important for applications, because the class of quantum Gaussian states includes coherent and squeezed states, together with their thermal mixtures. In this talk we present several results concerning the capacity of quantum Gaussian channels.

II. Classical signal plus quantum noise

We consider quantum system, such as cavity field with finite numbers of modes, described by annihilation operators $a_1, \ldots, a_s$ satisfying the canonical commutation relation (CCR) Let $\mathcal{H}$ be the Hilbert space of irreducible representation of CCR, and let $\rho(0)$ be a density operator in $\mathcal{H}$ describing state of the cavity field. Consider the family of density operators

$$\rho(\mu) = \mathcal{D}(\mu)\rho(0)\mathcal{D}(\mu)^\dagger \; ; \; \mu = (\mu_j) \in \mathbf{C}^s, \tag{1}$$

where $\mathcal{D}(\mu)$ is the *displacement operator* in $\mathcal{H}$. In communication theory $\rho(0)$ describes background noise, comprising quantum noise, and μ is the classical signal. Thus the mapping $\mu \to \rho(\mu)$ is classical-quantum channel in the sense of [2].

According to [3], the capacity of such a channel is equal to

$$C = \sup_{P \in \mathcal{P}_1} H(\rho_P) - H(\rho(0)). \tag{2}$$

where $H = -\mathrm{Tr}\rho\log\rho$ is the von Neumann entropy, $\rho_P = \int \rho(\mu)P(d\mu)$, and $\mathcal{P}_1$ is a convex subset of probability distributions $P(d\mu)$ on $\mathbf{C}^s$, satisfying the power constraint

$$\int \sum_{j=1}^{s} \hbar\omega_j |\mu_j|^2 P(d\mu) \le E. \tag{3}$$

III. The capacity of quantum Gaussian channels

Let $\rho(0)$ be the Gaussian density operator with $m = 0$ and the correlation matrix α. Let P be Gaussian probability distribution with correlation matrix β and zero mean. The inequality (3) then takes the form:

$$\mathrm{Sp}\,\varepsilon\beta \le E, \tag{4}$$

where ε is the diagonal energy matrix.

Theorem. The capacity of the Gaussian channel is equal to

$$C = \max_{\beta \in B_1} \frac{1}{2}\mathrm{Sp}\, g(\mathrm{abs}(\Delta^{-1}(\alpha+\beta)) - I/2) \tag{5}$$
$$-\frac{1}{2}\mathrm{Sp}\, g(\mathrm{abs}(\Delta^{-1}\alpha) - I/2)$$

where $g(x) = (x+1)\log(x+1) - x\log x$ and B_1 is the convex set of real positive matrices β, satisfying (4).

Example. In the case of squeezed state $\rho(0)$ in one mode let $N_s = E/\hbar\omega, N = \mathrm{Tr}\rho(0)a^\dagger a = (\omega^2\alpha^{qq} + \alpha^{pp})/2\hbar\omega$ be, correspondingly, the mean photon numbers in the signal and in the noise. Then if $N^2 + N \le N_s^2$, the capacity of the squeezed state channel is

$$C = g(N + N_s), \tag{6}$$

otherwise

$$C = g\left(\sqrt{N_s(2N+1+2\sqrt{N^2+N})} + \frac{1}{4} - \frac{1}{2}\right). \tag{7}$$

From these expressions one sees that using squeezing states under constrained input energy E does increase the capacity. On the other hand, with restricted output energy $\hbar\omega(N+N_s)$ one cannot obtain capacity greater than (6), which is known to be the absolute maximum under this constraint.

Acknowledgments

The first author acknowledges hospitality and stimulating discussions during his visit to the Research Center for Quantum Communications, Tamagawa University.

References

[1] A. S. Holevo, "The capacity of quantum communication channel with general signal states," IEEE Trans. Inform. Theory, vol. 44, no. 1, pp. 296-272 1998).

[2] A. S. Holevo, "Coding theorems for Quantum Channels", *Tamagawa University Research Review*, No.4, 1998.

[3] A. S. Holevo, M. Sohma, O. Hirota, "Capacity of quantum Gaussian channels", *Phys. Rev. A*, vol.59, no.3, pp. 1820-1828 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Quantum Arithmetic Coding

Isaac L. Chuang
Dharmendra S. Modha
IBM Almaden Research Center
650 Harry Road
San Jose, CA 95120
{ichuang,dmodha}@almaden.ibm.com

Abstract — **We study the problem of compressing a block of symbols (a block quantum state) emitted by a memoryless quantum Bernoulli source. We present a simple-to-implement quantum algorithm for projecting, with high probability, the block quantum state onto the *typical subspace* spanned by the leading eigenstates of its density matrix. We propose a fixed-rate quantum Shannon-Fano code to compress the projected block quantum state using a per symbol code rate that is slightly higher than the von Neumann entropy limit. Finally, we propose quantum arithmetic codes to efficiently implement quantum Shannon-Fano codes.**

I. Extended Abstract

Modern information theory makes fundamental assumptions concerning the physical representation and processing of information. Following the lead of classical mechanics, modern information theory assumes that a information bit can exist in either one of two states, say, 0 or 1. However, classical physics is known to fail spectacularly under many circumstances, for example, when the objects being described are very small or have very large energies. This regime of physics is described by the laws of quantum mechanics. Conventional information theory fails to properly describe how information can be represented and transformed in such physical systems, and must be replaced by an appropriate quantum analog: quantum information theory. In contrast to the classical information bit, a quantum information bit can exist in a superposition of two orthogonal quantum states.

The problem of compression is central to storage and transmission of quantum data. We investigate quantum algorithms for compressing a sequence of symbols emitted by a memoryless quantum Bernoulli source. The basis for compression of classical data is Shannon's noiseless coding theorem: if the per symbol code rate is slightly larger than the *Shannon entropy*, then there exists a block code (with sufficiently large block size) such that the compressed message can be recovered with *probability* close to unity. The quantum analogue to Shannon's theorem is Schumacher's theorem [2]: if the per symbol code rate is slightly larger than the von Neumann entropy, then there exists a block code (with sufficiently large block size) such that the compressed message can be recovered with *average fidelity* close to unity. The similarity of the two theorems makes it possible to use, to a limited extent, classical algorithms for performing quantum data compression. However, classical compression codes cannot immediately be translated into quantum versions; for example, in order to preserve the coherent quantum state, all operations performed on the data must be reversible and must not entangle the state with any temporary variables. Furthermore, it is essential that the original state must be entirely obliterated in producing the encoded state, because quantum states cannot be cloned.

The statistics underlying a quantum memoryless Bernoulli source is completely captured by its density matrix. The fundamental idea behind quantum data compression is to analyze the eigen-structure of the joint density matrix associated with a block quantum state emitted by the quantum memoryless Bernoulli source. As our first contribution, we present a quantum-mechanical algorithm for projecting the block quantum state onto the subspace spanned by the leading (or typical) eigenstates of the joint density matrix. Our algorithm computes, in parallel, an indicator function that is 0 if the eigenstate is typical and 1 otherwise. By making a measurement on the quantum bit associated with the indicator function, with very high probability, we project the block quantum state onto the *typical subspace* spanned by the leading eigenstates. Our theoretical results represent a strengthening of Schumacher's pioneering result in that they hold for fixed block sizes and they deliver a rate of convergence.

The projection onto the typical subspace wipes out the trailing eigenstates, and, hence, the projected quantum state lies in the low-dimensional typical subspace. Consequently, each leading eigenstate can be represented using roughly the logarithm of the dimension of the typical subspace. The central problem of quantum data compression is to efficiently compute such low-dimensional representations. As our second contribution, we propose a quantum Shannon-Fano code to represent and compress the projected block quantum state using a per symbol code rate that is slightly higher than the von Neumann entropy limit.

As our third contribution, we propose quantum arithmetic codes to efficiently implement quantum Shannon-Fano codes. Our arithmetic encoder/decoder use a certain finite-precision arithmetic process that is inspired by classical arithmetic coding. The novelty of quantum arithmetic coding is to implement finite-precision arithmetic processes in a quantum-mechanically reversible fashion. Our arithmetic encoder/decoder have a cubic circuit and a cubic computational complexity in the block size. The proposed encoder and decoder are quantum-mechanical inverses of each other, and constitute a very satisfying example of reversible quantum computation.

References

[1] I. L. Chuang and D. S. Modha, "Reversible Arithmetic Coding for Quantum Data Compression," to appear in *IEEE Trans. Inform. Theory*, May 2000. http://www.almaden.ibm.com/cs/people/dmodha

[2] B. Schumacher, "Quantum coding," *Physical Review A*, vol. 51, pp. 2738–2747, 1995.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Positive Capacity Region of Two-dimensional Asymmetric Run Length Constrained Channels*

Akiko Kato
Dept. of Mathematical Engineering and Information Physics, University of Tokyo, Tokyo 113-8656, Japan
(Died on Feb. 27, 2000, at age 32)

Kenneth Zeger
Department of Electrical and Computer Engineering, University of California, San Diego, CA 92103-0407
zeger@ucsd.edu

I. Introduction

Run length constraints derive from digital storage applications [2]. For nonnegative integers d and k, a binary sequence is said to satisfy a one-dimensional (d,k)-*constraint* if every run of zeros has length at least d and at most k (if two ones are adjacent in the sequence we say that a run of zeros of length zero is between them). A two-dimensional binary pattern arranged in an $m \times n$ rectangle is said to be (d_1,k_1,d_2,k_2)-*constrained* if it satisfies a one-dimensional (d_1,k_1)-constraint horizontally and a one-dimensional (d_2,k_2)-constraint vertically. The two-dimensional (d_1,k_1,d_2,k_2)-*capacity* is defined as

$$C_{d_1,k_1,d_2,k_2} = \lim_{m,n\to\infty} \frac{\log_2 N_{m,n}^{(d_1,k_1,d_2,k_2)}}{mn}$$

where $N_{m,n}^{(d_1,k_1,d_2,k_2)}$ denotes the number of $m \times n$ rectangles that are (d_1,k_1,d_2,k_2)-constrained. If $d = d_1 = d_2$ and $k = k_1 = k_2$ (this is called the *symmetric constraint*) then the two-dimensional (d_1,k_1,d_2,k_2)-capacity is called the two-dimensional (d,k)-*capacity*, and is denoted by $C_{d,k}$. A proof was given in [3] that shows the two-dimensional (d,k)-capacities exist, and essentially the same proof shows that the C_{d_1,k_1,d_2,k_2} exist.

The two-dimensional asymmetric *positive capacity region* is the set

$$\{(d_1,k_1,d_2,k_2) : C_{d_1,k_1;d_2,k_2} > 0\}.$$

A basic question is to determine which constraints actually lie in the positive capacity region and which do not. For the symmetric constraints, it was shown in [1] that $C_{1,2} = 0$ and a complete characterization of which (d,k) integer pairs yield positive capacities was given in [3] and is stated as the proposition below.

Proposition 1 *$C_{d,k} > 0$ if and only if $k - d \geq 2$ or $(d,k) = (0,1)$.*

II. Main Results

In the present paper we determine whether or not the two-dimensional capacity is positive, for a large set of asymmetric constraints (d_1,k_1,d_2,k_2), and the main results are summarized in Theorem 1. It is interesting to note that for the symmetric constraint (i.e. when $d_1 = d_2$ and $k_1 = k_2$), the capacity is zero whenever d and k are positive and differ by one, whereas for many asymmetric constraints the capacity is positive when the horizontal constraints or the vertical constraints differ by one (e.g. Theorem 1 part (ii(B)b)). However, in the asymmetric case if, for example, $k_1 = d_1 + 1 \leq d_2$ then the capacity is zero (by Theorem 1 part (i)).

*This work was supported in part by the National Science Foundation and by a JSPS Fellowship for Young Scientists.

Theorem 1 *Let d_1, k_1, d_2, and k_2 be nonnegative integers such that $d_1 \leq k_1$ and $d_2 \leq k_2$. Let $d = \min(d_1,d_2)$, $D = \max(d_1,d_2)$, $k = \min(k_1,k_2)$, $K = \max(k_1,k_2)$, $\delta = k - D$, and $\Delta = K - d$. Then the following partially characterizes the positive capacity region of two-dimensional run length constrained channels:*

(i) *If $\delta \leq 0$ then $C_{d_1,k_1;d_2,k_2} = 0$.*

(ii) *If $\delta = 1$ then*

(A) *If $d = 0$ then $C_{d_1,k_1;d_2,k_2} > 0$.*

(B) *If $d \geq 1$ then*

(a) *If $\Delta \leq 1$ then $C_{d_1,k_1;d_2,k_2} = 0$.*

(b) *If $\Delta > d_1 = d_2$ then $C_{d_1,k_1;d_2,k_2} > 0$.*

(c) *If $\Delta \geq 3$ and $d = 1$ then $C_{d_1,k_1;d_2,k_2} > 0$.*

(iii) *If $\delta \geq 2$ then $C_{d_1,k_1;d_2,k_2} > 0$.*

The only case that is presently not completely characterized in Theorem 1 is part (iiB), namely when $\delta = 1$, $d \geq 1$, and $\Delta \geq 2$. If $\delta = 1$, $d = 1$, and $\Delta = 2$ then the only capacities that need be considered are $C_{1,2,1,3}$ and $C_{1,3,2,3}$. But $C_{1,2,1,3} > 0$ from part (ii(B)b). Thus if we were able to show that $C_{1,3,2,3} > 0$ then we could replace $\Delta \geq 3$ by $\Delta \geq 2$ in part (ii(B)c). However, computer simulation suggests, but does not prove, that perhaps $C_{1,3,2,3} = 0$. This remains an open question.

Also, computer simulations suggest the plausibility of Conjecture 1 below, for which we presently do not have a proof either.

Conjecture 1 *$C_{d,d+1,d,2d} = 0$ whenever $d \geq 0$.*

Conjecture 1 would characterize with Theorem 1(ii(B)b) the positive capacity region for $k = d + 1$ and $d_1 = d_2$ as:

$$C_{d,K,d,d+1} = C_{d,d+1,d,K} = 0 \text{ if and only if } K \leq 2d.$$

References

[1] J. J. Ashley and B. H. Marcus, "Two-Dimensional Lowpass Filtering Codes," IBM Research Division, Almaden Research Center, IBM Research Report RJ 10045 (90541), October 1996.

[2] K. A. Immink, P. H. Siegel, and J. K. Wolf, "Codes for Digital Recorders," *IEEE Trans. Inform. Theory*, vol. 44, pp. 2260–2299, October 1998.

[3] A. Kato and K. Zeger, "On the Capacity of Two-Dimensional Run Length Constrained Channels," *IEEE Trans. Inform. Theory*, vol. 45, no. 5, July 1999, pp. 1527–1540.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

New Upper and Lower Bounds on the Channel Capacity of Read/Write Isolated Memory

M. Golin, X.R. Yong and Y.P. Zhang [1]
Department of Computer Science
Hong Kong UST
Clear Water Bay, Kowloon
Hong Kong, China
{golin,xryong,ypzhang}@cs.ust.hk

L. Sheng
Department of Mathematics & Computer Science
Drexel University
3141 Chestnut Street
Philadelphia, PA 19104, USA.
lsheng@mcs.drexel.edu

Abstract — **We show that a Read/Write Isolated Channel can be modelled as a constrained binary matrix. This permits the use of constrained matrix techniques to bound the capacity of the channel, improving on the older known bounds.**

I. Introduction

A serial binary $(0,1)$ memory is *read isolated* if no two consecutive positions in the memory may both store 1's. A serial binary $(0,1)$ memory that undergoes rewriting is *write isolated* if it satisfies the restriction that no two consecutive positions in the memory can be changed during one rewriting phase.

A *read/write isolated memory* (RWIM) is a binary, linearly ordered, rewritable storage medium that obeys both the read and write restrictions. This type of memory was considered by Cohn in [3], who examined its channel capacity. The set of all permissible binary memory configurations can be considered as a channel alphabet. The rewriting restrictions determine which characters may follow which characters in the channel. The *channel capacity* of this process can then be defined as follows [2] [8]: let k be the size of the memory in binary symbols, r the lifetime of the memory in rewrite cycles and $N(k,r)$ the number of distinct sequences of r characters. For fixed k, the *channel capacity,* measured in bits per rewrite, is defined to be [6]

$$C_k = \lim_{r\to\infty} \frac{1}{r} \log_2 N(k,r).$$

The channel capacity of the read/write isolated memory, in bits per symbol per rewrite, is then defined to be

$$C = \lim_{k\to\infty} \frac{1}{k} C_k.$$

In [3] Cohn established several expressions for the capacities C_k and derived the following upper and lower bounds on C: $0.50913\ldots \le C \le 0.56029\ldots$. In this paper we continue the investigation of the channel capacity and manage to refine the bounds to

$$0.53500\ldots \le C \le 0.55209\ldots.$$

We also provide reasons to conjecture that $C = 0.53500\ldots$.

II. Constrained Matrices

The main observation is that there is another way of viewing the rewriting process. Suppose k, the size of the memory and r, the number of rewrites, are known. Then we can define, B, a $r \times k$ binary matrix: $\forall 1 \le i \le k$, $1 \le j \le r$,

$B(j,i)$ = content of location i after the $(j-1)$st rewrite.

Thus the jth row of B is the content of the memory after the $(j-1)$st rewrite. Translating the RWIM rules into matrix notation shows that B satisfies the following two constraints:

1. *read restriction:* B does not contain any two horizontally consecutive ones, i.e., it does not contain any 1×2 submatrix $(1\,1)$;
2. *write restriction:* B does not contain any 2×2 submatrix of the form $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ or $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Note too that if B is *any* $r \times k$ binary matrix that obeys the two conditions above then B can be viewed as modelling a memory with the jth row of B being the content of the memory at time j. The memory thus modelled satisfies the read/write isolated conditions. We have therefore just seen that $N(k,r)$, previously defined as the number of distinct sequences of r characters, is also *the number of $r \times k$ binary matrices that satisfy conditions (1) and (2).*

This observation permits noticing that C is not only the capacity of the RWIM channel but also the capacity of the *constrained matrices* satisfying (1) and (2). We can therefore use transform matrix techniques developed to study the capacity of constrained matrices, e.g., in [1][4][5][7], to derive the better bounds. We note that these techniques have to be modified slightly to deal with the fact that the constraint system here is not symmetric, i.e., if matrix B satisfies (1) and (2) it is possible that B^T does not satisfy (1) and (2) (previously studied constraints all seem to have been symmetric and the techniques implicitly used this symmetry).

[1]This work partially supported by Hong Kong CERG grants HKUST652/95E, 6082/97E and 6137/98E and DIMACS

References

[1] N. Calkin and H. Wilf "The number of independent sets in a grid graph," *SIAM J. Discrete Math,* **11** (1998), 54-60.

[2] G. Cohen and G. Zemor, "Write-isolated memories," *Discrete Math,* **114** (1993) 105-113.

[3] M. Cohn, "On the channel capacity of read/write isolated memory," *Discrete Applied Math,* **56** (1995) 1-8.

[4] Konrad Engel "On the Fibonacci Number of an M X N Lattice," *Fibonacci Quarterly,* **28** (1990) 72-78.

[5] A. Kato and K. Zeger "On the Capacity of Two-Dimensional Run-Length Constrained Channels," *IEEE Transactions on Information Theory,* **45**(5), (July 1999) 1527-1540.

[6] C. E. Shannon, *The Mathematical Theory of Communication,* University of Illinois Press, Urbana, IL, (1949).

[7] W. Weeks and R. Blahut "The Capacity and Coding Gain of Certain Checkerboard Codes," *IEEE Transactions on Information Theory,* **44**(3), (May 1998) 1193-1203.

[8] J. K. Wolf, A. D. Wyner, J. Ziv and J. Körner, "Coding for write-once memory," *AT&T Bell Laboratories Tech. Journal,* **63**(6)(1984) 1089-1112.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Zero Capacity Region of Multidimensional Run Length Constraints*

Hisashi Ito
Dept. of Information Science,
Toho University,
Chiba 274-8510, Japan
his@kuro.is.sci.toho-u.ac.jp

Akiko Kato
Dept. of Math. Engineering
and Information Physics,
University of Tokyo,
Tokyo 113-8656, Japan
(Died on Feb. 27, 2000, age 32)

Zsigmond Nagy
Department of Electrical
and Computer Engineering,
University of California,
San Diego, CA 92093-0407
nagy@code.ucsd.edu

Kenneth Zeger
Department of Electrical
and Computer Engineering
University of California,
San Diego, CA 92093-0407
zeger@ucsd.edu

I. Introduction

Run length constraints derive from digital storage applications [3]. For nonnegative integers d and k, a binary sequence is (d,k)-*constrained* if there are at most k consecutive zeros and between every two ones there are at least d consecutive zeros. An n-dimensional pattern of zeros and ones arranged in an $m_1 \times m_2 \times \cdots \times m_n$ hyper-rectangle is (d,k)-*constrained* if it is (1-dimensional) (d,k)-constrained in each of the n coordinate axis directions. The n-dimensional (d,k)-*capacity* is defined as

$$C_{d,k}^{(n)} = \lim_{m_1,m_2,\ldots,m_n \to \infty} \frac{\log_2 N_{m_1,m_2,\ldots,m_n}^{(n;d,k)}}{m_1 m_2 \cdots m_n},$$

where $N_{m_1,m_2,\ldots,m_n}^{(n;d,k)}$ denotes the number of (d,k)-constrained patterns on an $m_1 \times m_2 \times \cdots \times m_n$ hyper-rectangle. A simple proof was given in [5] that shows the existence of two-dimensional (d,k)-capacities, and a slight modification of the proof can show that the n-dimensional (d,k)-capacities exist. The capacity $C_{d,k}^{(n)}$ represents the maximum number of bits of information that can be stored asymptotically per unit volume in n-dimensional space without violating the (d,k) constraint.

The study of 1-dimensional (d,k)-capacities was originally motivated by applications in magnetic storage. Interest in 2-dimensional (d,k)-capacities has recently increased due to emerging 2-dimensional optical recording devices, and the multidimensional (d,k)-capacities may play a role in future technologies as well. A tutorial on these topics is given in [3].

In general, the exact values of the various n-dimensional (d,k)-capacities are not known except in a few cases [6]. For example, in all dimensions, if $k = d$ the capacity is zero, and if $d = 0$ the capacity is positive for all $k \geq 1$. In one dimension the capacity is positive whenever $k > d \geq 0$. Very tight upper and lower bounds on the $(0,1)$-capacity were given for two dimensions in [1], improved in [2, 7], and extended to three dimensions in [7]. In [9] an encoding procedure for the 2-dimensional (d,∞)-constraint was given for all positive integer d's, and in [8] an encoding procedure for the 2-dimensional $(0,1)$-constraint was given whose coding rating comes very close to the capacity. It was shown [5] that whenever $k > d \geq 1$, the 2-dimensional capacity is zero if and only if $k = d+1$.

II. Main Results

We present two main results that characterize the zero capacity region for finite dimensions and in the limit of large dimensions. The first result generalizes the zero capacity characterization in [5] to all dimensions greater than one, which turns out to be exactly the same as in dimension 2. The second result gives a necessary and sufficient condition on d and k, such that the capacity approaches zero in the limit as the dimension n grows to infinity. These results are summarized in the following two theorems.

Theorem 1 *For every $n \geq 2$, $d \geq 1$, and $k > d$,*

$$C_{d,k}^{(n)} = 0 \Leftrightarrow k = d+1.$$

Theorem 2 *For every $d \geq 0$ and $k \geq d$,*

$$\lim_{n\to\infty} C_{d,k}^{(n)} = 0 \Leftrightarrow k \leq 2d.$$

*This work was supported in part by a JSPS Fellowship for Young Scientists and by the National Science Foundation.

References

[1] N. J. Calkin and H. S. Wilf, "The Number of Independent Sets in a Grid Graph," *SIAM J. on Discrete Mathematics*, vol. 11, February 1998, pp. 54–60.

[2] S. Forchhammer and J. Justesen, "Bounds on the Capacity of Constrained 2d Codes," preprint.

[3] K. A. Immink, P. H. Siegel, and J. K. Wolf, "Codes for Digital Recorders," *IEEE Trans. Inform. Theory*, vol. 44, pp. 2260–2299, October 1998.

[4] H. Ito, A. Kato, Zs. Nagy, and K. Zeger, "Zero Capacity Region of Multidimensional Run Length Constraints," *The Electronic Journal of Combinatorics*, vol. 6, no. 1, 1999, # R33. (http://www.combinatorics.org/Volume_6/Abstracts/v6i1r33.html).

[5] A. Kato and K. Zeger, "On the Capacity of Two-Dimensional Run Length Constrained Channels," *IEEE Trans. Inform. Theory*. vol. 45, no. 4, July 1999, pp.1527–1540.

[6] D. Lind and B. H. Marcus, *An Introduction to Symbolic Dynamics and Coding*, Cambridge University Press, New York, 1995.

[7] Zs. Nagy and K. Zeger, "Capacity Bounds for the 3-Dimensional (0,1) Runlength Limited Channel," *to appear in IEEE Trans. Inform. Theory.*

[8] R.M. Roth, P.H. Siegel, and J.K. Wolf, "Efficient Coding Schemes for the Hard-Square Model," *IEEE Trans. Inform. Theory*, (submitted October 1999).

[9] P. H. Siegel and J. K. Wolf, "Bit Stuffing Bounds on the Capacity of 2-Dimensional Constrained Arrays," *Proceedings of 1998 IEEE International Symposium on Information Theory*, Boston, MA, August 1998, p. 323.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Upper Bound on the Capacity of Constrained Three-Dimensional Codes

Søren Forchhammer
Dept. of Telecommunication, 371
Technical University of Denmark
DK-2800 Lyngby, Denmark
e-mail: sf@tele.dtu.dk

Abstract — **An upper bound on the capacity of constrained three-dimensional codes is presented. The bound for two-dimensional codes of Calkin and Wilf was extended to three dimensions by Nagy and Zeger. Both bounds apply to first order symmetric constraints. The bound in three dimensions is generalized in a weaker form to higher order and non-symmetric constraints.**

I. Introduction

In this paper we consider the capacity of constrained three-dimensional (3-D) codes defined by a set of constraints. We consider shift invariant constraints of finite extent (N, M, L), in the sense that the constraints may be defined on an N by M by L volume. Each element is taken from an alphabet A of size $|A|$. The $|A|^{NML}$ possible configurations on the volume are divided into a set of admissible and a set of non-admissible configurations. Let $F(n, m, l)$ be the number of distinct admissible configurations (or codewords) on an n by m by l volume not violating the constraints within the volume. The per symbol capacity (or maximum entropy), $C^{(3)}$ of the 3-D code defined by the constraints may be defined as:

$$C^{(3)} = \lim_{n,m,l\to\infty} \frac{\log F(n,m,l)}{nml}. \quad (1)$$

A more formal treatment of the entropy definition and its existence is given in [1].

Calkin and Wilf [2] presented a method giving tight bounds on capacity for the (hard square) 2-D constraint, with binary elements, specified by that for any two 4-neighbors, i.e. horizontal and vertical neighbors, both of them can not be '1'. The upper bound [2] is based on

$$\Lambda \le Trace(\mathbf{T}^{2p})^{1/2p}, p > 0. \quad (2)$$

where Λ is the largest eigenvalue of $\mathbf{T}$. (2) is valid for real symmetric matrices and it is applied to the transfer matrix of the constraint in one direction. Nagy and Zeger [3] extended the results to the 3-D version of the constraint above. (Two direct neighboring '1's in the direction of the third axis is also non-admissible.) Let D denote the dimension of the constraint. Their methods may be applied to other constraints, but they are restricted to constraints for which the transfer matrices are symmetric in at least $D-1$ directions. This is satisfied for constraints which are of 1st order and symmetric in (at least) all but one direction. Here we address the problem of bounding capacity for higher order and non-symmetric constraints in 3-D, eg. limits on run-lengths or distances (≥ 3).

II. Upper bound for higher order 3-D constraints

In order to achieve an upper bound we shall specify a source which has the required symmetric transfer matrices and as a subset can generate all configurations admissible by the original constraint. In [4] we presented a way to do this in 2-D. Extending to 3-D leads to the following construction. The states are defined by the admissible configurations within 4 sub-states, which are rectangular boxes of equal size. The sub-states forming one state must have the same boundary configuration of width $M-1$ in the m-direction and $L-1$ in the l-direction. The states extend $N-1$ in the n-direction. The admissible transitions between the combined states in all generating s_1 by s_2 distinct elements are specified by $\mathbf{G}_{s_1,s_2}$. The transitions are admissible iff the transitions of the 4 sub-states are.

Theorem 1: The capacity of a 3-D code specified by shift invariant constraints of finite extent (N, M, L), has the upper bound

$$C^{(3)} \le \frac{H''(s_1,s_2)}{s_1 s_2} \quad (3)$$

where H'' is the capacity determined by the logarithm of the largest eigenvalue of $\mathbf{G}_{s_1,s_2}$ of the given constraint. s_1 and s_2 are positive even integers.

The principles of the proof is as follows. (2) is applied first in one and then in another direction as in [3]. We need to ensure that the matrices are symmetric. Given a non-symmetric transfer matrix $\mathbf{T}$ (in one direction), introduce $\mathbf{A} = \mathbf{T}^p$ and the symmetric matrix $\mathbf{C} = \mathbf{A}+\mathbf{A}^*$, where * denotes the transpose. Applying (2) to $\mathbf{C}^2$, the bound is assymptotically dominated by $Trace(\mathbf{A}\mathbf{A}^*)$. $\mathbf{A}^*$ may be described as the reverse transition of $\mathbf{A}$. So the trace counts configurations which are given by two transitions starting and ending in the same state. Used in two directions leads to the construction above and $\mathbf{G}_{s_1,s_2}$.

We expect to achieve improved numerical results using (3) in 3-D as we did in 2-D [4] using the same approach to derive symmetric transfer matrices generating all admissible configurations as a subset.

References

[1] S. Friedland, "On the entropy of Z^d subshifts of finite type," *Linear Algebra Appl.*, vol. 252, pp. 199–220, 1997.

[2] N. J. Calkin and H. S. Wilf, "The number of independent sets in a grid graph," *SIAM Journal of Discrete Mathematics*, vol. 11, no. 1, pp. 54–60, Feb. 1998.

[3] Z. Nagy and K. Zeger, "Capacity Bounds for the 3-dimensional (0,1) Runlength Limited Channel," to appear *IEEE Trans. Inform. Theory.*

[4] S. Forchhammer and J. Justesen, "An upper bound on the entropy of constrained 2d fields," *Int'l Symp. Inform. Theory*, MIT, p. 72, 1998.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Space-Time Codes Based on Hadamard Matrices

Martin Bossert
University of Ulm
Dept. of Information Technology
Albert-Einstein-Allee 43
89081 Ulm, Germany
e-mail:
boss@it.e-technik.uni-ulm.de

Ernst M. Gabidulin
Moscow Institute of Physics and Technology
Dept. of Radio Engineering, Head
Institutskii per., 9
141700 Dolgoprudny, Russia
e-mail: gab@pop3.mipt.ru

Paul Lusina
University of Ulm
Dept. of Information Technology
Albert-Einstein-Allee 43
89081 Ulm, Germany
e-mail:
lusina@it.e-technik.uni-ulm.de

Abstract — **The Hadamard matrix structure is applied to the construction of space-time codes. Space-time Hadamard (STH) codes are statistically analyzed with respect to diversity and coding gain criteria and are shown to have good statistical properties.**

I. Introduction

Two design criteria are derived for space-time codes in [1]. The performance gain is shown to be dependent on the minimum rank and the minimum sum of eigen values based on codeword difference matrices. Present code designs consist of orthogonal block constructions [2], [3] which maximize the rank, and empirically constructed convolutional codes or codes found using exhaustive search algorithms. The challenge in finding a space-time code construction is complicated because the codes exist in an infinite complex field instead of a finite real field. STH codes offer a flexible design construction which produces statistically good codes.

II. Space-Time Hadamard (STH) Code Construction

[1] shows that for the codeword matrix difference $\mathbf{c} - \widetilde{\mathbf{c}}$, maximizing the rank corresponds to maximizing the rate that the BER decreases. This is the dominant gain criterion for asymptotic E_b/N_0. Space-time Hadamard code construction (STH codes) is based on Hadamard matrices H_n of order $m = 2^n$. These codes are designed to give statistically good rank properties which improve with increasing constellation size, and code length. STH codes can be recursively constructed as follows

$$H_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

$$H_n = \begin{pmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{pmatrix}, \; n = 2, 3, \ldots,$$

Let $\Lambda_{n+1} = diag(\lambda_1, \lambda_2, \ldots, \lambda_{2^{n+1}})$ be a diagonal matrix of eigen values of the codeword $\mathbf{c}$. The recursive codeword matrix is $W^{(n+1)}(l) = 2^{-(n+1)} H_{n+1} \Lambda_{n+1} H_{n+1}$. l corresponds to the order of the direct sum extension of STH codes where $W^n(l)$ has dimensions $n \times l \cdot n$. Denote $\Lambda_n^{(1)} = diag(\lambda_1, \lambda_2, \ldots, \lambda_{2^n})$, $\Lambda_n^{(2)} = diag(\lambda_{2^n+1}, \lambda_2, \ldots, \lambda_{2^{n+1}})$. Then

$$\Lambda_{n+1} = \begin{pmatrix} \Lambda_n^{(1)} & \mathbf{0} \\ \mathbf{0} & \Lambda_n^{(2)} \end{pmatrix}$$

and

$$W^{(n+1)}(1) = 2^{-n=1} H_{n+1} \Lambda_{n+1} H_{n+1}$$

$$= 2^{-(n+1)} \begin{pmatrix} H_n(\Lambda_n^{(1)} + \Lambda_n^{(2)}) H_n & H_n(\Lambda_n^{(1)} - \Lambda_n^{(2)}) H_n \\ H_n(\Lambda_n^{(1)} - \Lambda_n^{(2)}) H_n & H_n(\Lambda_n^{(1)} + \Lambda_n^{(2)}) H_n \end{pmatrix}.$$

The factor $2^{-(n+1)}$ is a normalization factor. The symmetric matrix has the first row

$$(w_1, w_2, \ldots, w_{2^{n+1}}) = 2^{-(n+1)} (\lambda_1, \lambda_2, \ldots, \lambda_{2^{(n+1)}}) H_{(n+1)}.$$

All other rows are permutations of the first row.

The basic structure of STH codes can be modified to give different code parameters. By selecting a subset of T columns of the codeword matrix, we obtain the *T-reduced STH* code. By taking the direct sum of several STH matrices, we obtain *extended STH* codes where $l > 1$.

III. Statistical Properties

Table 1 shows that as the constellation size and/or the extension order l increases, the fraction of full rank codewords approaches 1. Statistical analysis shows that as the rank decreases, the eigen value sum increases, which also produces a performance gain. Statistically good codes can be constructed for small constellations and code sizes.

Table 1: Rank statistics for STH codes $W^{(1)}(l)$ over different constellations.

q	% rank 1, $l = 1$	% rank 1, $l > 1$
4	16.7	$\approx 2 \times 10^{2-0.55l}$
8	5.2	$\approx 2 \times 10^{2-0.8l}$
16	1.4	$\approx 2 \times 10^{2-1.1l}$

IV. Conclusions

The STH code construction is presented and evaluated based on the rank and eigen value design criteria [1]. This code construction shows good statistical properties. The basic construction can be adapted to give different code parameters. The code properties improve with the code length and constellation size.

References

[1] V. Tarokh, H. Jafarkhani, and A.R. Calderbank, "Space-Time Codes for High Data Rate Wireless Communication: Performance Criterion and Code Construction," *IEEE Trans. on Information Theory*, vol. 44, No.2, pp. 744 - 765, March 1998.

[2] V. Tarokh, H. Jafarkhani, and A.R. Calderbank, "Space-Time Block Codes from Orthogonal Designs, " *Trans. on Information Theory*, vol. 45, No.5, July 1999.

[3] S. M. Alamouti, "A Simple Transmit Diversity Technique for Wireless Communications," *IEEE J. Select. Areas. Commun.*, vol. 16, No.8, pp. 1451 - 1458, October 1998.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Space-Time Codes Based on Rank Codes

Ernst M. Gabidulin
Moscow Institute of Physics and Technology
Dept. of Radio Engineering, Head
Institutskii per., 9
141700 Dolgoprudny, Russia
e-mail: gab@pop3.mipt.ru

Martin Bossert
University of Ulm
Dept. of Information Technology
Albert-Einstein-Allee 43
89081 Ulm, Germany
e-mail:
boss@it.e-technik.uni-ulm.de

Paul Lusina
University of Ulm
Dept. of Information Technology
Albert-Einstein-Allee 43
89081 Ulm, Germany
e-mail:
lusina@it.e-technik.uni-ulm.de

Abstract — **The application of Maximum Rank Distance (MRD) codes is investigated with respect to the space-time code scenario. A construction method is presented based on primitive polynomials over extended Galois fields. A one-to-one mapping is then performed between the Galois field code symbols and the complex transmission symbols.**

I. Introduction

In [2] the design criteria for space-time codes was derived which showed that for asymptotic E_b/N_0, the rate of performance gain was dominated by the minimum rank of the codeword difference matrices (*diversity gain*). Present space-time constructions include the class of orthogonal space-time codes, where all codeword matrix columns are mutually orthogonal and convolutional space-time codes which are constructed by hand or found through exhaustive searches. Both types of codes seek to maximize the minimum rank over the set of all codeword differences.

The rank code construction based on [1] is applied to space-time codes. The codeword rank is maximized to give maximum rank distance (MRD) codes. This results in a new design technique for space-time code construction.

II. MRD Code Construction

We define the matrix primitive polynomial as

$$f(x) = x^T + b_{T-1}x^{T-1} + b_{T-2}x^{T-2} + \ldots + b_1 x + b_0, \quad (1)$$

where $b_i \in GF(q)$, $i = 0, 1, \ldots, T-1$ with the restriction that $b_T = 1$. $\beta \in GF(q)$ is a primitive element such that $f(\beta) = 0$. Furthermore, let $p(x)$ be the element primitive polynomial for the extension field $q = p^s$:

$$p(x) = x^s + a_{s-1}x^{s-1} + a_{s-2}x^{s-2} + \ldots a_1 x + a_0, \quad (2)$$

where $a_i \in GF(p)$, $i = 0, 1, \ldots, s-1$ with the restriction that $a_s = 1$. α is a primitive element of $GF(p)$ such that $p(\alpha) = 0$ and p is a prime number. The associated (primitive) matrix $\mathbf{C}$ constructed from $f(\beta)$ is written as

$$\mathbf{C} = \begin{pmatrix} 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ b_0 & b_1 & \cdots & b_{T-1} \end{pmatrix}$$

The elements b_i can be represented in terms of α based on equation 2. This primitive matrix has analogous properties to primitive elements for vector fields.

The resulting $T \times T$ matrices

$$\mathcal{C} = \{\mathbf{0}, \mathbf{C}, \mathbf{C}^2, \ldots, \mathbf{C}^{q^T-2}, \mathbf{C}^{q^T-1}\} \quad (3)$$

define an MRD code of cardinality q^T with rank distance T. Furthermore, these codes are linear [1].

We now map the $GF(q)$ elements to a complex signal constellation. Let $\mathcal{A}_C$ be a complex signal constellation of size q. Define a one-to-one map $\mathcal{A}_{GF(q)} \Longleftrightarrow \mathcal{A}_C$. If $GF(q) = \{\alpha^{-\infty} = 0 \cup \alpha^i,\ i = 0, 1, \ldots, q-2\}$ and $|\mathcal{A}_C| = q$ then we define the following mapping $0 = \alpha^{-\infty} := \gamma_{\alpha^{-\infty}}$ and $\alpha^i := \gamma_{\alpha^i}$, $i = 0, 1, \ldots, q-2$.

Consider an MRD code $\mathcal{C}$ of $T \times T$ matrices with rank distance T generated by equation (3). We replace every element of $GF(q)$ by the corresponding element from the constellation $\mathcal{A}_C$ using the defined mapping. This gives the code $\mathcal{C}(\mathcal{A}_C)$ over the constellation $\mathcal{A}_C$. For a given constellation, we have to verify whether the resulting code is MDR.

III. Search Results for MRD codes.

The authors have found that the mapping from $GF(2)$ MRD codes to any complex binary constellation produces complex MRD codes. For the 2×2, $GF(2^2)$ MRD code, it has been shown that the 4 PSK constellation produces a complex MRD code.

We note that the complex MDR code space is a finite subset of an infinite complex space. The challenge is in finding a modulation alphabet which produces complex MDR code, and which is still practical for an information system.

IV. Conclusions

The matrix rank of codewords is maximized to give maximum rank distance (MRD) codes. These codes are first constructed in $GF(q)$ and then mapped to a complex signal constellation. The properties of the chosen signal constellation determines the resulting code which may no longer be MRD. MRD codes exist for all binary constellations, and for the 2×2 MDR code over 4 PSK.

References

[1] E.M.Gabidulin, "Theory of Codes with Maximum Rank Distance," *Problems of Information Transmission*, v. 21, No. 1, pp. 3-14, 1985.

[2] V. Tarokh, H. Jafarkhani, and A.R. Calderbank, "Space-Time Codes for High Data Rate Wireless Communication: Performance Criterion and Code Construction," *IEEE Trans. on Information Theory*, vol. 44, No.2, pp. 744 - 765, March 1998.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Extensions to the Theory of Differential Space-Time Modulation

Brian L. Hughes[1]
Center for Advanced Computing and Communication
Department of Electrical and Computer Engineering
North Carolina State University
Raleigh, NC 27695-7914
e-mail: blhughes@eos.ncsu.edu

Abstract — **Recently, a general approach to differential modulation for multiple transmit and receive antennas was proposed by Hughes, and by Hochwald and Sweldens. In this approach, data are differentially encoded using a restricted class of space-time group codes in which each code matrix is square and has equal-energy, orthogonal rows. In this talk, we remove the restrictions imposed in earlier work and extend the theory of differential transmission to arbitrary Slepian-type group codes. This extension leads to new modulation techniques that significantly outperform previously known methods, both for single and multiple antenna systems. Applications to universal channel coding for discrete memoryless channels are also discussed.**

I. Summary

In wireless communication, fading due to multipath signal propagation often has a severe impact on system performance. One way to improve performance is to increase diversity through the use of multiple antennas at the transmitter and/or receiver. Modulation techniques designed for multiple transmit antennas — called *space-time modulation* or *transmit diversity* — have been shown to be highly effective in reducing the effects of fading, and can also dramatically increase the capacity of multipath radio channels, especially when combined with multiple antennas at the receiver.

In recent years, a wealth of space-time coding and modulation techniques have been proposed. Most early work focused on the coherent case, when accurate channel estimates are available at the receiver but not the transmitter. More recently, there has also been considerable interest in the noncoherent case, when channel estimates are not available at the transmitter or receiver. In this case, Marzetta and Hochwald [3] have shown that, for large signal-to-noise ratios, the capacity of a multi-antenna quasi-static Rayleigh fading channel is approached by unitary space-time block codes, in which the signals transmitted by different antennas have equal energy and are mutually orthogonal.

Recently, Hughes [2] and Hochwald and Sweldens [1] independently proposed a general approach to differential modulation for multiple transmit and receive antennas (see [4, 5] for other approaches). In this approach, data are differentially encoded using a restricted class of space-time group codes in which each code matrix is square and has equal-energy, orthogonal rows.

[1]This work was supported in part by the National Science Foundation under grant CCR-9903107, and by the Center for Advanced Computing and Communication.

In this talk, we remove the restrictions imposed in earlier work and extend the theory of differential transmission to arbitrary Slepian-type group codes. For a system with t transmit antennas, we consider block codes in which each code matrix is of the form

$$C = DG ,$$

where D is a fixed $t \times n$ complex matrix, and where G belongs to an algebraic group $\mathcal{G}$ of $n \times n$ unitary matrices ($GG^\dagger = I$). Here, the rows of C represent symbols transmitted by different antennas, and the columns represent symbols transmitted at different times. Using this code, a sequence of messages $G_k \in \mathcal{G}$ can be differentially encoded in a way similar to differential PSK: At time $k = 0$ we send the block $C_0 = D$ to initialize transmission. Thereafter, to send message G_k in block k, we send

$$C_k = C_{k-1}G_k , \; k = 1, 2, \ldots$$

The group property ensures that $C_k \in D\mathcal{G}$ for all k.

In this work, we consider transmission of the differentially encoded sequence C_k over a flat-fading Rayleigh channel in the presence of additive Gaussian noise. We derive a differential receiver that reliably recovers G_k without knowledge of current channel fading conditions. We further derive a bound on the error probability of this receiver as well as modulator design criteria. The design criteria lead to new differential modulation techniques for both single and multiple antenna channels that significantly outperform the best codes in [1, 2]. Extensions to universal channel coding for discrete memoryless channels are also discussed.

References

[1] B. M. Hochwald and W. Sweldens, "Differential unitary space-time modulation," submitted to *IEEE Trans. on Commun.*, 1999.

[2] B. L. Hughes, "Differential space-time modulation," submitted to *IEEE Trans. on Inform. Theory*, 1999. Also *Proc. IEEE Wireless Networking and Communications Conf. (WCNC '99)*, vol.1, pp. 145-149, Sept. 1999.

[3] T. L. Marzetta and B. M. Hochwald, "Capacity of a mobile multiple-antenna communication link in Rayleigh flat-fading," *IEEE Trans. Inform. Theory*, vol. 45, no. 1, pp. 139-157, Jan. 1999.

[4] V. Tarokh and H. Jafarkhani, "A differential detection scheme for transmit diversity," to appear in *IEEE J. Sel. Areas Commun.*, 2000.

[5] D. Warrier and U. Madhow, "Noncoherent communication in space and time," submitted to *IEEE Trans. Inform. Theory*, 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Concatenation of Error-Correcting Codes and Multiple Transmit Antennas

Xiaodong Li, Harish Viswanathan, and Howard Huang
Bell Labs, Lucent Technologies
791 Holmdel-Keyport Road
Holmdel, NJ 07733, USA

Abstract — **Many wireless systems today employ error correcting coding. Adding transmit diversity may further improve the performance. We study the options to achieve the goal without significant change to the existing systems.**

I. Introduction

Transmit diversity is an effective technique to mitigate channel fading in wireless communication systems. Many space-time coding (STC) techniques have been suggested to provide transmit diversity [1, 2].

Most modern wireless systems employ forward error-correcting coding (FEC). Providing additional transmit diversity to such systems is of practical interest and also challenging. In this paper, we study several possible techniques to achieve the diversity gain.

II. Combination of FEC and Antenna Hopping

One simple way to achieve transmit diversity for coded systems is to use the Alamouti STC scheme [3]. A possibly simpler method is to use antenna hopping [4]. The coded bits from the FEC encoder are first interleaved and then transmitted alternately, in bursts, through multiple transmit antennas.

Without coding this scheme clearly provides no diversity. The bit-error rate can be very high if the path from any antenna is in a deep fade. However, coding groups together many symbols with potentially different fading levels into one codeword. For a powerful FEC code with large free Hamming distance, diversity combining can take place during the calculation of codeword metrics for maximum likelihood decoding.

To obtain more insight, we consider the pairwise error probability between a pair of codewords with Hamming distance d, for a two-antenna system. We assume that each bit can be transmitted from either antenna equally likely. Then the probability that a total of k out of d bits are transmitted from antenna 1 is of a binomial distribution $\binom{d}{k}0.5^d$. For Rayleigh channels with AWGN, we obtain an upper bound on the average pairwise error probability (APEP) for a two-antenna system

$$\text{APEP} \leq 0.5^d \sum_{k=0}^{d} \binom{d}{k} \frac{1}{1+\frac{kE_s}{N_0}} \frac{1}{1+\frac{(d-k)E_s}{N_0}}, \quad (1)$$

where E_s is the energy per symbol and N_0 is the noise density. For large d, a diversity order of two is achieved with high probability. We will show that the bounds for antenna hopping and the Alamouti scheme are quite close for large d. Calculation of channel cutoff rate also shows that the performance of the two schemes is close. Note that the binomial distribution is a conservative estimation. For practical coding schemes, a simple (even-odd) hopping can often ensure a diversity order two.

For a large number of transmit antennas, it is difficult to design STC based on orthogonal design [2]. In this case, we can combine antenna hopping with STC. For example, we can partition four antennas into two two-antenna groups. The interleaved FEC output is switched alternately, in bursts, to the two groups. In each group, a STC is used for the two antennas. With this method, more transmit antennas can be used to increase the diversity order.

In Figure 1, we compare the performance of FEC concatenated with a single antenna, two-antenna (even-odd) hopping, and two-antenna STC, four-antenna hopping, group hopping with two-antenna STC, and a *hypothetical* four-antenna STC. The FEC code is a rate-1/3 parallel concatenated convolutional (turbo) code with 16-state component codes.

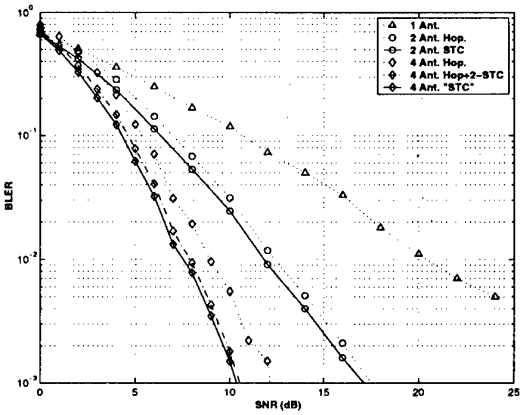


Figure 1: Performance of turbo-coded BPSK over block Rayleigh fading channels.

III. Other Concatenation Methods

We will also discuss the design of and show results for space-time turbo coding and other trellis based methods.

References

[1] S. M. Alamouti, "A simple transmitter diversity scheme for wireless communications", *IEEE J. Select. Areas Commun.*, vol. 16, pp. 1451-1458, Oct. 1998.

[2] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Space-time block codes from orthogonal designs", *IEEE Trans. on Inform. Theory*, vol. 45, pp. 1456-1467, July 1999.

[3] S. M. Alamouti, V. Tarokh, and P. Poon, "Trellis-coded modulation and transmit diversity: design criteria and performance evaluation", *ICUPC'98.*

[4] H. Olofsson, M. Almgren, and M. Hook, "Transmitter diversity with antenna hopping for wireless communication systems", *VTC'97.*

0-7803-5857-0/00/$10.00 ©2000 IEEE.

An Algorithm to Compute the Free Distance of Turbo Codes

Roberto Garello *, Paola Pierleoni *, Sergio Benedetto **, Guido Montorsi **

* Dipartimento di Elettronica ed Automatica
Università di Ancona, Italy
e-mail: roberto.garello@ieee.org

** Dipartimento di Elettronica
Politecnico di Torino, Italy
e-mail: benedetto@polito.it

Abstract — **A new algorithm for computing the free distance of turbo codes is applied to the CCSDS and the UMTS standard codes. Results on the free distance behaviour for increasing interleaver length are also presented.**

I. Introduction

It is known that turbo codes may have low free distances d_{free}, despite of very large interleaver lengths N. This causes their BER curves to flatten following the "error floor" imposed by d_{free}, after the "water-fall" decrease at low signal-to-noise ratios. This behaviour may be not admissible for applications requiring very low Bit Error Rates (BER $\leq 10^{-8} - 10^{-10}$). In [1] we have developed a new algorithm for computing the free distance d_{free} of parallel and serially concatenated codes with interleavers, based on the new notion of constrained subcodes. The algorithm permits to compute large distances without constraint on the input sequence weight. Since d_{free} and its multiplicity dominate the code performance at very high signal-to-noise ratios, their knowledge allows to analytically estimate the code error floor, *i.e.*, the code performance for very low probabilities where simulation is not feasible.

As a first example of application, we present some results concerning the free distance behaviour for turbo codes with growing interleaver length. They provides some information on these two issues: (i) the improvement in terms of error floor potentially available by increasing the interleaver length, and (ii) the probability of choosing at random an "optimal" (in terms of d_{free}) interleaver of a certain length. In Fig. 1 we report the behaviour of the best and the average free distance for 16-state rate-1/3 turbo codes, obtained by randomly generating a very large number of turbo codes and evaluating their free distance.

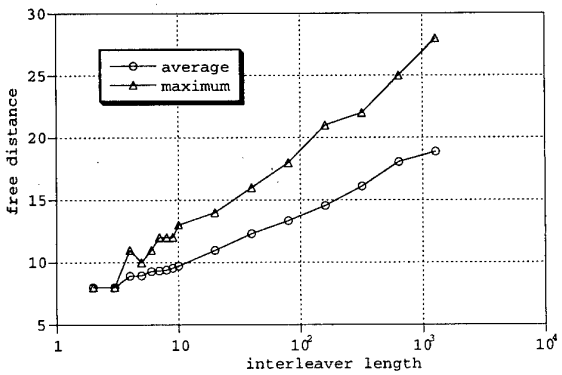


Fig. 1: Distribution of d_{free} for 16-state rate-1/3 turbo codes.

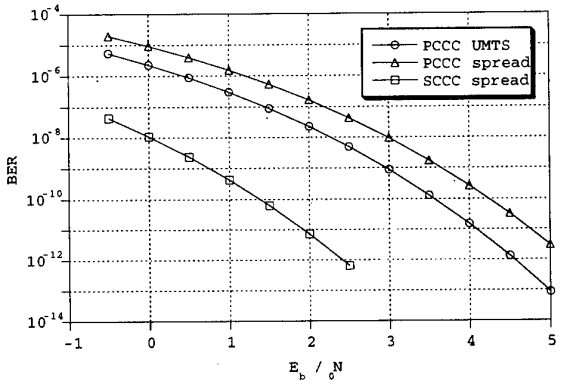


Fig. 2: The error floors for the Bit Error Rates of the rate-1/3 UMTS turbo code and the other two codes.

II. Application 1: the CCSDS standard

Recently, the CCSDS telemetry channel coding standard has been updated for including turbo codes. They consist of the parallel concatenation of two 16-state rate-1/4 binary convolutional encoders and a block Berrou's analytical interleaver with length N =1784, 3568, 7136, 8920, or 16384. Four nominal code rates $1/r$, for r = 2, 3, 4, and 6, can be obtained through puncturing.

We have successfully applied our new algorithm to the whole class of CCSDS turbo codes with N = 1784. By denoting with $(d_{\text{free}}/N_{\text{free}}/w_{\text{free}})$ their free distance, multiplicity, and input bit multiplicity, the results are (17/2/6), (32/1/2), (42/1/2), and (70/1/2) for r = 2, 3, 4, and 6, respectively.

III. Application 2: the UMTS standard

The UMTS/3GPP standard for third generation personal communications will use a turbo code. Its encoder consists of the parallel concatenation of two 8-state rate-1/2 binary convolutional encoders and a block interleaver with length N, with $320 \leq N \leq 5120$. Two nominal rates $1/r$, with $r = 2$ and 3, can be obtained through puncturing. For the rate-1/3 code with $N = 320$, we have applied the new algorithm and obtained $d_{\text{free}} = 24$, $N_{\text{free}} = 1$ and $w_{\text{free}} = 4$. For comparison, we have considered the classes of 8-state parallel concatenated codes (PCCC) and 4-state serially concatenated codes (SCCC) employing spread interleavers. At best, we have obtained two codes yielding (21/2/6) and (38/1/2), respectively. The error floors for these three codes are depicted in Fig. 2. We can observe that the UMTS turbo code has very good performance at very low BER, better than the best PCCC spread found, even if a SCCC could overcome it.

References

[1] R. Garello, P. Pierleoni, S. Benedetto. "Computing the free distance of turbo codes and serially concatenated convolutional codes: algorithms and applications", *to be submitted.*

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Upper bounds to error probabilities of coded systems beyond the cutoff rate

Dariush Divsalar* and Ezio Biglieri
Jet Propulsion Laboratory, 4800 Oak Grove Drive, Pasadena, CA. Politecnico di Torino, Italy
e-mail: dariush@shannon.jpl.nasa.gov, biglieri@polito.it

Abstract — **New upper bounds to error probabilities of coded systems such as turbo codes on the additive white Gaussian noise and fading channels were obtained.**

I. A New Bound for AWGN Channels

For binary (n, k) block codes which include turbo and serial codes the bit and word error probabilities using a technique in [1] can be bounded by [2]

$$P_e \le \sum_{h=h_{min}}^{n-k+1} \min\left\{e^{-nE(c,h)}, e^{nr(\delta)} Q(\sqrt{2\,c\,h})\right\}$$

where

$$E(c,h) = \frac{1}{2}\ln[1-2c_0(\delta)f(c)] + \frac{cf(c)}{1+f(c)}, \quad c_0(\delta) < c < \frac{e^{2r(\delta)}-1}{2\delta(1-\delta)},$$

otherwise $E(c,h) = -r(\delta) + \delta c$. Also $\delta = h/n$, $c = R_c \frac{E_b}{N_o}$, $c_0(\delta) = (1-e^{-2r(\delta)})\frac{1-\delta}{2\delta}$, and $f(c) = \sqrt{c/c_0 + 2c + c^2} - c - 1$. For bit error probability $r(\delta) \triangleq \frac{1}{n}\ln\sum_w \frac{w}{k} A_{w,h}$ ($A_{w,h}$ is the input-output weight distribution), and for word error probability $r(\delta) \triangleq \frac{1}{n}\ln A_h$ (A_h is the output weight distribution). This is the tightest "closed form" upper bound on decoding error rate. The minimum E_b/N_o threshold can be computed as $(E_b/N_o)_{\text{threshold}} = \max_\delta c_0(\delta)/R_c$. In [2] we proved that the threshold for Poltyrev bound (see [3] and references there) is the same as our threshold, thus the proposed bound is as tight as Poltyrev bound for very large blocksize n. The simple bound for AWGN channel is applied to obtain the ML performance of rate 1/4 Repeat Accumulate (RA) codes as in Fig. 1. Also in the Figure the performance of suboptimum iterative turbo decoder for RA codes are shown.

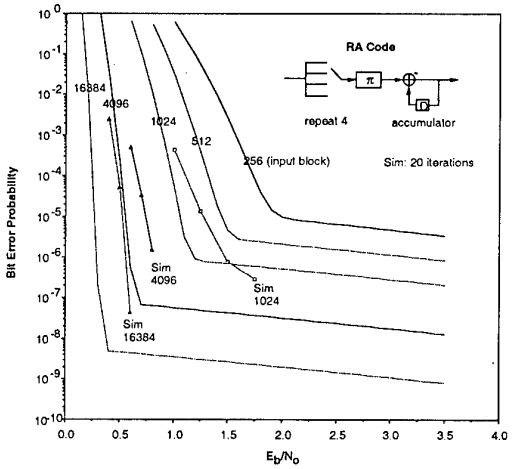


Figure 1: ML upperbound on the bit error probability of a rate 1/4 RA codes over AWGN Channel

*The work described was funded by the TMOD Technology Program and performed at the Jet Propulsion Laboratory, California Institute of Technology under contract with the National Aeronautics and Space Administration.

II. A New Bound for Fading Channels

For independent Rayleigh fading with CSI

$$P_e \le \sum_{h=h_{min}}^{n-k+1} \min\left\{e^{-nE(c,h)}, e^{nr(\delta)} \frac{1}{\pi}\int_0^{\frac{\pi}{2}} \left[\frac{sin^2\theta}{sin^2\theta + c}\right]^h d\theta\right\}$$

where

$$\begin{aligned} E(c,h) = \max_{\rho,\beta,r,\phi}\Bigg\{ & -\rho r(\delta) + \frac{\rho}{2}\ln\frac{\beta}{\rho} + \frac{1-\rho}{2}\ln\frac{1-\beta}{1-\rho} \\ & + \rho\delta\ln[1+c(1-2r\phi)] \\ & + \rho(1-\delta)\ln\left[1+c\left(1-2r\phi-\frac{(1-r)^2\rho}{\beta}\right)\right] \\ & + (1-\rho)\ln\left[1+c\left(\frac{1-\rho(1-2r\phi)}{1-\rho} - \frac{(1-\rho(1-r))^2}{(1-\rho)(1-\beta)}\right)\right]\Bigg\} \end{aligned}$$

δ, c, and $r(\delta)$ are defined as in the previous section. The maximum with respect to ϕ can be obtained in a closed-form, then the remaining maximizations must be performed numerically. The simple bound for Rayleigh fading channel is applied to obtain the ML performance of rate 1/4 Repeat Accumulate (RA) codes as in Fig. 2. Also in the Figure the performance of suboptimum iterative turbo decoder for RA codes over independent Rayleigh fading with CSI are shown.

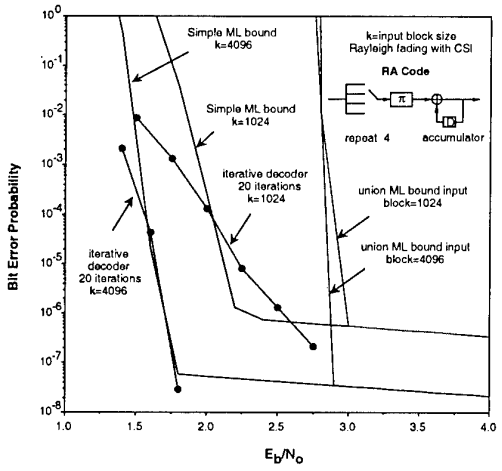


Figure 2: ML upperbound on the bit error probability of rate 1/4 RA codes for Rayleigh fading channel

References

[1] R. G. Gallager, *Low Density Parity Check Codes*. Cambridge, MA: MIT Press, 1963.

[2] D. Divsalar, "A simple tight bound on error probability of block codes with application to turbo codes," Jet Propulsion Laboratory TMO progress report 42-139, November 15, 1999.
http://tmo.jpl.nasa.gov/tmo/progress_report/

[3] I. Sason and S. Shamai, "Improved upper bounds on the ML decoding error probability of parallel and serial concatenated turbo codes via their ensemble distance spectrum,"*the IEEE Trans. on Information Theory* , January 2000.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

An Upper Bound on the Number of Errors Corrected by a Convolutional code

Jørn Justesen
Department of Telecommunication
Technical University of Denmark, Building 371
DK-2800 Lyngby, Denmark
e-mail: jju@tele.dtu.dk

Abstract - **The number of errors that a convolutional codes can correct in a segment of the encoded sequence is upper bounded by the number of distrinct syndrome sequences of the relevant length.**

I. Introduction

We shall analyse the error correcting power of a convolutional code by relating the number of correctable errors to the available syndromes. The results are related to the bound in [1], but we take a more direct approach. Syndromes for convolutional codes have not received much attention since the structural results appeared in [2]. The main difficulty compared to block codes, is that different sequence lengths have to be considered. Even though a Hamming type upper bound usually cannot be reached, it is an important estimate of the number of errors that can be corrected with high probability by a typical code.

II. Correctable Errors for Short Sequences

In [3] a general method for relating bounds for block codes to convolutional codes was introduced. Thus an upper bound on the number of errors that can be corrected independent of their location, t_0 , may be derived from the Hamming bound for block codes. However, a direct analysis of errors and syndromes in convolutional codes gives a tighter bound, since some error patterns give rize to short syndromes.

Theorem 1: If a binary (n,k) convolutional code with encoder memory M (blocks) and syndrome former memory M' corrects all combinations of t_0 errors, the inequality

$$\sum \binom{ns}{j} c(j) \le 2^{(n-k)(s+M')}$$

is satisfied for any s>M and $j \le t_0$. Here c(j) is the number of truncated codewords of weight j.

The bound will be applied to examples of short high rate codes, and we shall demonstrate how the factor c(j) makes the bound sharper than the translated Hamming bound. It is essential to the performance of convolutional codes that the number of correctable errors increases with the length of the sequence. Thus we are interested in the number of errors, t_j , that can be corrected in a sequence of length j blocks, provided that no more than t_0 errors occur in a sequence of length j-1. This approach may be extended to yield a description of distributions of correctable errors in short sequences.

III. A Variable Length Description of Errors

An obvious question about a convolutional code is, how often can a burst of t_0 errors be corrected? Our first approach above does not give a convenient answer to questions of this type, since the syndromes are simply assumed to be zero outside the window under consideration. Thus we seek a rule for segmenting the error pattern into finite strings in such a way that any concatenation of correctable strings form a correctable error sequence. This gives a variable length description of the correctable error patterns which may be related to a segmentation of the syndrome sequence. The segments may be mapped on the leaves of a tree where the branches are labeled by the syndrome bits.

IV. An Upper Bound by the Kraft Inequality

We may obtain a Hamming type upper bound by relating the error sequence and the syndrome sequence through a version of Kraft's inequality:

Theorem 2: For a tree of correctable error patterns, the number of paths of length L (blocks) is A(L). Then the number of check symbols per block, r, must satisfy

$$\sum A(L)\ 2^{rL} \le 1$$

This version of the upper bound indicates that for short codes there is a trade-off between a high value of t_0 and a rapid increase in the number of correctable errors with the length of the sequence. Clearly for long codes, the fraction of errors is given by the saymptotic Hamming bound.

V. Relation to the Bound by Finite State Algorithms

While the bound of Theorem 2 gives a convenient way of testing partial descriptions of error patterns, the variable length description usually leads to an infinite tree. Thus a complete weight specification is naturally described by a finite state algorithm, and we arrive at the upper bound discussed in [1].

References.

[1] J. Justesen, "Bounded distance decoding of unit memory codes," *IEEE Trans. Info. Th.*, vol. IT-39, September 1993, pp. 1616-1627.

[2] G. David Forney, Jr., "Structural analysis of convolutional codes via dual codes," *IEEE Trans. Info. Th.*, vol. IT-19, July 1973, pp. 512-518.

[3] G. David Forney, Jr., "Convolutional codes II: Maximum likelihood decoding," *Information and Control*, vol. 25, July, 1974, pp. 222-266.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Bounds on the Maximum Likelihood Decoding Error Probability of Low Density Parity Check Codes

Gadi Miller and David Burshtein
Dept. of Electrical Engineering Systems
Tel-Aviv University
Tel-Aviv 69978, Israel
e-mail: gmiller,burstyn@eng.tau.ac.il

Abstract — **We derive bounds on the error probability of ML decoded LDPC codes, for any binary-input symmetric-output channel. For appropriately chosen ensembles of LDPC codes, reliable communication is possible up to channel capacity. The lower and upper bounds coincide asymptotically, indicating a polynomially decreasing ensemble averaged error probability. For ensembles with suitably chosen parameters, the error probability of almost all codes is exponentially decreasing. Furthermore, the error exponent can be set arbitrarily close to the standard random coding exponent.**

I. Introduction

In this paper we examine the error probability of optimal (Maximum Likelihood) decoding of low density parity check (LDPC) codes, first introduced by Gallager [1] in 1963.

We consider two ensembles of LDPC codes. The first ensemble was proposed by Mackay [2]. The second ensemble is based on bipartite regular graphs, and was used by several researchers, e.g. [3].

II. An independent matrix column ensemble

We consider the ensemble of parity check matrices $A_{L\times N}$ (corresponding to a code with block length N and L parity check equations) defined by applying the following procedure to each column of A, for some integer t. First set the entire column to 0's. Then t times an index is drawn uniformly and independently from $\{1,2,...,L\}$ and the corresponding bit is flipped. We claim the following:

Theorem 1 *Consider the ensemble of binary parity check matrices $A_{L\times N}$ described above, over a memoryless binary-input symmetric-output channel. Let C denote channel capacity, $R\triangleq 1-L/N$ and suppose that the following conditions are satisfied for $t\geq 3$ and some $0<\gamma<1/2$ and $K>0$:*

$$\frac{6\ln\left(t/(1-R)\right)}{t}\leq K \tag{1}$$

$$h_2(\gamma)+(1-R)\left(\log\left(1+e^{-4e^{-12-K}}\right)-1\right)<0 \tag{2}$$

and

$$R+G(R,\gamma t)<C \tag{3}$$

where

$$G(R,\gamma t)\triangleq\max_{0\leq x\leq 1/2}\left\{(1-R)h_2(x)+\gamma t\log(1-2x)\right\}$$

Denote the ensemble averaged maximum likelihood decoding error probability by $\overline{P}_e$. Then

$$\lim_{N\to\infty}\frac{-\log\overline{P}_e}{\log N}=\begin{cases}\frac{t}{2}-1 & t \text{ even}\\ t-2 & t \text{ odd}\end{cases} \tag{4}$$

$h_2(x)$ is the (base-2) entropy function. The rate of the code is in fact lower bounded by R, due to possible redundancy in the parity check equations. Perhaps the most striking feature of the theorem is that the right hand side of (4) is independent of both R and C. This behavior stands in contrast to the various bounds on the probability of error when using random coding, where the bound is monotonically increasing with increasing R or decreasing C.

Furthermore, it can be shown that (1)-(3) hold when either $R<C$ and t is large enough, or when for given t, $D>0$ is small enough, where D is a quality parameter of the channel, $D\triangleq\sum_y\sqrt{P(y|0)P(y|1)}$ ($P(y|x)$ describes the channel).

III. Codes derived from bipartite regular graphs

A popular method for obtaining an ensemble of sparse parity-check codes is defined in terms of a bipartite graph. This is done by constructing a $c-d$ regular bipartite graph in which there are N vertices on the left side of the graph, each of degree c, and L vertices on the right, each of degree d, so that $Nc=Ld$. This ensemble is described in [3].

It can be shown that the following holds,

$$\lim_{N\to\infty}\frac{-\log\overline{P}_e}{\log N}=\begin{cases}\frac{c}{2}-1 & c \text{ even}\\ c-2 & c \text{ odd}\end{cases}$$

provided that c and d satisfy conditions analogous to the conditions set in Theorem 1.

IV. Expurgated ensembles

Our results can be greatly improved by expurgating from the ensembles codes which have small minimal distance. It turns out that when the ensemble parameter t (c and d) is sufficiently large, the error probability of the expurgated ensemble is exponentially decreasing, and the exponent is arbitrarily close to the random-coding exponent.

Acknowledgments

We thank Nadav Shulman for helpful discussions and in particular to his contributions that led to some of the results on lower bounds and expurgated ensembles.

References

[1] R. G. Gallager, *Low Density Parity Check Codes*, M.I.T Press, Cambridge, Massachusetts, 1963.

[2] D. J. C. MacKay, "Good error-correcting codes based on very sparse matrices", *IEEE Trans. Inform. Theory*, vol. 45, pp. 399–431, March 1999.

[3] T. Richardson and R. Urbanke, "The capacity of low-density parity check codes under message-passing decoding", submitted to *IEEE Trans. Inform. Theory*, available at http://cm.bell-labs.com/cm/ms/who/tjr/pub.html.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Punctured Recursive Convolutional Encoders and Their Applications in Turbo Codes

Ba-Zhong Shen
Broadcom Corporation
Irvine, CA 92619, USA

Ara Patapoutian
Quantum Corporation
Shrewsbury MA 01545, USA

Peter McEwen
Quantum Corporation
Milpitas, CA 95035, USA

Abstract — **Puncturing is the predominant strategy to construct high code rate convolutional encoders, and infinite impulse response convolutional encoders are an essential building block in Turbo codes. In this paper various properties of convolutional encoders with these characteristics are developed. In particular, the closed form representation of a punctured convolutional encoder and its generator matrix is constructed, necessary and sufficient conditions are given such that the punctured encoders retain the infinite impulse response property, and various lower bounds on distance properties, such as effective free distance, are developed. Finally, necessary and sufficient conditions are given on the inverse puncturing problem: representing a known convolutional encoder as a punctured encoder.**

Turbo codes, introduced in 1993 by Berrou *et al.*[1], use systematic infinite impulse response (IIR) convolutional encoders as building blocks. The IIR or recursive constraint is imposed to achieve interleaver gain [2]. The systematic constraint is imposed so that the information bits are used only once in a codeword together with the parity bits from both constituent binary systematic convolutional encoders. In this paper the interest is in convolutional codes for Turbo codes on bandlimited channels. Such channels force the code rate of each constituent code to be high. Since punctured convolutional encoders are the most practical class of convolutional encoders that generate high code-rate codes, puncturing is imposed on the constituent convolutional encoders. In this paper, we refer to the original encoder from which the punctured encoder is derived as the *parent encoder*.

In this paper, we are interested in designing binary punctured convolutional codes that are IIR, may or may not be systematic, and that perform well when used in a Turbo setting. To characterize the effectiveness of such encoders, in [2, 3, 4] the commonly used free distance is replaced with the effective free distance d_2, the minimum weight among all codewords with weight 2 information sequences.

In this paper, *polyphase representation* and *polyphase decomposition* [5] are generalized. We also introduced *polyphase composition*. Some properties of these polyphase transforms are derived that will form the building blocks for the rest of the paper. Also in this paper, a punctured convolutional encoder is represented in closed form using polyphase transforms. Finally, the generator matrix of a punctured encoder is concisely derived similarly to McEliece [5] and Hole [6] where the parent encoder was assumed to be finite impulse response (FIR). Generator matrices for rate-2/3 punctured systematic encoders were derived from a parent rate-1/2 encoder in [4].

When an IIR convolutional code is punctured the resultant encoder is not necessarily IIR. In this paper, given an IIR convolutional encoder, necessary and sufficient conditions are derived to ensure that the resulting punctured encoder is IIR.

Various lower bounds are found in this paper on the effective free distance d_2 for punctured parent codes. More specifically, for any rate-$1/n_0$ parent encoder, a sufficient condition is given that guarantees a punctured rate-k/n encoder with $d_2 \geq t$, where $1 \leq t \leq n$. Also, for a systematic rate-1/2 parent encoder with irreducible feedback polynomial, sufficient conditions, which include a necessary and sufficient condition for a class of parent encoders, are given on $d_2 \geq 3$ of the generated punctured rate-$k/(k+1)$ encoders. Note that when the encoder is IIR $d_2 \geq 3$ also implies minimum free distance greater or equal to 3 which, as pointed out by Divsalar *et al.* in [7], is a crucial condition on the outer code for serial turbo codes to have interleave gain.

Good non-punctured convolutional codes have been comprehensively studied [5, 8]. In general, using these codes, punctured encoders are constructed. However, it is not known whether the rate-k/n good convolutional codes themselves can be encoded as a punctured encoder with rate-k_0/n_0 parent encoder such that k_0 is much smaller than k. It is shown in this paper that any rate-k/n systematic convolutional code can be encoded by a punctured systematic encoder with a rate-k_0/n_0 parent encoder for any factor k_0 of k and for some n_0 ($\leq n$). Furthermore, given k_0 and n_0, a necessary and sufficient condition is given that guarantee that a rate-k/n convolutional code can be generated from rate-k_0/n_0 parent convolutional encoder.

References

[1] C. Berrou, A. Glavieux and P. Thitimajshima, "Near Optimum Error Correcting Coding and Decoding: Turbo codes," *Proceedings of 1993 International Conference on Communications* , (Geneva, Switzerland), pp. 1064-1070, May 1993.

[2] S. Benedetto and G. Montorsi, "Design of Parallel Concatenated Convolutional Codes," *IEEE Trans. Communications* , vol. 44, pp. 591-600, 1996.

[3] D. Divsalar and R. McEliece, "The Effective Free Distance of Turbo Codes," *Electron. Lett.* , vol. 32, 1996.

[4] D. Divsalar and F. Pollara, "On the Design of Turbo Codes," *TDA Progress Report* , vol. 42-123, pp. 99-121, 1995.

[5] R.J. McEliece, "The Algebraic Theory of Convolutional Codes," in *Handbook of Coding Theory* (V. Pless and W.C. Huffman, ed.), (Amsterdam), Elsevier Science, 1999.

[6] K.J. Hole, "Punctured Convolutional Codes for the 1-D Partial-Response Channel," *IEEE Trans. Inform. Theory* , vol. 37, pp. 808-817, 1991.

[7] D. Divsalar, H. Jin and R. McEliece, "Coding Theorems for "Turbo-Like" Codes," in *Proceedings of Thirty-Six Annual Allerton Conference on Communication, Control, and Computing*(Monticello, Illinois), 1998.

[8] G.D. Forney, "Convolutional Codes I: Algebraic Structure," *IEEE Trans. Inform. Theory* , vol. IT-16, pp. 720-738, 1970.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On the Search For Self-Doubly Orthogonal Codes

Brice Baechler[1], David Haccoun[1] and François Gagnon[2]

[1]Department of electrical and computer engineering
Ecole Polytechnique de Montréal
P.O. Box 6079 Station Centre Ville
Montréal, QC, Canada
H3C 3A7

[2]Department of electrical engineering
Ecole de Technologie Supérieure
1100, Notre-Dame W.
Montréal, QC, Canada
H3C 1K3

Abstract— **In this paper we present the search and determination of a subset of orthogonal convolutional codes called Convolutional Self Doubly Orthogonal Codes (CSO^2C). These codes may be advantageously utilised for the novel coding/iterative decoding technique introduced as an important amelioration of Turbo Codes. For this technique the code constraint length corresponds to the latency of each decoding iteration. Hence, an important parameter in the code searching is the minimisation of the code constraint length for a given error correcting capability.**

I. Introduction

The new coding system presented in [1], [2] represents an important improvement over the classical turbo code architecture. However it requires the use of threshold decodable codes which must exhibit further orthogonal properties than the well known orthogonal codes [4]. The methods initially used to generate these codes were based on principles of finite field Projective Geometry. We present new techniques based on the use of a random parameter which produces CSO^2C with substantially reduced length.

II. Wide-sense rate CSO^2C with rate $R = \frac{1}{2}$

A rate R=$\frac{1}{2}$ convolutional code having J connections is said to be doubly orthogonal in the wide sense, if its J generators $\{g_i\}$ satisfy the relation :

$$\begin{cases} \forall(i,j,k,l)\ i \neq j,\ k \neq l,\ j \neq k,\ i \neq l \\ \textit{the differences } g_i - g_j - (g_l - g_k) \textit{ are distinct} \\ \textit{(except for unavoidable index permutations).} \end{cases} \quad (1)$$

`Code generation technique :`
A pseudo-random constructive method for determining the code generators is used. Starting from a set of J acceptable generators, we try to add an element taken among the natural integers arranged in ascending order. Should the new set of J+1 elements so obtained proved to be self-doubly orthogonal, a random test is run in order to decide whether or not to retain this additional integer. The procedure is repeated anew until the required number of elements is obtained.

`Length reduction :`
Improvement on the code length is attemped by using a reduction method based on the following observation : any addition or multiplication applied to $\{g_i\}$ maintains the double orthogonality property. The reduction consists in performing theses elementary operations modulo an integer n which is gradually decreased until the largest reduction is obtained.

`Results :`
The code generation method and its ensuing reduction procedure has yielded good novel CSO^2C codes which were superior to those obtained by the previous procedure.

III. Strict-sense CSO^2C with rates $R = \frac{J}{2J}$

The self-double orthogonality in the strict sense is obtained by allowing a single connection between each information sequence and each parity sequence [1]. That is, the code generators $\{g_{i,j}\}$ must satisfy :

$$\begin{cases} \textit{be } (k,v),\ \forall(l,m,n)\ l \neq n,\ m \neq n \textit{ and } m \neq v \\ g_{k,l} - g_{m,l} - (g_{v,n} - g_{m,n}) \textit{ are distinct.} \end{cases} \quad (2)$$

`Code generation technique :`
Once again we investigate a method which includes a random parameter. Starting from a set of generators that we know to be self-doubly orthogonal, we perform a random repartition of the index order of our matrix $(g_{i,j})$. Then, we replace each generator (taken in the order previously etablished) with the smallest natural integer that maintains the property of double orthogonality.

`Length reduction :`
The reduction procedure is based on the method proposed by Wu [3]. Simple addition and substraction operations are performed over the rows and columns of the initial matrix of generators. An algorithm was developed for executing the procedure iteratively until a set of generators whose largest element is as small as possible is obtained.

`Results :`
The results obtained show that substantial reduction of the lengths of the codes could be achieved without requiring an excessive computation time.

Conclusion

The novel methods have yielded very interesting results with the generation of different sets of CSO^2C with reduced lengths. Both types of self-doubly orthogonal codes (wide and strict sense) have been analysed and compared. The error performances of all these codes have been determined by simulation using the novel iterative decoding algorithm [1]. The new sets of CSO^2C generated improve significantly the performance of the novel coding/iterative decoding system by limiting both the latency at the decoding and the amount of memory required.

References

[1] Cardinal, C., Haccoun, D., Gagnon, F. and Batani, N., *Iterative Threshold Decoding without Interleaving for Convolutional Self-Doubly Orthogonal Codes*, IEEE International Symposium on Information Theory, Cambridge, MA., August 1998.

[2] Gagnon, F., Haccoun, D., Batani, N., and Cardinal, C., *Apparatus for Convolutional Self-Doubly Orthogonal Encoding and Decoding*, US Patent Application Field, October 2^{nd} 1997, US Patent and Trademark Office, Washington DC, and European Patent Application Field, October 2^{nd} 1998, European Patent Office, Netherlands.

[3] Wu, W.W., *New Convolutional Codes, Part I*, IEEE Transactions on Communications, Vol. COM-23, pp. 942-956, September 1975.

[4] Massey, J.L., Threshold decoding, MIT Press, Cambridge, MA., 1963.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On Rate-$k/2k$ Self-Dual Convolutional Codes

Ajay Dholakia
IBM Zurich Research Laboratory
Säumerstrasse 4
CH 8803 Rüschlikon Switzerland
e-mail: adh@zurich.ibm.com

Abstract — **A class of rate-$k/2k$ self-dual convolutional codes is defined, which includes, for instance, the Golay Convolutional Code. It is shown that codes in this class are not asymptotically catastrophic in the sense defined by Hemmati and Costello [3].**

I. Introduction

Block codes can be obtained from convolutional codes via the tail-biting construction where zero-tail termination is replaced by tail-biting, avoiding the rate loss. If the convolutional code used has long low-weight codewords, the resulting block code can have poor weight distribution. Convolutional codes which have long codewords of low weight were called asymptotically catastrophic by Hemmati and Costello [3]. In this paper, we show that the class of time-invariant unit-memory rate-$k/2k$ self-dual convolutional codes is not asymptotically catastrophic.

II. Self-Dual $(2k, k, k)$ Convolutional Codes

A rate-k/n convolutional code with overall constraint length ν and memory order m [2] can have a time-varying or time-invariant encoder. A time-varying (n, k, ν) convolutional encoder can altenatively be viewed as a time-invariant *unit-memory* $(n' = nm, k' = km, \nu)$ encoder with memory order $m' = 1$ [2].

A linear code (block or convolutional) is *self-orthogonal* if it is contained in its dual, and *self-dual* if it is equal to its dual [1]. The dual of a linear code is the set of all codewords that are orthogonal to the codewords in the code. For convolutional codes, we have the related concept of the *convolutional* dual code. If a convolutional code is generated by a matrix $\mathbf{G}(D)$, then its convolutional dual code is generated by a matrix $\mathbf{H}(D)$, with $\mathbf{G}(D)\mathbf{H}^T(D) = \mathbf{0}$.

We define the class $\mathcal{S}$ of $(2k, k, k)$ self-dual convolutional codes as follows. We only consider time-invariant unit-memory $(2k, k, \nu)$ convolutional codes that also have $\nu = k$, for $k \geq 1$. Then, we further restrict ourselves to self-dual $(2k, k, k)$ codes to get the class $\mathcal{S}$. Note that the Golay Convolutional Code [1] belongs to this class as an (8,4,4) code.

III. Main Result

Let w_0 denote the minimum average weight per branch over all cycles in the state transition diagram of a convolutional encoder, excluding the zero-weight self-loop around the zero state. Hemmati and Costello [3] defined a class of codes to be *asymptotically catastrophic* if w_0 approaches zero as codes with increasing ν are considered. Many convolutional code classes are asymptotically catastrophic [3, 4].

Let $\mathbf{H}(D)$ be a canonical parity-check matrix for the convolutional code, and let e_i, $1 \leq i \leq r = n - k$, be the maximum degree of the polynomials in the ith row of the matrix. Without loss of generality, assume the ordering $e_1 = e_2 = ... = e_\gamma = 0$ for some γ, $0 \leq \gamma < r$, and $1 \leq e_{\gamma+1} \leq ... \leq e_r = e_{max}$. If $\gamma > 0$, the first γ rows of $\mathbf{H}(D)$ define a parity-check matrix for an $[n, n-\gamma]$ binary block code $\mathcal{E}$, with minimum distance $d_\mathcal{E}$ [5]. For $\gamma = 0$, let $\mathcal{E}$ be the trivial $[n, n]$ block code having all possible binary n-tuples, with $d_\mathcal{E} = 1$. Hole [5] has recently obtained the lower bound

$$w_0 \geq d_\mathcal{E}/e_{max}. \quad (1)$$

A class of convolutional codes is not asymptotically catastrophic if w_0 is bounded away from zero as ν increases. In practice, it is often important to ensure that a class of codes is not asymptotically catastrophic. For instance, if longer block codes are obtained via tail-biting constructions from convolutional codes, the resulting distance properties can become dependent on whether the parameter w_0 is high or low.

Proposition 1 *The class $\mathcal{S}$ of $(2k, k, k)$ self-dual convolutional codes defined above is not asymtotically catastrophic.*

Proof: For any code in $\mathcal{S}$, the corresponding convolutional dual code is generated by the reverse $\tilde{\mathbf{G}}(D)$ of the generator matrix $\mathbf{G}(D)$, i.e., $\mathbf{H}(D) = \tilde{\mathbf{G}}(D)$. Since $\mathbf{G}(D)$ has all its row degrees equal to one, the corresponding parity-check matrix $\mathbf{H}(D)$ must have overall constraint length $\nu = k$. But $\mathbf{H}(D)$ is also a $k \times 2k$ matrix whose row degrees $e_1, e_2, ..., e_r = e_k$ must sum to k. Hence all dual row degrees $e_1, ..., e_k = e_{max} = 1$, so $w_0 \geq d_\mathcal{E}$. Further, since no e_i is equal to zero, we have $\gamma = 0$ and $d_\mathcal{E} = 1$. Therefore, $w_0 \geq 1$, and the statement of the proposition follows. Q.E.D.

This implies that block codes obtained from convolutional codes in the class $\mathcal{S}$ via the tail-biting construction are good from the weight distribution perspective, as shown for block codes obtained from the Golay Convolutional Code [6].

Acknowledgments

The author thanks Dr. K.J. Hole for advance copy of [5].

References

[1] A.R. Calderbank, G.D. Forney, Jr., and A. Vardy. Minimal tail-biting trellises: The Golay code and more. *IEEE Trans. Inf. Theory*, 45(5):1435–1455, 1999.

[2] A. Dholakia. *Introduction to convolutional codes with applications*. Kluwer Academic Publishers, Boston, MA, USA, 1994.

[3] F. Hemmati and D.J. Costello, Jr. Asymptotically catastrophic convolutional codes. *IEEE Trans. Inf. Theory*, IT-26(3):298–304, 1980.

[4] K.J. Hole. A note on asymptotically catastrophic convolutional codes of rate $(n-1)/n$. *IEEE Trans. Comm.*, 45(9):1014–1016, 1997.

[5] K.J. Hole. On classes of convolutional codes that are not asymptotically catastrophic. submitted to *IEEE Trans. Inf. Theory*, 1999.

[6] S. Riedel and C. Weiss. The Golay convolutional code–some application aspects. *IEEE Trans. Inf. Theory*, 45(6):2191–2199, 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Construction Results for MDS-Convolutional Codes[1]

Roxana Smarandache
Department of Mathematics,
University of Notre Dame
Notre Dame, IN 46556-5683 USA
Smarandache.1@nd.edu
www.nd.edu/~rsmarand/

Heide Gluesing-Luerssen
Fachbereich Mathematik,
Universität Oldenburg
D-26111, Oldenburg, Germany
gluesing@mathematik.uni-oldenburg.de

Joachim Rosenthal
Department of Mathematics,
University of Notre Dame
Notre Dame, IN 46556-5683 USA
Rosenthal.1@nd.edu
www.nd.edu/~rosen/

Abstract — **The generalized Singleton bound and MDS-convolutional codes are reviewed. For each n, k and δ an elementary construction of rate k/n MDS convolutional codes of degree δ is given.**

I. Introduction

The minimum distance of a block code is upper bounded by the Singleton bound $d_{min} \leq n-k+1$. Codes attaining this bound are called MDS block codes and Reed Solomon codes are examples of such codes. Since convolutional codes generalize block codes, it is natural to study the way the Singleton bound is generalized to convolutional codes.

Let $\mathbb{F}$ be a finite field and $G(D)$ be a $k \times n$ full rank matrix over $\mathbb{F}[D]$. Let $\mathcal{C} = \{u(D)G(D) \mid u(D) \in \mathbb{F}^k[D]\}$ be the rate k/n convolutional code generated by $G(D)$. Two generator matrices $G(D)$ and $G'(D)$ are equivalent if they generate the same convolutional code $\mathcal{C}$. Then there exists a $k \times k$ unimodular matrix $U(D)$ with $G'(D) = U(D)G(D)$. We say that $G(D)$ is *catastrophic* if a non-polynomial message $u(D)$ can result in a polynomial codeword $u(D)G(D)$. This can happen if and only if the $k \times k$-minors of the matrix $G(D)$ have a non-constant common divisor other than D. We will suppose $G(D)$ is noncatastrophic.

Along with n and k, there is a third important parameter of a convolutional code $\mathcal{C}$, called the *degree*. It is defined as the maximal degree δ of the $k \times k$ minors of $G(D)$. Equivalent encoding matrices have the same degree so the degree is an invariant of the code. See [3] for details.

We define the weight of a polynomial $v(D) \in \mathbb{F}^n[D]$ as the sum of the Hamming weights of all its $\mathbb{F}^n$-coefficients and the *free distance* of the code as:

$$d_{free} = \min\{\mathrm{wt}(v(D)) \mid v(D) \in \mathcal{C}, v(D) \neq 0\}.$$

Lemma 1 [3] *Let $\mathcal{C}$ be a convolutional code of rate k/n and degree δ. Then the free distance must satisfy:*

$$d_{free} \leq (n-k)\left(\lfloor \delta/k \rfloor + 1\right) + \delta + 1. \tag{1}$$

We call the bound (1) the generalized Singleton bound. For $\delta = 0$ the bound is the classical bound $n-k+1$. We showed in [3] that there are codes attaining this bound over sufficiently large finite fields. We called such codes *MDS* convolutional codes. The existence proof in [3] was non-constructive and it was based on methods from algebraic geometry.

II. A construction of rate k/n-MDS Convolutional Codes

In this section we follow [5] and provide a concrete construction of an MDS convolutional code for each degree δ and each rate k/n. The construction makes use of [1, 2].

As defined in [1, 2], a convolutional code is said to be *generated by a polynomial*

$$g(D) = g_0(D^n) + g_1(D^n)D + \ldots + g_{n-1}(D^n)D^{n-1},$$

if it has a polynomial encoder of the form

$$G(D) = \begin{bmatrix} g_0(D) & g_1(D) & \cdots & g_{n-1}(D) \\ Dg_{n-1}(D) & g_0(D) & \cdots & g_{n-2}(D) \\ \vdots & \vdots & & \vdots \\ Dg_{n-k+1}(D) & Dg_{n-k+2}(D) & \cdots & g_{n-k}(D) \end{bmatrix}. \tag{2}$$

The code $\mathcal{C}$ generated by $G(D)$ is isomorphic to

$$\left\{\left(u_0(D^n) + u_1(D^n)D + \ldots + u_{k-1}(D^n)D^{k-1}\right) \cdot g(D)\right\},$$

where $(u_0(D), \ldots, u_{k-1}(D)) \in \mathbb{F}^k[D]$ is an information vector.

Lemma 2 [5] *Let p be a prime and $k < n$, δ nonnegative integers with p and n relatively prime. Then there exist positive integers r and a with*

$$a \geq \lfloor \delta/k \rfloor + 1 + \delta/(n-k), \ an = p^r - 1.$$

Assume that a, r is as in the Lemma 2 and let $N = an$, $K = N - (n-k)\left(\lfloor \delta/k \rfloor + 1\right) - \delta$, and $\alpha \in \mathbb{F}_{p^r}$ a primitive element of $\mathbb{F}_{p^r}$. Define $g(D) = (D-\alpha^0)(D-\alpha^1)\cdots(D-\alpha^{N-K-1}) \in \mathbb{F}_{p^r}[D]$. The polynomial $g(D)$ defines an $[N, K]$ Reed-Solomon block code with distance $d_g = N-K+1 = (n-k)\left(\lfloor \delta/k \rfloor + 1\right) + \delta + 1$.

Using [1, Theorem 3] we obtain:

Theorem 3 [5] *Let $g(D)$ be defined as above. Then the convolutional code defined by (2) is MDS.*

Example 4 [5] Let α be a primitive of $\mathbb{F}_{2^6}$. The rate 2/3 encoder

$$\begin{bmatrix} \alpha^{28}+\alpha^{35}D+\alpha^{57}D^2 & 1+\alpha^6 D+\alpha^{42}D^2 & \alpha^8+\alpha^{26}D+D^2 \\ \alpha^8 D+\alpha^{26}D^2+D^3 & \alpha^{28}+\alpha^{35}D+\alpha^{57}D^2 & 1+\alpha^6 D+\alpha^{42}D^2 \end{bmatrix}.$$

has degree 5 and has free distance 9. The code attains the generalized Singleton bound (1) and therefore is an MDS convolutional code.

If one is interested to do the construction with small fields then one should construct a prime power q for which

$$n \mid (q-1) \text{ and } q > \delta \frac{n^2}{k(n-k)}. \tag{3}$$

The first author recently showed [4] that there are alternative constructions for unit memory MDS convolutional codes, these are codes where $\delta \leq k$.

[1]The authors were supported in part by NSF grant DMS-96-10389. The first author was also supported by a fellowship from the Center of Applied Mathematics at the University of Notre Dame.

References

[1] J. Justesen. New convolutional code constructions and a class of asymptotically good time-varying codes. *IEEE Trans. Inform. Theory*, IT-19(2):220–225, 1973.

[2] J. L. Massey, D. J. Costello, and J. Justesen. Polynomial weights and code constructions. *IEEE Trans. Inform. Theory*, IT-19(1):101–110, 1973.

[3] J. Rosenthal and R. Smarandache. Maximum distance separable convolutional codes. *Appl. Algebra Engrg. Comm. Comput.*, 10(1):15–32, 1999.

[4] R. Smarandache. Unit memory convolutional codes with maximum distance. In B. Marcus and J. Rosenthal, editors, *Codes, Systems and Graphical Models*, IMA Vol. in Math. and its Appl. Springer-Verlag, 2000. To appear.

[5] R. Smarandache, H. Gluesing-Luerssen, and J. Rosenthal. Constructions of MDS-convolutional codes. Submitted to IEEE Trans. Inform. Theory, August 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

A Universal Lossless Resolution Scalable Progressive Image Code

John Kieffer and Ross Stites[1]
ECE Department
University of Minnesota
Minneapolis, MN 55455

En-Hui Yang[2]
ECE Department
University of Waterloo
Waterloo, Ontario N2L 3G1

Abstract — **A universal lossless resolution scalable progressive image code is presented which is based on the concept of a conditional quadrisection grammar.**

I. Introduction

Let $\mathcal{A}$ be a finite alphabet. For each nonnegative integer n, let $\mathcal{M}_n$ be the set of all $2^n \times 2^n$ matrices over $\mathcal{A}$. Let $\mathcal{M} = \cup_n \mathcal{M}_n$; $\mathcal{M}$ is the class of images that we deal with here. If $n \geq 1$ and $M = [M(i,j) : i,j = 0,1,\cdots,2^n-1]$ is an image in $\mathcal{M}_n$, we let $\downarrow M = [M(2i,2j) : i,j = 0,1,\cdots,2^{n-1}-1]$ be the image in $\mathcal{M}_{n-1}$ obtained by downsampling M. For each image $Q \in \mathcal{M}$, let $\mathcal{M}(Q)$ be the set of all images M for which $\downarrow M = Q$. For each $n \geq 0$ and each $M \in \mathcal{M}_n$, let $M^0, M^1, \cdots, M^n$ be the images such that $M^n = M$ and

$$M^i = \downarrow M^{i+1}, \quad 0 \leq i < n$$

A lossless resolution scalable progressive image code (LRSPIC) ϕ on $\mathcal{M}$ consists of a collection of binary words

$$\phi = \{w(a) : a \in \mathcal{A}\} \cup \{w(M|Q) : Q \in \mathcal{M}, \ M \in \mathcal{M}(Q)\} \quad (1)$$

such that

(i) The words $\{w(a) : a \in \mathcal{A}\}$ satisfy the prefix condition.

(ii) For each $Q \in \mathcal{M}$, the words $\{w(M|Q) : M \in \mathcal{M}(Q)\}$ satisfy the prefix condition.

For each $n \geq 0$ and each $M \in \mathcal{M}_n$, the LRSPIC ϕ given by (1) encodes M into the binary codeword $w_\phi(M)$ given by

$$w_\phi(M) \triangleq w(M^0)w(M^1|M^0)\cdots w(M^n|M^{n-1}), \quad (2)$$

the left-to-right concatenation of the words $w(M^0)$, $w(M^1|M^0)$, $w(M^2|M^1), \cdots, w(M^n|M^{n-1})$.

II. Conditional Quadrisection

Let Q and M be images such that $M \in \mathcal{M}(Q)$. Supposing that Q is $2^j \times 2^j$, we let $\mathcal{I}(Q)$ denote the distinct subimages of Q that appear in the partitions of Q into $2^i \times 2^i$ subimages, $0 \leq i \leq j$. The *conditional quadrisection grammar* $G(M|Q)$ [1] is a set of production rules of the form

$$B \xrightarrow{R} \begin{bmatrix} C & D \\ E & F \end{bmatrix}, \quad (3)$$

where R is a member of $\mathcal{I}(Q)$, B is an abstract symbol, C, D, E, F are all abstract symbols if $R \notin \mathcal{M}_0$ (in which case (3) is said to be *nonterminal*) or are all members of $\mathcal{A}$ if $R \in \mathcal{M}_0$ (in which case (3) is said to be *terminal*). The grammar $G(M|Q)$ satisfies the properties:

(a) Given R and B, there is at most one production rule in $G(M|Q)$ of form (3).

(b) There is exactly one production rule (3) in $G(M|Q)$ with $R = Q$ (called the *root production rule* of $G(M|Q)$).

(c) A square array of nonterminal production rules can be made bigger by simultaneous replacement of each entry (3) with a 2×2 array of rules

$$\begin{matrix} C \xrightarrow{S} [\ ] & D \xrightarrow{T} [\ ] \\ E \xrightarrow{U} [\ ] & F \xrightarrow{V} [\ ] \end{matrix},$$

where

$$R = \begin{bmatrix} S & T \\ U & V \end{bmatrix}.$$

Repeated application of this operation, starting from the root production rule, eventually results in a matrix of terminal production rules which yields M.

Example: Let $Q = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ and let $G(M|Q)$ be the conditional quadrisection grammar

$$\left\{ A \xrightarrow{Q} \begin{bmatrix} A & A \\ A & A \end{bmatrix}, \ A \xrightarrow{0} \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \ A \xrightarrow{1} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \right\}. \quad (4)$$

The reconstruction method (c) yields

$$M = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

Given Q, M can be encoded with 9 codebits, because each rule in (4) can be encoded with 3 codebits.

III. Universality Results

To each conditional quadrisection grammar $G(M|Q)$ there corresponds a binary codeword $w(M|Q)$ such that $G(M|Q)$ is recoverable from Q and $w(M|Q)$. The binary codewords $\{w(M|Q) : Q \in \mathcal{M}, \ M \in \mathcal{M}(Q)\}$, augmented by any binary codewords $\{w(a) : a \in \mathcal{A}\}$ satisfying (i), induce a unique LRSPIC on $\mathcal{M}$. Let $L(M)$ be the length of the codeword (2) assigned to $M \in \mathcal{M}$ by this LRSPIC, and let $L_{fs}(M)$ be the length of the codeword assigned to M by a fixed (but arbitrary) finite-state LRSPIC on $\mathcal{M}$.

Theorem 1 *For some positive constant C,*

$$\max_{M \in \mathcal{M}_n} \{L(M) - L_{fs}(M)\} \leq C \left[\frac{4^n}{n}\right], \quad n \geq 1$$

Corollary 1 *Let $[X(i,j) : i,j$ integers$]$ be a stationary random field with entropy H. Let $M_n = [X(i,j) : i,j = 0,1,\ldots,2^n-1]$. Then*

$$\lim_{n\to\infty} E[L(M_n)]/4^n = H$$

References

[1] J. Kieffer, R. Stites, and E-H. Yang, "Universal Lossless Resolution Scalable Progressive Image Coding Via the Conditional Quadrisection Algorithm," paper in preparation.

[1]Supported by NSF Grants NCR-9627965 and CCR-9902081.
[2]Supported by Canadian NSERC Grant RGPIN203035-98.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Data Compression Via Binary Decision Diagrams

John Kieffer[1]
ECE Department
University of Minnesota
Minneapolis, MN 55455

Philippe Flajolet
INRIA Rocquencourt
F-78153, Le Chesnay, France

En-Hui Yang[2]
ECE Department
University of Waterloo
Waterloo, Ontario N2L 3G1

Abstract — **A binary data string of length 2^k induces a Boolean function of k variables which can be represented by a unique reduced binary decision diagram. We losslessly compress the data string indirectly by compressing this binary decision diagram. The resulting data compression algorithm is universal.**

I. Introduction

We start with the observation that a binary data string of length 2^k induces a Boolean function of k variables in a natural way. The following example illustrates the procedure.

Example 1: A general binary data string

$$u = u_1u_2u_3u_4u_5u_6u_7u_8u_9u_{10}u_{11}u_{12}u_{13}u_{14}u_{15}u_{16} \quad (1)$$

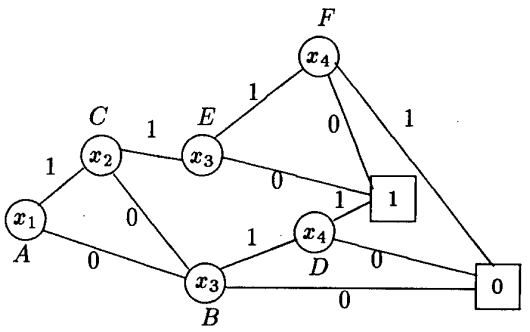
of length 16 induces the following Boolean function $f_u(x_1, x_2, x_3, x_4)$ of four variables:

$f_u(0,0,0,0) = u_1$ $f_u(0,0,0,1) = u_2$ $f_u(0,0,1,0) = u_3$
$f_u(0,0,1,1) = u_4$ $f_u(0,1,0,0) = u_5$ $f_u(0,1,0,1) = u_6$
$f_u(0,1,1,0) = u_7$ $f_u(0,1,1,1) = u_8$ $f_u(1,0,0,0) = u_9$
$f_u(1,0,0,1) = u_{10}$ $f_u(1,0,1,0) = u_{11}$ $f_u(1,0,1,1) = u_{12}$
$f_u(1,1,0,0) = u_{13}$ $f_u(1,1,0,1) = u_{14}$ $f_u(1,1,1,0) = u_{15}$
$f_u(1,1,1,1) = u_{16}$

Notice that we assigned values to $f_u(x_1, x_2, x_3, x_4)$ by running through the 16 possibilities for the vector variable (x_1, x_2, x_3, x_4) in lexicographical order.

Boolean functions are commonly represented by finite, binary, rooted, directed, acyclic, labelled graphs called binary decision diagrams (BDD's) [1]. The BDD with the minimal number of vertices that represents a given Boolean function is unique and is called the ROBDD representation of the Boolean function. (ROBDD stands for Reduced Ordered Binary Decision Diagram.)

Example 2: Taking the string in (1) to be u = 0001000100011110, the figure below depicts the ROBDD representation of the Boolean function $f_u(x_1, x_2, x_3, x_4)$.



[1]Supported by NSF Grants NCR-9627965 and CCR-9902081.
[2]Supported by Canadian NSERC Grant RGPIN203035-98.

The preceding discussion suggests a lossless data compression algorithm which encodes a binary data string u of length a power of two in two steps:

Step 1: Find the ROBDD representation of the Boolean function induced by u.

Step 2: Compress the ROBDD representation.

II. Compression Details

The ROBDD representing the Boolean function induced by a binary string of length 2^k is reconstructible from $k+1$ recursively generated strings $S_1, S_2, \cdots, S_{k+1}$, constructed as in the following example.

Example 3: The ROBDD representation in the figure is coded into the five strings:

$$S_1 = A, \quad S_2 = B^2C, \quad S_3 = BBE,$$
$$S_4 = 0^2D1^2F, \quad S_5 = 001110$$

Each first appearance of a symbol in $\{A, B, C, D, E, F\}$ in a string S_i (corresponding to a nonterminal vertex of the BDD) produces two symbols in the next string S_{i+1} (corresponding to the two daughter vertices, bottom daughter vertex first). Powers are used to indicate the presence of missing variables—for example, in S_2, the bottom daughter vertex of A is denoted B^2 to indicate that there are $2 - 1 = 1$ missing variables between vertex A and vertex B. Each first appearance of a symbol in $\{A, B, C, D, E, F, 0, 1\}$ raised to a power ≥ 2 in a string S_i brings about an appearance of that symbol to a power one less in the next string S_{i+1} (e.g., B^2 in S_2 becomes B in S_3). The decoder knows the first string S_1, and is sent codebits by the encoder to allow each S_i to be built from S_{i-1}. (For complete encoder/decoder description, see [2].)

III. Universality Result

For each $k \geq 1$, let $\mathcal{B}_k$ denote the set of all nonconstant binary strings of length 2^k for which the left half of the string is not equal to the right half of the string. For u a member of $\cup_k \mathcal{B}_k$, let $L(u)$ denote the number of codebits into which u is encoded by our ROBDD-based compression method. Let $L_{fs}(u)$ be the number of codebits into which u is encoded by any fixed (but arbitrary) finite-state lossless compression algorithm.

Theorem 1 *For any $k \geq 1$,*

$$\max_{u \in \mathcal{B}_k} \{L(u) - L_{fs}(u)\} \leq C \left[\frac{2^k}{k}\right],$$

where C is a positive constant depending only on the number of states of the fixed finite-state compression algorithm.

References

[1] R. Bryant, "Symbolic Boolean Manipulation with Ordered Binary-Decision Diagrams," *ACM Computing Surveys*, Vol. 24, pp. 293–318, 1992.

[2] J. Kieffer, P. Flajolet, and E-H. Yang, "Universal Lossless Data Compression Via the ROBDD Representation of Boolean Functions," paper in preparation.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On Modeling and Ordering for Embedded Image Coding

Erik Ordentlich[1]
iCompression
Santa Clara, CA 95051, USA
eordentlich@icompression.com

Marcelo J. Weinberger
Hewlett-Packard Labs
Palo Alto, CA 94303, USA
marcelo@hpl.hp.com

Gadiel Seroussi
Hewlett-Packard Labs
Palo Alto, CA 94303, USA
seroussi@hpl.hp.com

Abstract — **We present an information-theoretic framework for the optimization of the order in which embedded bit-plane coders encode image data.**

I. Summary

An *embedded* image coder generates a code-stream with the property that every prefix of the stream can be decoded to reconstruct the original image data with a fidelity approaching that of an "optimal" compression algorithm, tailored to produce the same code length (data rate) as the prefix. Embedding raises the problem of ordering information according to its "value": since the code-stream can be truncated at any time, we wish to transmit the most valuable information (in the sense of reducing the distortion of the reconstructed image the most) as early as possible. This ordering constraint, in turn, can affect causality relations that are usually relied upon to optimize the sequential probability assignment used for coding. *Bit-plane* coding is a simple and natural embedded coding technique that sequentially encodes the bits in the binary representation of the coefficients produced by a linear (e.g., wavelet) transformation of the image data. Until recently, the importance of the ordering problem had not been appreciated, and most early schemes, especially those based on context modeling and arithmetic coding, simply encode bit-planes in order of decreasing significance and according to a fixed scanning pattern within bit-planes. A more principled approach to the ordering problem was proposed in [1, 2, 3].

In this work, we formulate a fairly general framework for the bit-plane technique, the embedding problem, and the desired characteristics of the solution. A generalized notion of bit-plane coding is formalized as a sequence of *steps*, each step culminating with the encoding of either a ternary *significance* event (whether or not a coefficient becomes non-zero at a certain precision level, and possibly its sign), or a binary *refinement* event (an additional precision bit for an already significant coefficient). We index coefficients linearly as a sequence $x^n = x_1 x_2 \cdots x_n$, and denote by $Q_i^{(m)}$ the value of x_i quantized by a dead-zone quantizer with step size $2^{-(m_0+m)}\Delta$, where $m \geq 0$ is the *precision level* of $Q_i^{(m)}$, the integer m_0 satisfies $1 > 2^{m_0} \max_i |x_i|/\Delta \geq 1/2$, and $\Delta > 0$. Thus, the m-th bit-plane is given by the values of $Q_i^{(m)}$ conditioned on $Q_i^{(m-1)}$, $1 \leq i \leq n$. We denote by $\mathcal{Q}_j$ the information encoded up through and including step j, by I_j the index of the coefficient whose quantized representation is updated at step j, and by M_j the new level of precision attained on that coefficient with the update. Finally, we seek functions $\{f_j(\cdot)\}$ such that $I_j = f_j(\mathcal{Q}_{j-1})$, and probability assignments $p_j(Q_{I_j}^{(M_j)} | \mathcal{Q}_{j-1})$, used to encode the events. A sequence of pairs $\{(f_j, p_j)\}$ characterizes a generalized bit-plane coding scheme.

The selection of $\{(f_j, p_j)\}$ should strive to minimize, in some sense, a distortion measure $D(R)$ over as wide a range of rates R as possible, and for as many images as possible. The resulting global optimization problem appears intractable at present, which has lead to more localized, "greedy" heuristic approaches. In [2], the following *embedding principle* is defined: Select I_j so as to maximize $E[D_{j-1} - D_j \mid \mathcal{Q}_{j-1}]/E[R_j - R_{j-1} \mid \mathcal{Q}_{j-1}]$, the expected distortion reduction per expected bit of description. Here, D_j and R_j denote, respectively, the distortion and total code length after step j, and expectation is taken with respect to some model for x^n. The separation of significance and refinement decisions in EZW [4] roughly conforms to this principle.

Although the embedding principle can still be computationally demanding [3], it can also be applied to derive an *intra-bit-plane* ordering of decisions. In this framework, we generalize results in [2] to show that for a broad class of conditional distributions on $\{x^n\}$, the principle dictates the encoding of significance decisions in decreasing order of their likelihood of being non-zero. This result follows from Proposition 1 below, where subscripts f_k denote the underlying densities, p_{m,f_k} is the conditional probability that $|Q_i^{(m+1)}| = 1$, and $D_{m,f_k}(0)$ (resp. $R_{m,f_k}(0)$) denotes the decrement (resp. increment) in distortion (resp. ideal code length) when encoding $Q_i^{(m+1)}$ conditioned on $Q_i^{(m)} = 0$.

Proposition 1 *Given two symmetric densities f_1 and f_2 having the property that $f_1(y)/f_1(x) \leq f_2(y)/f_2(x)$ for all $0 \leq x < y$, then, the following hold for all m, i and Δ:*

1. $p_{m,f_1} \leq p_{m,f_2}$.
2. $E_{f_1}[x_i \mid Q_i^{(m)} = 1] \leq E_{f_2}[x_i \mid Q_i^{(m)} = 1]$.
3. $D_{m,f_1}(0)/R_{m,f_1}(0) \leq D_{m,f_2}(0)/R_{m,f_2}(0)$.

Proposition 1 covers zero-mean Laplacian and, more broadly, generalized Gaussian densities. These families are often used to model wavelet transform coefficients.

The established equivalence leads to an effective implementation of the embedding principle as shown in [2], where context modeling for ordering and coding are combined. These ideas and techniques have been incorporated into the algorithm at the core of the emerging image compression standard JPEG2000. The formal framework presented also provides new insight into the effectiveness of other established practical algorithms like SPIHT [5].

References

[1] J. Li and S. Lei. Rate-distortion optimized embedding. *Picture Coding Symposium,* Berlin, pp. 201–206, 1997.

[2] E. Ordentlich, M. Weinberger, and G. Seroussi. A low-complexity modeling approach for embedded coding of wavelet coefficients. *Proc. DCC'98*, Snowbird, March 1998.

[3] J. Li and S. Lei. An embedded still image coder with rate-distortion optimization. *IEEE Trans. Image Proc.*, 8(7), 1999.

[4] J. M. Shapiro. Embedded image coding using zerotrees of wavelet coefficients. *IEEE Trans. Signal Proc.*, 41(12), 1993.

[5] A. Said and W.A. Pearlman. A new, fast, and efficient image codec based on set partitioning in hierarchical trees. *IEEE Trans. on Circuits and Systems for Video Tech.*, 6(3), 1996.

[1] Work done while the author was at HP Labs.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Universal Lossless Data Compression with Side Information by using a Conditional MPM Grammar Transform*

En-hui Yang[1] Alexei Kaltchenko[2] John C. Kieffer[3]

I. Introduction and Algorithm

Recently proposed in [1], the MPM (Multilevel Pattern Matching) grammar transform underlies a lossless data compression algorithm developed in [1]. In this paper, we extend the MPM grammar transform to the case of side information known to both the encoder and decoder, yielding a conditional MPM grammar transform which is referred to as the CMPM(r, I) transform throughout this paper. Based on the CMPM(r, I) transform, we develop a universal lossless data compression algorithm with side information called the CMPM algorithm, which has linear time and storage complexity and asymptotically achieves the conditional entropy rate of any stationary, ergodic source pair. The advantage of using side information, if any, for data compression is obvious; one can considerably reduce the compression rate if the side information is highly correlated with a sequence to be compressed.

Let $\mathcal{A}^n$ denote the set of all sequences of length n drawn from an finite alphabet $\mathcal{A}$, and let $x^n \triangleq x_1 \dots x_n \in \mathcal{A}^n$. In the CMPM algorithm, x^n is compressed indirectly via the CMPM(r, I) transform (for some positive integer parameters r and I) followed by conditional arithmetic coding. The input to the transform is a sequence of pairs $\binom{x_1}{y_1}, \dots, \binom{x_n}{y_n}$ from a joint alphabet $\mathcal{A} \times \mathcal{A}_y$, where the sequence y^n, drawn from the finite alphabet $\mathcal{A}_y$, is regarded as side information and known to both the encoder and decoder. The transform output is a multilevel structure called a CMPM grammar, in which each level i is represented by a pair of sequences $v^{(i)} \triangleq v_1^{(i)} \dots v_{|v^{(i)}|}^{(i)}$ and $t^{(i)} \triangleq t_1^{(i)} \dots t_{|t^{(i)}|}^{(i)}$. The sequence $v^{(i)}$ is then encoded conditionally on $t^{(i)}$ by a zero-order arithmetic encoder for $i = I, I-1, \dots, 0$.

II. CMPM(r, I) Grammar Transform

To simplify the description of the transform, we assume that n is a multiple of r^I. Then, the CMPM(r, I) transform generates the levels I through 2 by repeating the following three steps for each level i:

S1: $(i = I)$ Partition x^n into blocks of $\mathcal{A}$-symbols of length r^I. Denote these blocks by variables $\tilde{v}_1^{(I)}, \dots, \tilde{v}_{n/r^I}^{(I)}$ and the resulting sequence $\tilde{v}_1^{(I)} \dots \tilde{v}_{n/r^I}^{(I)}$ by $\tilde{v}^{(I)}$. Analogously, partition y^n into blocks of $\mathcal{A}_y$-symbols of length r^I, and denote these blocks by variables $\tilde{t}_1^{(I)}, \dots, \tilde{t}_{n/r^I}^{(I)}$, and the resulting sequence $\tilde{t}_1^{(I)} \dots \tilde{t}_{n/r^I}^{(I)}$ by $\tilde{t}^{(I)}$. For brevity, we will call a block of $\mathcal{A}$-symbols an "$\mathcal{A}$-block" and a block of $\mathcal{A}_y$-symbols an "$\mathcal{A}_y$-block".

S1: $(i < I)$ For every j such that $v_j^{(i+1)} = s$, partition the $\mathcal{A}$-block $\tilde{v}_j^{(i+1)}$ and the $\mathcal{A}_y$-block $\tilde{t}_j^{(i+1)}$ into r sub-blocks of length r^i, yielding a sequence $\tilde{v}^{(i)}$ of $\mathcal{A}$-blocks and a sequence $\tilde{t}^{(i)}$ of $\mathcal{A}_y$-blocks.

S2: Visit every $\mathcal{A}_y$-block in the sequence $\tilde{t}^{(i)}$ from left to right, and label all identical $\mathcal{A}_y$-blocks with the same integers and all distinct $\mathcal{A}_y$-blocks with distinct integers in increasing order, starting with 1. Denote each label, or a *y-token*, corresponding to an $\mathcal{A}_y$-block $\tilde{t}_j^{(i)}$ by $t_j^{(i)}$. For every distinct y-token γ, let $\tilde{v}^{(i)}|\gamma$ denote the subsequence $\left\{\tilde{v}_j^{(i)} : \ t_j^{(i)} = \gamma\right\}$. We call this subsequence a *conditional subsequence of* $\tilde{v}^{(i)}$ since $\tilde{v}^{(i)}|\gamma$ can be regarded as the sequence $\tilde{v}^{(i)}$ conditioned on the y-token γ. All conditional subsequences of $\tilde{v}^{(i)}$ are processed independently from each other in step **S3**.

S3: For each distinct y-token γ, visit every $\mathcal{A}$-block in the conditional subsequence $\tilde{v}^{(i)}|\gamma$ from left to right and label the first appearance of each distinct $\mathcal{A}$-block α in this subsequence by a special symbol 's'. If the same $\mathcal{A}$-block α appears in $\tilde{v}^{(i)}|\gamma$ again, label it by an integer so that all identical $\mathcal{A}$-blocks α in $\tilde{v}^{(i)}|\gamma$, except for the most left one, will be labeled by the same integer, which is just the number of distinct $\mathcal{A}$-blocks in $\tilde{v}^{(i)}|\gamma$ up to the first appearance of the $\mathcal{A}$-block α inclusive. We use variable $v_j^{(i)}$ to denote the label of $\mathcal{A}$-block $\tilde{v}_j^{(i)}$ in $\tilde{v}^{(i)}$.

For level 1, we perform only step **S1**, and instead of performing steps **S2** and **S3**, we let $v^{(0)}$ and $t^{(0)}$ be $\tilde{v}^{(0)}$ and $\tilde{t}^{(0)}$ respectively.

III. Optimality Results

Let $r_{cmpm}(x^n|y^n)$ be the compression rate in bits per letter resulting from using our CMPM algorithm to encode x^n given y^n. Let $r_k^*(x^n|y^n)$ be the smallest compression rate among all conditional arithmetic coding algorithms with k contexts which condition on y^n and operate letter by letter. Then, based on the framework of grammar-based codes[2], we have established the following optimality results:

Theorem 1. $\max_{\substack{x^n \in \mathcal{A}^n \\ y^n \in \mathcal{A}_y^n}} \left[r_{cmpm}(x^n|y^n) - r_k^*(x^n|y^n)\right] = O\left(\frac{1}{\log n}\right)$

Corollary 1. *For any stationary, ergodic source pair* $XY = \{X_iY_i\}_{i=1}^{\infty}$ *with alphabet* $\mathcal{A} \times \mathcal{A}_y$, $r_{cmpm}(x^n|y^n)$ *converges to* $H_\infty(X|Y) \triangleq \lim_{m\to\infty}\left(\frac{1}{m}H(X_1, \dots, X_m|Y_1, \dots, Y_m)\right)$ *with probability one as* $n \to \infty$.

References

[1] *J. C. Kieffer, E.-H. Yang, G. Nelson, and P. Cosman*, "Lossless compression via multilevel pattern matching", *IEEE Trans. on Inform. Theory*, July, 2000.

[2] E.-H. Yang and J. C. Kieffer, "Universal Source Coding Theory Based on Grammar Transforms", *Proc. 1999 IEEE Inform. Theory and Comm. Workshop (Kruger National Park, South Africa)*, pp. 75-77.

*This work was supported in part by NSERC of Canada under Grant RGPIN203035-98, by CITO, by the Premier's Research Excellence Awards of Ontario, and by NSF under Grant CCR-9902081.

[1,2]ECE Department, University of Waterloo, Waterloo, ON N2L3G1, Canada, {ehyang, akaltche}@bbcr.uwaterloo.ca.

[3]ECE Department, University of Minnesota, Minneapolis, MN 55455, USA, kieffer@ece.umn.edu.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Balanced and Almost Balanced Binary Sequences of Period $p^m - 1$ with Optimal Autocorrelation Using the Polynomial $(z+1)^d + az^d + b$ over GF(p^m)

Jong-Seon No
School of Electrical Eng.
Seoul National University
Seoul 151-742, Korea
e-mail:jsno@snu.ac.kr

Habong Chung
School of EE Eng.
Hong-Ik University
Seoul 121-791, Korea
e-mail:habchung@wow.hongik.ac.kr

Hong-Yeop Song
Dept. of EC Eng.
Yonsei University
Seoul 120-749, Korea
e-mail:hysong@bubble.yonsei.ac.kr

Kyeongcheol Yang
Dept. of EE Eng.
POSTECH
Pohang 790-784, Korea
e-mail:kcyang@postech.ac.kr

Jung-Do Lee
Dept. of Electronic Eng.
Konkuk University
Seoul 143-701, Korea
e-mail:hawk@kkucc.konkuk.ac.kr

Tor Helleseth
Dept. of Informatics
University of Bergen
N-5020 Bergen, Norway
e-mail:torh@ii.uib.no

Abstract — **In this paper, we present a construction for binary sequences $\{s(t)\}$ of period $N = p^m - 1$ for an odd prime p based on the polynomial $(z+1)^d + az^d + b$ with *optimal three-level autocorrelation*.**

I. Construction of New Binary Sequences

Recently, there has been a big progress in constructing balanced binary sequences of period $2^m - 1$ with ideal autocorrelation [1, 2, 4]. The idea of the (new) construction is to use a special polynomial over finite fields. In this paper, we generalize it to generate *binary* sequences of period $p^m - 1$ with optimal autocorrelation for any prime p and an integer m.

Let F denote the field of p^m elements and $F^* = F\backslash\{0\}$. For $a, b \in F$ and a positive integer d, consider the subset of F^* given by

$$I(a,b) = \{\, x \,|\, x = (z+1)^d + az^d + b,\ z \in F \,\}\backslash\{0\}.$$

The characteristic sequence $\{s_{a,b}(t)\}$ of the set $I(a,b)$ in F^* is defined by $s_{a,b}(t) = 1$ if $\alpha^t \in I(a,b)$ and $s_{a,b}(t) = 0$ otherwise, where α is a primitive element of F.

Proposition 1 *Let $p \geq 3$, $d = 2$, and $a, b \in F$ with $a+1 \neq 0$. Then, $\{s_{a,b}(t)\}$ is a cyclic shift of the characteristic sequence of the polynomial $z^2 - c$, where $c \in F$ depends on b.*

By virtue of the above proposition, we may define, for short notation,

$$I_c = \{\, x \mid x = z^2 - c,\ z \in F \,\}\backslash\{0\}, \quad (1)$$

$$I_c^* = \{\, x \mid x = z^2 - c,\ z \in F^* \,\}\backslash\{0\}, \quad (2)$$

$\{s_c(t)\}$ ($\{s_c^*(t)\}$) to be its characteristic sequence in F^* of period $N = p^m - 1$, and $\theta_c(\tau)$ ($\theta_c^*(\tau)$) its periodic autocorrelation function. There are two more cases in which $\{s_{a,b}(t)\}$ becomes a cyclic shift of $\{s_c(t)\}$ for some $c \in F$.

Proposition 2 *Let $p \geq 5$, $d = 3$, and $a = -1$. For any positive integer m and any $b \in F$, $\{s_{a,b}(t)\}$ is a cyclic shift of $\{s_c(t)\}$, where $c \in F$ depends on b.*

Proposition 3 *Let $p = 3$, $d = 4$, $a = 1$, and m is odd so that $N = 3^m - 1 \equiv 2 \pmod 4$. For any $b \in F$, $\{s_{a,b}(t)\}$ is a cyclic shift of $\{s_c(t)\}$, where $c \in F$ depends on b.*

Theorem 4 *Let $\{s_c(t)\}$ and $\{s_c^*(t)\}$ be the characteristic sequences of I_c and I_c^*, respectively, of period $N = p^m - 1$, and α be a primitive element of F. Then, both $\{s_\alpha^*(t)\}$ and $\{s_1(t)\}$ are balanced, and both $\{s_\alpha(t)\}$ and $\{s_1^*(t)\}$ are almost balanced. Furthermore, we have (i) $s_\alpha^*(t) = s_1(t-1) + 1$ for all t; (ii) $s_\alpha(t) = s_1^*(t-1) + 1$ for all t; (iii) $s_\alpha(N/2+1) = s_1(N/2) = 1$ and $s_1(t) = s_\alpha(t+1) + 1$ for all $t \neq N/2$; and (iv) $s_\alpha^*(N/2) = s_1^*(N/2-1) = 0$ and $s_1^*(t) = s_\alpha^*(t+1) + 1$ for all $t \neq N/2 - 1$.*

Theorem 5 *The sequences $\{s_\alpha^*(t)\}$ and $\{s_1(t)\}$ of period N are balanced and have optimal autocorrelation. Specifically, for $\tau \not\equiv 0 \pmod N$*

$$\theta_\alpha^*(\tau) = \begin{cases} -4\epsilon, & \text{if } N \equiv 0 \pmod 4 \\ 2 - 4\epsilon, & \text{if } N \equiv 2 \pmod 4 \end{cases}$$

where $\epsilon \in \{0, 1\}$.

Theorem 6 *The sequences $\{s_1^*(t)\}$ and $\{s_\alpha(t)\}$ of period N are almost balanced and have optimal autocorrelation. Specifically, for $\tau \not\equiv 0 \pmod N$,*

$$\theta_1^*(\tau) = \begin{cases} -4\epsilon, & \text{if } N \equiv 0 \pmod 4 \\ 2 - 4\epsilon, & \text{if } N \equiv 2 \pmod 4 \end{cases}$$

where $\epsilon \in \{0, 1\}$.

References

[1] J. F. Dillon, "Multiplicative Difference Sets via Additive Characters," preprint, 1998.

[2] Hans Dobbertin, "Kasami Power functions, permutation polynomials and cyclic difference sets," in Proceedings of *Difference Sets, Sequences and their Correlation Properties*, NATO Advanced Study Institute Workshop, held in Bad Windshiem, Germany, August 3-14, 1998.

[3] A. Lempel, M. Cohn, and W. L. Eastman, "A class of binary sequences with optimal autocorrelation properties," *IEEE Trans. Inform. Theory*, vol. 23, No. 1, pp. 38-42, Jan. 1977.

[4] J. -S. No, H. Chung, and M. -S. Yun, "Binary Pseudorandom Sequences of Period $2^m - 1$ with Ideal Autocorrelation Generated by the Polynomial $z^d + (z+1)^d$," *IEEE Trans. Inform. Theory*, vol. 44, No. 3, pp. 1278-1282, May 1999.

[5] T. Storer, *Cyclotomy and Difference Sets*, Lecture Notes in Advanced Mathematics, Markham Publishing Company, Chicago, 1967.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Inverse Hadamard Transforms of Two-Level Autocorrelation Sequences

Guang Gong
Department of Combinatorics and Optimization
University of Waterloo
Waterloo, Ontario, Canada.

Solomon W. Golomb
Communication Sciences Institute
Electrical Engineering/Systems
University of Southern California
Los Angeles, CA, U.S.A.

Abstract — It is well-known [1] that a balanced binary sequence $\{a_k\}$ of period $2^n - 1$ with two-level autocorrelation is constant on cyclotomic cosets, i.e. $\{a_{2k}\} = \{a_{k+r}\}$ for all k and some fixed value of r. Moreover, there is a cyclic shift of the original sequence for which $r = 0$. Such two-level autocorrelation sequences are in one-to-one correspondence with cyclic Hadamard difference sets with parameters $(2^n - 1, 2^{n-1} - 1, 2^{n-2} - 1)$. Perhaps best known among such sequences are the m-sequences, which correspond to Singer difference sets. For any primitive element α in $GF(2^n)$, the set of m-sequences is given by $S_q = \{Tr(\alpha^{qk})\}$, $(q, 2^n - 1) = 1$, where S_q and $S_{q'}$ are distinct m-sequences iff q and q' belong to different cyclotomic cosets.

If $B = \{b_k\}$ is any binary sequence of period $2^n - 1$ which is constant on cyclotomic cosets, then B can be written as a sum (term-by-term, modulo 2) of sequences of the form $\{Tr(\alpha^{qk})\}$, where q need not be coprime to $2^n - 1$. That is, the linear feedback sequences of all periods which divide $2^n - 1$ form a basis for the set of sequences which are constant on cyclotomic cosets. We conjecture (based on numerical evidence) that for two-level autocorrelation sequences, only values of q which belong to cyclotomic cosets of size n are involved in this basis representation. However, not all the component sequences in this representation need to be m-sequences.

It has recently been shown [2] that when n is odd, all the known cases of two-level autocorrelation sequences of period $2^n - 1$ have the same Hadamard transform as one of the m-sequences. A similar result holds for even n, but instead of an m-sequence, only a linear feedback sequence appears.

Using the inverse Hadamard transform, and starting with a single m-sequence (when n is odd), we can obtain all the known two-level autocorrelation sequences of period $2^n - 1$ which have no subfield factorization. (Here we say that the binary sequence $B = \{b_k\}$ where $b_k = f(\alpha^k)$ and $f(x) = \sum_q Tr(x^q)$ has a ***subfield factorization*** if there is m, a proper factor of n, such that $f(x)$ can be decomposed into a composition of a function from $GF(2^m)$ to $GF(2)$ and the trace function from $GF(2^n)$ to $GF(2^m)$.) We have verified this for odd $n \leq 19$. Interestingly, no previously unknown examples were found by this inverse Hadamard transform process for any odd $n \leq 19$. This is supporting evidence (albeit weak) for the conjecture that all families of cyclic Hadamard difference sets of period $2^n - 1$ having no subfield factorization are now known, at least for odd n.

We will continue to investigate odd values of n, and to look for analogous results with n even.

References

[1] S. Golomb, *Shift Register Sequences,* Holden-Day, Inc., 1967. Revised edition, Aegean Park Press, 1982.

[2] J.F. Dillon and H. Dobbertin, "New cyclic difference sets with Singer parameters," preprint, 12 August, 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Crosscorrelation Functions of m-Sequences and Their Decimation Sequences

Zhentao Zhang[1],Wei Sun,Yixian Yang,Zhengming Hu,and Xin Li
P. O. Box 126, Information Security Center
Beijing University of Posts and Telecommunications
100876 Beijing, China
e-mail: yxyang@bupt.edu.cn

Abstract — **Crosscorrelation functions $C_d(t)$ of m-sequences over finite field GF(p) and their decimation sequences are investigated in this paper.**

I. Introduction

Maximal length linear shift-register sequences (or called m-sequences) have desirable autocorrelation functions, thus they have been widely used, e.g. in crytography and communications. However, the problems about the crosscorrelation of m-sequences and their decimation sequences still keep open, although much research has been done.

Let p be a prime, n a positive integer, $q = p^n$, and GF(q) the finite field with q elements, Tr denote the trace function from GF(q) to GF(p),and α be a primitive element in GF(q), then the sequence $(a_i = \mathrm{Tr}(\gamma\alpha^i))_i$ is an m-sequence over GF(p) ([2, 4]), where$\gamma = \alpha^{-t}$ is an element of GF(q). The sequence $(b_i = a_{di} = \mathrm{Tr}(\gamma\alpha^{di}))_i$ is called a decimation sequence of $(a_i)_i$ with the decimation factor d.

Let $(a_i)_i$ and $(b_j)_j$ be periodic sequences over GF(p) with period l, and $\xi = e^{2\pi i/p}$ be the primitive complex pth root of unity, the **crosscorrelation function** of $(a_i)_i$ and $(b_j)_j$ is defined by

$$C_{ab}(t) = \sum_{i=0}^{l-1} \xi^{a_{i-t}\overline{\xi^{b_i}}} = \sum_{i=0}^{l-1} \xi^{a_{i-t}-b_i}, 0 \le t < l-1. \quad (1)$$

In particular, when $(a_i)_i$ is identical to $(b_j)_j$, $C_{ab}(t)$ is the **autocorrelation function** of $(a_i)_i$. In this paper, we consider only the case that $(a_i)_i$ is an m-sequence over GF(p) and $(b_j)_j$ is its decimation sequence with decimation factor d, so (1) can be simplified as

$$\begin{aligned} C_{ab}(t) &= \sum_{i=0}^{p^n-2} \xi^{a_{i-t}-b_i} \\ &= \sum_{i=0}^{p^n-2} \xi^{\mathrm{Tr}(\alpha^{i-t}-\alpha^{di})} \\ &= \sum_{x\in \mathrm{GF}(p^n)^*} \xi^{\mathrm{Tr}(\gamma x - x^d)} \\ &= -1 + \sum_{x\in \mathrm{GF}(p^n)} \xi^{\mathrm{Tr}(\gamma x - x^d)} \\ &= C_d(t) \end{aligned}$$

[1]Projected Supported by National Natural Sicence Foundation of China(No. 69802002, 69882002, 69772035), and by National "863" (No. 863-306-ZT05-05-2)

For convenience, we consider

$$1 + C_d(t) = \sum_{x\in \mathrm{GF}(p^n)} \xi^{\mathrm{Tr}(x-\gamma x^d)} \quad (2)$$

Muller [1] studied the upper bound of $|1+C_d(t)|$ for decimation factor $d = \frac{p^n+1}{p+1} + \frac{p^n-1}{2}$, n odd and $p = 3$, and proposed an open problem: what is the upper bound of $|1+C_d(t)|$ when $p > 3$? In this paper, we have solved this open problem and get more results.

II. Main Results

(1) If the decimation factor $d = \frac{p^n+1}{p+1} + \frac{p^n-1}{2}$, $p \equiv 3(\mathrm{mod}4)$, n odd, then

$$|1 + C_d(t)| \le \frac{1+p}{2}\sqrt{p^n}.$$

Therefore the problem proposed by Muller [1] is solved.

(2) If the decimation factor $d = \frac{p^n+1}{p+1}$, n odd, $p \equiv 3(\mathrm{mod}4)$, then

$$C_d(t) \in \{-1, -1+\sqrt{p^{n+1}}, -1-\sqrt{p^{n+1}}\}.$$

(3)Under the condition of (1),we have

$$P(|\,1 + C_d(t)\,| = \tfrac{1+p}{2}\sqrt{p^n}) < \tfrac{2}{p^2-1},$$
$$P(|\,1 + C_d(t)\,| = \sqrt{p^n}) \ge 1 - \tfrac{2}{p-1}.$$

(4)Under the condition of (2),we get the result:

$$P\,|\,1 + C_d(t)\,| = \sqrt{p}\sqrt{p^n}) \le \tfrac{1}{p-1},$$
$$P(1 + C_d(t) = 0) \ge 1 - \tfrac{1}{p-1}.$$

III. Conclusions

In this paper, we have studied in detail the crosscorrelation functions of m-sequences and their decimation sequences in two different cases. This paper generalizes the conclusion of Muller in [1], and therefore solved an open problem proposed by Muller in [1]. In addition, we have investigated the distribution of the value of crosscorrelation functions, and get the result that when p is large enough, the probability of the crosscorrelation function achieving the maximal absolute value is very small.

References

[1] Eva Nuria Müller, *On the Crosscorrelation of Sequences Over GF(p) with Short Periods*, IEEE Transaction on Information Theory, Vol.45, NO.1, pp.289-295, JANUARY 1999.

[2] R.Lidl and H.Niederreiter, *Finite Fields*, Vol.20 of Encyclopedia of Mathematics and its Applications. Reading, MA: Addison-wesley, 1980.

[3] Luogeng Hua, *the introduction of number theory*, Science press, Beijing, 1957.

[4] Zhexian Wan, *algebra and coding theory*, Science press, Beijing, 1980.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Constabent Properties of Golay-Davis-Jedwab Sequences

M.G.Parker[1]
Code Theory Group,Institutt for
Informatikk, University of
Bergen,N-5020 Bergen, Norway
e-mail: matthew@ii.uib.no

Abstract — **We conjecture that length 2^t bipolar sequences with optimal or near-optimal Hadamard and Negahadamard Peak Factors are exactly the set of Golay Complementary sequences, as formed using the Davis-Jedwab construction. It appears Golay sequences are both Bent and Negabent for lengths 2^t where t is even and $t \neq 2$ mod 3. We also conjecture this sequence family has near-maximum distance from all constaaffine functions.**

I. Introduction

The sum of aperiodic autocorrelations of Golay sequence pairs is a δ pulse [2]. [1, 4] describe a construction for length 2^t Golay sequences (Golay-Davis-Jedwab construction (GDJ)) that probably covers all Golay sequences of length 2^t. We define Hadamard, Negahadamard and Constahadamard Transforms (HT, NHT and CHT), these being multidimensional Cyclic, Negacyclic and Constacyclic Discrete Fourier Transforms (DFT). Negabent and Constabent sequences are sequences whose NHTs and CHTs, respectively, have completely flat power profile. Extensive computation suggests that bipolar GDJ sequences always have flat or near-flat HTs, NHTs and CHTs. It is conjectured that these sequences are the unique intersection of the set of bipolar sequences with Bent or known near-Bent properties with those with NegaBent or known near-NegaBent properties. It is known that GDJ sequences are Bent for length 2^t, t even, [3], but the near-Bent property for length 2^t, t odd, and the Negabent and near-Negabent properties are new results. It is conjectured that bipolar GDJ sequences are both Bent and Negabent for a specified infinite set of lengths and therefore their associated boolean functions have maximum distance from affine and negaaffine functions. Further computations suggest they have near-maximum distance from all constaaffine functions in all cases. This may be desirable for cryptographic applications.

II. The Constahadamard Transform

The Walsh-Hadamard Transform (HT), $\mathbf{H_t}$, is constructed from the direct product of 2-point DFT matrices, $\mathbf{H_t} = \mathbf{H_1} \otimes \mathbf{H_1} \otimes \mathbf{H_1} \otimes \ldots = \otimes_{i=1}^{t} \mathbf{H_1}$ where $\mathbf{H_1} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and $\otimes$ is the direct product. The Negahadamard Transform (NHT), $\mathbf{NH_t}$, is the direct product of 2-point Discrete Negacyclic Fourier Transform matrices, $\mathbf{NH_t} = \mathbf{NH_1} \otimes \mathbf{NH_1} \otimes \mathbf{NH_1} \otimes \ldots = \otimes_{i=1}^{t} \mathbf{NH_1}$ where $\mathbf{NH_1} = \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$, and $i^2 = -1$. The Constahadamard Transform (CHT), $\mathbf{C_{n,j}H_t}$, is the tth direct product of 2-point index j Discrete Constacyclic Fourier Transform (DCFT) matrices over nth complex roots where $2|n$, $\mathbf{C_{n,j}H_t} = \mathbf{C_{n,j}H_1} \otimes \mathbf{C_{n,j}H_1} \otimes \mathbf{C_{n,j}H_1} \otimes \ldots = \otimes_{i=1}^{t} \mathbf{C_{n,j}H_1}$ where $\mathbf{C_{n,j}H_1} = \begin{pmatrix} 1 & \alpha^j \\ 1 & \alpha^{j+\frac{n}{2}} \end{pmatrix}$, $\alpha = e^{\frac{2\pi i j}{n}}$, j is one of the $\frac{\phi(n)}{2}$ integers in Z_n mutually prime to n and less than $\frac{n}{2}$, and ϕ is Euler's Totient Function. e.g., $\mathbf{H_t} = \mathbf{C_{2,1}H_t}$, $\mathbf{NH_t} = \mathbf{C_{4,1}H_t}$, and, $\mathbf{C_{12,5}H_1} = \begin{pmatrix} 1 & \alpha^5 \\ 1 & \alpha^{11} \end{pmatrix}$, where $\alpha = e^{\frac{2\pi i}{12}}$.

Constahadamard Peak Factor: Let $\mathbf{A} = \mathbf{C_{n,j}H_t a} = (A_0, A_1, \ldots, A_{2^t-1})^T$ for some n, j. The Constahadamard Peak Factor of $\mathbf{a}$ is CHPF($\mathbf{a}$) $= 2^{-t}\max\{A_i A_i^* | 0 \leq i < 2^t\}$. All CHT matrices obey Parseval's Theorem. $1.0 \leq$ CHPF($\mathbf{a}$) $\leq 2^t$ $\forall n, j$ if $\mathbf{a}$ is unimodular. A unimodular sequence is Bent if it has Hadamard Peak Factor (HPF) of 1.0, Negabent if it has Negahadamard Peak Factor (NHPF) of 1.0, and ConstaBent if it has CHPF of 1.0.

III. CHPF Properties of GDJ Sequences

GDJ Sequences are detailed in [1, 4]. They are certain second order cosets of Reed Muller $(1, t)$ which are length 2^t Golay Complementary Sequences. Bipolar GDJ sequences are bent for even t [3]. From computational results we state,

Conjecture 1: *The HPF of a bipolar GDJ sequence is* 1.0 *for even t and* 2.0 *for odd t.*

Conjecture 2: *The NHPF of a bipolar GDJ sequence is* 1.0 *for $t \neq 2$ mod 3 and* 2.0 *for $t = 2$ mod 3.*

Conjecture 3: *Bipolar GDJ sequences of length 2^t are both Bent and Negabent for even t, $t \neq 2$ mod 3.*

Conjecture 4: *Let* $\mathbf{F}$ *be the set of length 2^t bipolar sequences with HPF = 1.0 and 2.0 for t even and odd, respectively. Let* $\mathbf{G}$ *be the set of length 2^t bipolar sequences with NHPF = 1.0 and 2.0 for $t \neq 2$ mod 3 and $t = 2$ mod 3, respectively. The set of GDJ bipolar sequences is exactly* $\mathbf{F} \cap \mathbf{G}$.

Conjecture 5: *The CHPF of GDJ bipolar sequences is always ≤ 2.00, $\forall n, t, j$.*

Conjecture 3 follows from Conjectures 1 and 2. Conjecture 4 may not hold for t large. Conjecture 5 implies GDJ boolean functions have near-maximum distance from all constaaffine functions.

IV. Conclusion

Bipolar Golay-Davis-Jedwab (GDJ) sequences appear not only to possess low one-dimensional peak factors ≤ 2.0, but also possess low multi-dimensional peak factors ≤ 2.0. We conjecture these sequences are Bent or near-Bent and NegaBent or near-NegaBent. They appear to be Bent and Negabent for lengths 2^t, $t = 0$ or 4, mod 6.

References

[1] J.A.Davis,J.Jedwab, "Peak-to-mean Power Control in OFDM, Golay Complementary Sequences and Reed-Muller Codes," *HP Laboratories Tech. Rep.*, HP Laboratories Bristol, HPL-97-158, Dec '97

[2] M.J.E.Golay, "Complementary Series," *IRE Trans. Inform. Theory*, Vol IT-7, pp 82–87, Apr '61

[3] F.J.MacWilliams,N.J.A.Sloane, **The Theory of Error-Correcting Codes**, Amsterdam: North-Holland, '77

[4] K.G.Paterson, "Generalised Reed-Muller Codes and Power Control in OFDM Modulation," *HP Tech. Rep., HPL-98-57* March '98

[1]This work was funded by NFR Project Number 119390/431

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Outage Analysis for Multiple Access Channel with Rayleigh Fading

Ido Bettesh and Shlomo Shamai (Shitz)
EE department, Technion - IIT
Haifa, Israel
e-mail: idob@tx.technion.ac.il
e-mail: sshlomo@ee.technion.ac.il

Abstract — **In this paper we consider the outage probabilities of three multiuser scheduling/power control algorithm: TDMA, the K&H algorithm which achieves maximal Shannon capacity [1], and TD-KH - a combination of the former two [2]. For flat block fading channel, the outage probability of these algorithms can be asymptotically modeled as a reward renewal process. Employing Large deviations analysis, TDMA and TD-KH are shown to be superior over K&H under outage probability criteria.**

I. Introduction

The maximal Shannon capacity for single user in flat fading channel (channel state information assumed at the transmitter) is achieved by the water pouring solution for each channel use [3]. The K&H [1] power control expands it for multiple users i.e., only the user with the best fading should transmit. The K&H power control has a significant drawback: Assuming flat block fading channel, an arbitrary user might wait for a long time until it reaches temporal maximal fading, allowing him to transmit. Thus, when delay criteria are imposed, the K&H power control is not always suitable. Note the contradicting approach of K&H when compared to TDMA where the time interval between successive transmissions of each user is fixed.

The TD-KH algorithm can be regarded as a compromise between the above contradicting approaches. Its Shannon capacity is below that of K&H and above TDMA capacity and by setting a user controlled parameter can achieve any value between the two [2]. In this article we show that TDMA and TD-KH algorithms are advantageous over K&H when outage capacity is concerned. Exact analytic calculation seems intractable, we adhere therefore to asymptotic calculation for large number of slots $T \to \infty$. The achieved result is applicable for general renewal process defined over discrete time.

II. Channel model

For the sake of clarity, we shortly repeat the description of the TD-KH algorithm. Consider a multiple-user flat block fading Gaussian channel [3] where each of the N users has the same independent fading statistics and the same average power. Setting a user chosen parameter $L \geq N-1$ the scheduling policy of TD-KH is as follows: Inspect the previous L slots before the next one. If each of the N users has transmitted at least once in one of the L slots then let the user with the best fading transmit by the K&H power control. Otherwise, the user who has not transmitted in the last L slots (there is only one possible user) transmits using fixed power as in TDMA. Note that for $L = N - 1$ the TD-KH algorithm degenerates into TDMA while for $L/N \to \infty$ it identifies with K&H.

Assume an arbitrary user transmitted in n slots out of T contiguous slots. We define the outage as the probability of the average information transmitted in these n slots being less then a certain threshold $\alpha\bar{C}$ where $\alpha \in [0,1]$ and $\bar{C}$ is the average sum rate capacity. Formally,

$$\text{Outage Pr}(T) = Pr(n=0) + \sum_{n=1}^{T} Pr(n) Pr\Big(\frac{1}{n}\sum_{j=1}^{n} C_j < \alpha\bar{C}\Big) \tag{1}$$

where C_j is information transmitted in each of these n slots by the user.

III. Outage asymptotic

Analytic calculation of (1) seems complicated. However, we notice that both TDMA and K&H are renewal process since the time intervals X_1 between two subsequent transmission of the same user are either fixed (TDMA) or iid (K&H). The TD-KH algorithm can be shown to behave asymptotically also as a renewal process. In addition $X_2 = C_j$ depends at most on the last interval length, thus making the process $\mathbf{X} = (X_1, X_2)$ a reward renewal process. Using Cramér's theorem for $\mathbb{R}^2$ we reach:

$$\lim_{T\to\infty} -(1/T)\log(\text{Outage prob}(T)) = \Big[\frac{\partial}{\partial y_1} I(y_1, \alpha\bar{C})\Big] \tag{2}$$

$$\text{where} \quad I(y_1, \alpha\bar{C}) - \frac{\partial}{\partial y_1} I(y_1, \alpha\bar{C}) = 0\,,$$

where $I(y_1, y_2)$ is the rate function of $(X_1, X2)$.

IV. Results and Conclusions

Inspecting (2) we note that the outage exponent of TDMA and TD-KH increase both as α decreases, where the TDMA exponent is always above the TD-KH . For $\alpha \in [0, \alpha_0\bar{C}]$ the TDMA and K&H exponents are larger then K&H. The K&H exponent is upper bounded by $\log(1 - 1/N)$ even for $\alpha \to 0$. The TD-KH exponent on the other hand, is not upper bounded as in K&H even for large L/N (e.g. $L/N = 5$). Thus, we conclude that under the asymptotic outage criteria the TD-KH is superior over K&H.

References

[1] R. Knopp and P. A. Humblet, "Information capacity and power control in single-cell multiuser communications," in *Int. Con on Commun., ICC'95*, (Seattle, WA), pp. 331–335, June 18-22 1996.

[2] I. Bettesh and S. Shamai (Shitz), "A low delay algorithm for the multiple access channel with Rayleigh fading," in *The ninth IEEE int. Symposium, PIMRC '98*, September 8-11 1998.

[3] E. Biglieri, J. Proakis, and S. Shamai (Shitz), "Fading channels: Information-theoretic and communications aspects," *IEEE Trans. Inform. Theory*, vol. 44, pp. 2619–2692, October 1998.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

An MGF-Based Numerical Technique for the Outage Probability Evaluation of Diversity Systems[1]

Young-Chai Ko
Department of ECE
University of Minnesota
Minneapolis, MN, U.S.A.
ycko@ece.umn.edu

Mohamed-Slim Alouini
Department of ECE
University of Minnesota
Minneapolis, MN, U.S.A.
alouini@ece.umn.edu

Marvin K. Simon
Jet Propulsion Laboratory (JPL)
California Institute of Technology
Pasadena, CA, U.S.A.
marvin.k.simon@jpl.nasa.gov

Abstract — **Relying on a simple algorithm for the Laplace transform inversion of cumulative distribution functions, we develop a moment generating function-based numerical technique for the outage probability evaluation of maximal-ratio and equal-gain combining over generalized fading channels.**

I. Introduction

Recently, a unified moment generating function (MGF)-based approach was adopted for the exact average error rate analysis of several modulation schemes in conjunction with maximal-ratio combining (MRC) and equal-gain combining (EGC) diversity reception [1]. In addition to the average error rate, outage probability, P_{out}, is another standard performance criterion of communication systems operating over fading channels. It is defined as the probability that the combined signal-to-noise ratio (SNR), γ_t, falls below a threshold γ_{th}, i.e., $P_{\text{out}} = P[0 \le \gamma_t \le \gamma_{\text{th}}] = \int_0^{\gamma_{\text{th}}} p_{\gamma_t}(\gamma_t)\, d\gamma_t$, where $p_{\gamma_t}(\gamma_t)$ is the probability density function (PDF) of γ_t. Since finding the PDF of γ_t in closed form is often restricted to some special cases while the MGF of γ_t, $\mathcal{M}_{\gamma_t}(s) = E_{\gamma_t}[e^{s\gamma_t}]$, can be obtained in a simple form for various fading conditions, we present an MGF-based approach for the outage probability evaluation of diversity systems over generalized fading channels in which the diversity paths are not necessarily independent, identically distributed nor even distributed according to the same family of distribution.

II. Outage Probability Evaluation

The total conditional SNR per symbol, γ_t, at the output of an L-branch MRC combiner or a postdetection EGC combiner is given by $\gamma_t = \sum_{l=1}^{L} \gamma_l$, where γ_l is the lth-path instantaneous SNR per symbol. Applying the numerical technique developed in [2] and after some manipulation we obtain P_{out} as [3]

$$P_{\text{out}} = P_{\gamma_t}(\gamma_{\text{th}}; A, N, Q) = \frac{2^{-Q} e^{A/2}}{\gamma_{\text{th}}} \sum_{q=0}^{Q} \binom{Q}{q} \sum_{n=0}^{N+q} \frac{(-1)^n}{\beta_n} \times \mathcal{R}\left\{ \frac{\mathcal{M}_{\gamma_t}\left(-\frac{A+2\pi jn}{2\gamma_{\text{th}}}\right)}{\frac{A+2\pi jn}{2\gamma_{\text{th}}}} \right\} + E(A, N, Q), \quad (1)$$

where the parameters A, N, and Q can be set to guarantee an overall error given by

$$|E(A, N, Q)| \simeq \frac{e^{-A}}{1-e^{-A}} + \left| \frac{2^{-Q} e^{A/2}}{\gamma_{\text{th}}} \sum_{q=0}^{Q} (-1)^{N+1+q} \binom{Q}{q} \times \mathcal{R}\left\{ \frac{\mathcal{M}_{\gamma_t}\left(-\frac{A+2\pi j(N+q+1)}{2\gamma_{\text{th}}}\right)}{\frac{A+2\pi j(N+q+1)}{2\gamma_{\text{th}}}} \right\} \right|. \quad (2)$$

[1]This work was supported by the Graduate School of the University of Minnesota and by the National Science Foundation.

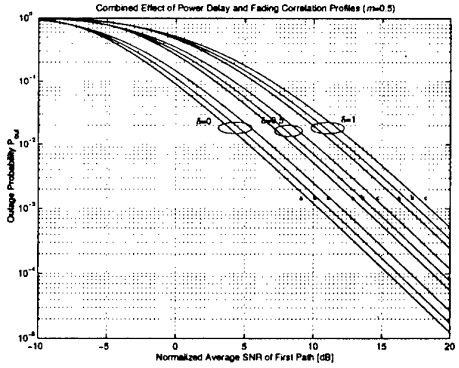


Figure 1: Outage probability with MRC or postdetection EGC ($L = 4$) versus normalized average SNR of the first path $\overline{\gamma}_1/\gamma_{\text{th}}$ over an exponentially decaying PDP and an exponential correlation profile across the mutipaths ((a) $\rho = 0$, (b) $\rho = 0.2$, and (c) $\rho = 0.4$).

For coherent EGC, the conditional combined SNR per symbol, γ_t, is given by $\gamma_t = \frac{1}{L}\left(\sum_{l=1}^{L} \sqrt{\gamma_l}\right)^2$. The outage probability P_{out} can hence be rewritten as $P_{\text{out}} = P[0 \le \tilde{\gamma}_t \le \tilde{\gamma}_{\text{th}}]$, where $\tilde{\gamma}_t \triangleq \sum_{l=1}^{L} \sqrt{\gamma_l}$ and $\tilde{\gamma}_{\text{th}} \triangleq \sqrt{L\gamma_{\text{th}}}$. Since the MGF of $\sqrt{\gamma_l}$ can be found in closed-form for the Nakagami-m case, the outage probability of coherent EGC receivers can also be computed using (1), and the corresponding numerical error can be estimated from (2), where in these two expressions γ_t and γ_{th} are replaced by $\tilde{\gamma}_t$ and $\tilde{\gamma}_{\text{th}}$, respectively.

III. Numerical Example

As an illustration of the applicability of the approach to cases where a "classical" PDF-based approach fails to give an easy-to-compute solution, Fig. 1 shows the outage probability of MRC RAKE reception over a Nakagami chanel with an exponentially decaying power delay profile (PDP) ($\overline{\gamma}_l = e^{-\delta(l-1)}\overline{\gamma}_1$, where δ is the power decay factor) and an exponential correlation profile (such as $\rho_{ll'} = \rho^{|l-l'|}$) across the multipaths.

References

[1] M. K. Simon and M. -S. Alouini, "A unified approach to the performance analysis of digital communications over generalized fading channels," *Proc. IEEE*, vol. 86-9, pp. 1860-1877, September 1998.

[2] J. Abate and W. Whitt, "Numerical inversion of Laplace transforms of probability distribution," *ORSA Journal on Computing*, vol. 7, no. 1, pp. 36–43, 1995.

[3] Y. -C. Ko, M. -S. Alouini, and M. K. Simon, "Outage probability of diversity systems over generalized fading channels," To appear *IEEE Trans. Commun.*

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Minimum Outage Probability and Optimal Power Allocation for Fading Multiple-Access Channels[1]

Lifang Li
California Institute of Technology
<lifang@systems.caltech.edu>

Andrea Goldsmith
Stanford University
<andrea@systems.stanford.edu>

Abstract — **We derive the optimal power allocation and minimum outage probability for fading multiple-access channels under the assumption that both the transmitters and the receiver have perfect channel side information. This minimum outage probability implicitly defines the outage capacity region. Two different assumptions about whether the outage declaration from each user is simultaneous or independent are considered.**

Wireless communication channels vary over time due to user mobility. Assuming that the channel side information (CSI) is available at both the transmitter(s) and the receiver(s), the zero-outage capacity regions are derived for fading multiple-access channels (MAC) and for fading broadcast channels in [1] and [2], respectively. This type of capacity is the maximum constant rate that can be maintained in all fading conditions through optimal power control. By allowing some transmission outage under severe fading conditions, the maximum rate that can be kept constant during non-outage will increase. Finding the optimal power allocation that achieves the outage capacity for a given outage probability is tantamount to deriving the allocation strategy that minimizes the outage probability for a given rate or rate vector. This minimum outage probability problem is solved for a single-user fading channel in [3] and for a fading broadcast channel in [2].

In this paper we consider the optimal power allocation and minimum outage probability problem for an M-user fading MAC under different assumptions about whether the outage declaration from each user is simultaneous or independent. A discrete-time M-user fading MAC model as discussed in [1] is characterized by the output

$$Y(n) = \sum_{i=1}^{M} \sqrt{H_i(n)} X_i(n) + Z(n),$$

where $X_i(n)$ and $H_i(n)$ are the transmitted waveform and the fading process of the ith user, respectively, and $Z(n)$ is the Gaussian noise with variance σ^2. For a slowly time-varying MAC, let $\mathbf{h} = (h_1, h_2, \cdots, h_M)$ be the joint fading state at a particular time n, i.e., $\mathbf{H}(n) = \mathbf{h}$.

In the zero-outage case, given an average power constraint vector $\bar{\mathbf{P}}^* = (\bar{P}_1^*, \bar{P}_2^*, \cdots, \bar{P}_M^*)$ and a rate vector $\mathbf{R} = (R_1, R_2, \cdots, R_M)$ for the M users, an iterative algorithm (we will refer to it as the *Hanly-Tse (HT) Algorithm*) is proposed in [1] for obtaining the optimal power allocation strategy that solves

$$\inf_{\mathcal{P}} \max_{1 \le i \le M} \frac{\bar{P}_i(\mathbf{R})}{\bar{P}_i^*}, \tag{1}$$

where $\mathcal{P}$ denotes a power allocation policy and $\bar{P}_i(\mathbf{R})$ is the resulting average transmit power of each user i required to support $\mathbf{R}$ in every fading state without any outage. Therefore, rate vector $\mathbf{R}$ lies in the zero-outage capacity region if and only if the infimum in (1) is no greater than 1.

Now if the infimum in (1) is larger than 1, the given rate vector $\mathbf{R}$ can only be maintained with a non-zero outage probability for some or all of the M users. In this case, under the assumption that the transmission from all users is turned on or off simultaneously, we wish to obtain the minimum common outage probability $Pr^* \triangleq Pr_{min}(\bar{\mathbf{P}}^*, \mathbf{R})$ and the corresponding optimal power allocation. Under the alternative assumption that the transmission from each user is turned on or off independently, we wish to obtain the outage probability region $\mathcal{O}_I(\bar{\mathbf{P}}^*, \mathbf{R})$ and the optimal power allocation that achieves the boundary surface of $\mathcal{O}_I(\bar{\mathbf{P}}^*, \mathbf{R})$, where $\mathcal{O}_I(\bar{\mathbf{P}}^*, \mathbf{R})$ is the set of all average outage probability vectors for which $\mathbf{R}$ can be maintained with the average transmit power of each user i no larger than $\bar{P}_i^*$, $\forall 1 \le i \le M$.

Under the first assumption, given the rate vector $\mathbf{R}$ and power constraint vector $\bar{\mathbf{P}}^*$ fixed, for each common outage probability $Pr > 0$, we use a similar algorithm as the *HT Algorithm* to find the power allocation that solves

$$\inf_{\mathcal{P}} \max_{1 \le i \le M} \frac{\bar{P}_i(Pr, \mathbf{R})}{\bar{P}_i^*}, \tag{2}$$

where $\mathcal{P}$ denotes a power allocation policy for which the common outage probability is Pr and the resulting average transmit power of each user i is $\bar{P}_i(Pr, \mathbf{R})$. By denoting the infimum in (2) as $Inf(Pr)$, it can be shown that $Inf(Pr)$ is a strictly decreasing function of Pr [4]. Therefore, it is clear that $Inf(Pr) > 1$ if $Pr > Pr^*$ and $Inf(Pr) \le 1$ otherwise, with equality achieved when $Pr = Pr^*$. We propose an iterative algorithm that converges to the power allocation satisfying $Inf(Pr^*) = 1$, and finds the minimum common outage probability Pr^*.

Under the alternative assumption that an outage can be declared independently for each user, a similar iterative algorithm is proposed to obtain the boundary surface of the outage probability region $\mathcal{O}_I(\bar{\mathbf{P}}^*, \mathbf{R})$.

[1] This work was supported by NSF Career Award NCR-9501452 and by a grant from Pacific Bell.

References

[1] S. Hanly and D. Tse, "Multiple-access fading channels: Part II: delay-limited capacities," *IEEE Trans. Inform. Theory*, vol. 44, pp. 2816-2831, Nov. 1998.

[2] L. Li and A. Goldsmith, "Capacity and optimal resource allocation for fading broadcast channels: Part II: outage capacity," Under revision for *IEEE Trans. Inform. Theory.*

[3] G. Caire, G. Taricco, and E. Biglieri, "Optimum power control over fading channels," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1468-1489, July 1999.

[4] L. Li and A. Goldsmith, "Outage capacities and optimal power allocation for fading multiple-access channels," Submitted to *IEEE Trans. Inform. Theory.*

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Error Bounds for the Amplitude Limited Flat Fading Channel[1]

Walid K. M. Ahmed
Bell labs, lucent Technologies
101 Crawfords Corner Road
Holmdel, NJ 07733, U.S.A.
walidahmed@lucent.com

Peter J. McLane
ECE Dept., Queen's University
Kingston, Ontario
Canada K7L 3N6
mclanep@qucdnee.ee.queensu.ca

Abstract — **Peak transmitted power is a key issue in wireless systems. In this paper we consider upper and lower bounds to Gallager's random coding error exponent [1] for the two dimensional (or quadrature) memoryless flat fading channel with perfect channel state information (CSI) at the receiver and when a peak power constraint is imposed at the transmitter.**

I. Summary

Due to space limitations, we only provide the final results. For more detials, the reader is referred to [2].

Let us assume a discrete-time memoryless fading channel (with AWGN) for which the received symbol Y is equal to $y = \upsilon x + w$, where X is a transmitted symbol, Υ is a known fading variable and W is the AWGN term. For an input per-letter peak power constraint of the form $|x|^2 \leq \mathcal{P}$, an upper bound to the ensemble block decoding error probability, for any choice of ρ; $0 \leq \rho \leq 1$, is easily determined to be [2][1] $P_e \leq \exp\{-N E_r(q(x), \rho, R)\}$, where the error exponent, $E_r(\rho, p(x), R)$, is defined as $E_r(q(x), \rho, R) = E_o(q(x), \rho) - \rho R$, where $E_o(q(x), \rho) = -\ln\left[\int_\upsilon p(\upsilon) \int_y \left[\int_x q(x)\, p(y|x,\upsilon)^{1/(1+\rho)}\, dx\right]^{1+\rho} dy\, d\upsilon\right]$. The input distribution $q(x)$ follows the general form $q(x) = g(x)\, u\left(\mathcal{P} - |x|^2\right)$, where $u(\cdot)$ is the unit-step function and $g(x)$ satisfies $\int_{x:\,|x|^2 \leq \mathcal{P}} g(x)\, dx = 1$. The random coding exponent $E_r(R)$ is achieved by maximizing $E_r(q(x), \rho, R)$ over all $q(x)$ and ρ. Finally, and without loss of generality, let $\sigma_\Upsilon^2 = 0.5$, in order to obtain a unity power fading. Also, let $\sigma_W^2 = 1$, then the peak-power-to-noise-ratio (PPNR) is defined as $\text{PPNR} = \frac{\sigma_\Upsilon^2 \mathcal{P}}{\sigma_W^2} = \mathcal{P}/2$.

Instead of optimizing over the input distribution, which is a difficult task, we propose upper- and lower-bounds to the exponent so as to trap this function to a reasonable degree of accuracy.

An upper bound to the error-exponent $E_r(R)$, can be shown to be [2] $E_r(R) \leq \max_{0\leq\rho\leq 1}\{E_{o,U}(\rho) - \rho R\}$, where $E_{o,U}(\rho) = \rho - \ln(1+\rho) - \ln E_{p(\upsilon)}\left\{\left(1 + \frac{|\upsilon|^2\mathcal{P}}{2(1+\rho)}\right)^{-\rho}\right\}$. It should be mentioned that the aforementioned upper bound not only is an upper bound to the error exponent of the per-letter peak-power limited channel, but also is an upper bound to the random coding exponent of the per-letter average-power limited channel (see [2] for clarification).

A lower bound to the random coding exponent for the peak-power-limited ideal fading channel can be determined using any input distribution that satisfies the peak-power constraint. We have attempted three different input distributions. The first is a *rectangular-uniform* input distribution which has the pdf $q(x) = \left(\frac{1}{2\mathcal{P}}\right) U\left(\frac{x_R}{\sqrt{\mathcal{P}/2}}\right) \cdot U\left(\frac{x_I}{\sqrt{\mathcal{P}/2}}\right)$, where $\mathrm{U}(\cdot)$ is defined as $\mathrm{U}(t) = \begin{cases} 1 & ;\ |t| \leq 1 \\ 0 & ;\ \text{otherwise} \end{cases}$. The second attempt is a *circular-uniform* distribution which has the pdf $q(x) = \begin{cases} \frac{1}{\pi\mathcal{P}} & ;\ |x|^2 \leq \mathcal{P} \\ 0 & ;\ \text{otherwise} \end{cases}$. The last attempt is a *conical* distribution with pdf $q(x) = \left(\frac{3}{\pi\mathcal{P}}\right)\left(1 - \frac{|x|}{\sqrt{\mathcal{P}}}\right) u\left(\mathcal{P} - |x|^2\right)$, where $u(\cdot)$ denotes the unit-step function. It has been possible [2] to derive a closed-form expression for the lower bound based on the conical input pdf. For the rectangular-uniform pdf, a Monte-Carlo-integration based methodology has been used to numerically calculate the bound. Finally, for the circular-uniform pdf, only asymptotic results at high peak-power-to-noise ratio (PPNR), as well as cut-off rate numerical calculations at any PPNR, have been feasible. On the other hand, the lower bound based on the concial pdf is the loosest, the bound based on the rectangular-uniform pdf is tighter than the one based on the concial pdf. Finally, the bound based on the circular-uniform pdf is the tightest.

II. Results

Upon evaluation of the upper and lower bounds proposed in this paper, it has been found that at high PPNR, the differences between the upper bound to the cut-off[1] rate and the corresponding lower bounds, due to the rectangular- and the circular-uniform inputs, are 1.45 and 1.0 nats/symbol, respectively. Also, the differences between the upper bound to the cut-off rate and the corresponding lower bound based on the conical pdf is 1.61 nats/symbol. It should be mentioned that the aforementioned asymptotic (high PPNR) differences are, in fact, independent of the fading distribution.

In conclusion, since the upper bound we propose is also an upper bound to the random coding exponent for the channel with average-power-constrained inputs, it follows that the loss in the error exponent, due to the peak-power constraint and relative to the average-power-constrained channel, is no more than 1.0 nats/symbol, which is equal to 1.44 bits/symbol.

References

[1] R. Gallager, *Information Theory and Reliable Communication*, John Wiley and Sons, 1968.

[2] Walid K. M. Ahmed, "Information Theoretic Reliability Function for Flat Fading Channels," *Ph.D. Thesis*, ECE Dept., Queen's University, 1997.

[1] This research has been performed at the ECE Dept. Queen's Univ., Canada. It has been partially supported by the Telecommunications Research Institute of Ontario (TRIO) and the Natural Sciences and Engineering Council of Canada NSERC.

[1] The maximum gap between the upper and lower bounds to the error exponent always occurs at the ($E_r(R)$ = cut-off-rate, $R = 0$) point on the exponent-rate curve, and it increases monotonically with PPNR until it reaches a maximum value at asymptotically high PPNR.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Efficient Coding Schemes for the Hard-Square Model[1]

Ron M. Roth
Computer Science Department
Technion
Haifa 32000, Israel.
e-mail: ronny@cs.technion.ac.il.

Paul H. Siegel
ECE Department
Univ. of California, San Diego
9500 Gilman Drive
La Jolla, CA 92093, USA.
e-mail: psiegel@ucsd.edu.

Jack K. Wolf
CMRR
Univ. of California, San Diego
9500 Gilman Drive
La Jolla, CA 92093, USA.
e-mail: jwolf@ucsd.edu.

Abstract — **The hard-square model consists of all binary arrays in which the 1's are isolated both horizontally and vertically. Based on a certain probability measure defined on those arrays, an efficient variable-to-fixed-rate encoding scheme is obtained that maps unconstrained binary words into arrays that satisfy the hard-square model. For sufficiently large arrays, the average rate of the encoder approaches a value which is only 0.1% below the capacity of the constraint. A second, fixed-rate encoder is obtained whose rate for large arrays is within 1.2% of the capacity value.**

I. Introduction

Recent developments in optical storage are attempting to increase the recording density by exploiting the fact that the recording device is two-dimensional in nature. This, in turn, motivates the study of coding schemes for two-dimensional constraints that may be present in those devices.

The hard-square model, defined next, is a notable example of such a constraint. Consider (without real loss of generality) the parallelograms

$$\Delta_{m,n} = \{(i,j) \in \mathbb{Z}^2 \ : \ 0 \le i < m, \ \ 0 \le i+j < n\}$$

and mappings $x : \Delta_{m,n} \to \{0,1\}$, where hereafter $x_{i,j}$ denotes the value of x at location $(i,j) \in \Delta_{m,n}$. We say that such a mapping x satisfies the hard-square model if $x_{i,j} = 1$ implies $x_{i,j+1} = 0$ (when $j < n-1$) and $x_{i+1,j} = 0$ (when $i < m-1$). The set of all mappings over $\Delta_{m,n}$ that satisfy the hard-square model will be denoted by $\mathcal{S}(\Delta_{m,n})$.

The main goal of this work is designing efficient lossless coding schemes of unconstrained binary words into elements of $\mathcal{S}(\Delta_{m,n})$.

II. Variable-to-fixed-rate encoder

Based on the idea of two-dimensional bit-stuffing introduced in [3], we obtain a variable-to-fixed-rate encoder into $\mathcal{S}(\Delta_{m,n})$. Our encoder effectively realizes the following probability measure $\mu_{m,n}$ on $\mathcal{S}(\Delta_{m,n})$: for every $x \in \mathcal{S}(\Delta_{m,n})$,

$$\begin{aligned}\mu_{m,n}(x) \ &= \ \mu_n^{(\mathrm{h})}(x_{0,0}, x_{0,1}, \ldots, x_{0,n-1}) \\ &\cdot \ \mu_m^{(\mathrm{d})}(x_{1,-1}, x_{2,-2}, \ldots, x_{m-1,-(m-1)}) \\ &\cdot \ \prod_{i=1}^{m-1} \prod_{j=-i+1}^{n-1-i} \vartheta(x_{i,j} \,|\, x_{i,j-1}, x_{i-1,j}, x_{i-1,j+1}) \ ,\end{aligned}$$

where, for two parameters $q_0 \in [0,1)$ and $q_1 \in (0,1]$,

$$\vartheta(0 \,|\, u,y,v) = 1 - \vartheta(1 \,|\, u,y,v) = \begin{cases} q_v & \text{if } u = y = 0 \\ 1 & \text{otherwise} \end{cases} .$$

The boundary measures, $\mu_n^{(\mathrm{h})}$ and $\mu_m^{(\mathrm{d})}$, are set so that the non-boundary values have a stationary distribution. The limit

$$H = \lim_{m,n\to\infty} -\frac{1}{mn} \sum_{x \in \mathcal{S}(\Delta_{m,n})} \mu_{m,n}(x) \log_2 \mu_{m,n}(x)$$

exists and can be written explicitly as a function of q_0 and q_1. Maximizing this function yields $H \approx 0.587277$, which is the average rate of our encoder. This rate is only 0.1% below the capacity value of the hard-square model [1], [2], [4].

III. Fixed-rate encoding scheme

With a slight compromise on the rate, we can also obtain an efficient fixed-rate encoder into $\mathcal{S}(\Delta_{m,n})$. Let $\mathcal{S}_{\ell,r}$ be the set of all words in $\{0,1\}^\ell$ of Hamming weight r in which the 1's are isolated, and for a prescribed positive integer t define

$$K(n,t) = \sum_{s=0}^{t-1} 2^s \cdot \binom{t-1}{s} \cdot |\mathcal{S}_{n-3t+2,t-s}| \ .$$

The images of our encoder are elements $x \in \mathcal{S}(\Delta_{m,n})$ that satisfy the weight constraint $\sum_j x_{i,j} = t$ for each i. The coding rate is $\lfloor (\log_2 K(n,t))/n \rfloor$, and the weight constraint allows to obtain efficient encoding through enumerative coding.

It can be shown that for every fixed rational δ,

$$\limsup_{n\to\infty} \ (1/n) \cdot \log_2 K(n, \delta n) \ge \sup_{\rho} F(\delta, \rho) \ ,$$

where ρ ranges over $[0, \min\{\delta/(1-3\delta), 1/2\}]$ and

$$F(\delta,\rho) = \delta \cdot [1 + h((1/\delta - 3)\rho)] + (1-3\delta) \cdot [(1-\rho) \cdot h(\rho/(1-\rho)) - \rho] \ ,$$

with $h(t)$ standing for $-t \cdot (\log_2 t) - (1-t) \cdot \log_2(1-t)$. Maximizing over δ, we thus obtain the coding rate

$$\max_{(\delta,\rho)} F(\delta,\rho) \approx 0.581074 \ ,$$

which is within 1.2% of the capacity value of the hard-square model.

References

[1] N. Calkin, H.S. Wilf, *The number of independent sets in a grid graph, SIAM J. Discrete Math.*, 11 (1997), 54–60.

[2] K. Engel, *On the Fibonacci number of an $m \times n$ lattice, Fibonacci Quarterly*, 28 (1990), 72–78.

[3] P.H. Siegel, J.K. Wolf, *Bit-stuffing bounds on the capacity of 2-dimensional constrained arrays, ISIT'98 — IEEE Int'l Symp. Inform. Theory*, Cambridge, Massachusetts, 1998.

[4] W. Weeks IV, R.E. Blahut, *The capacity and coding gain of certain checkerboard codes, IEEE Trans. Inform. Theory*, 44 (1998), 1193–1203.

[1] This work was supported in part by Grants Nos. 95-00522 and 98-00199 from the United-States–Israel Binational Science Foundation (BSF), Jerusalem, Israel, by Grant No. NCR-9612802 of the National Science Foundation (NSF), and by the Center for Magnetic Recording Research at the University of California, San Diego.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Two-Dimensional Codes for Second Order Spectral Null Constraints

Hiroshi Kamabe
Department of Information Science, Gifu University
1-1, Yanagido, Gifu, 501-1193, JAPAN
e-mail: Hiroshi.Kamabe@kmb.info.gifu-u.ac.jp

Abstract — **A two-dimensional code for a second order spectral null constraint is given and it is shown that the rate of the code is asymptotically equal to 1.**

I. Introduction

Recently two-dimensional recording devices are developed. Therefore several authors have studied two-dimensional codes for these devices [1], [2].

It has been shown that there are encoding algorithms for two-dimensional spectral null constraints with asymptotical code rate 1 [3]. In this paper we introduce a coding rule for two-dimensional second order spectral null constraints and show that its code rate is asymptotically 1. We describe an outline of our coding rule.

II. Preliminaries

Let $\boldsymbol{a} = a_0 a_1 \cdots a_{L-1}$ be a finite sequence of numbers. The *running digital sum* of $\boldsymbol{a}$, denoted by $\mathrm{RDS}(\boldsymbol{a})$, and the *second order running digital sum* of $\boldsymbol{a}$, denoted by $\mathrm{RDS}^{(2)}(\boldsymbol{a})$, are defined as follows: $\mathrm{RDS}(\boldsymbol{a}) = \sum_{j=0}^{L-1} a_j$ and $\mathrm{RDS}^{(2)}(\boldsymbol{a}) = \sum_{j=0}^{L-1} \mathrm{RDS}(a_0 a_1 \cdots a_j)$. If $\mathrm{RDS}(\boldsymbol{a}) = 0$ then we say that $\boldsymbol{a}$ satisfies a *spectral null constraint at dc*. If $\mathrm{RDS}(\boldsymbol{a}) = \mathrm{RDS}^{(2)}(\boldsymbol{a}) = 0$ then we say that $\boldsymbol{a}$ satisfies a *second order spectral null constraint at dc*. For a symbol a we define $\overline{a}$ by $\overline{a} = -a$ and $\overline{\boldsymbol{a}}$ by $\overline{\boldsymbol{a}} = \overline{a_0}\,\overline{a_1} \cdots \overline{a_{L-1}}$. We introduce an equivalence relation '$\equiv$' of sequences $\boldsymbol{a}$ and $\boldsymbol{b}$ such that $\boldsymbol{a} \equiv \boldsymbol{b}$ if $\boldsymbol{a} = \boldsymbol{b}$ or $\boldsymbol{a} = \overline{\boldsymbol{b}}$.

Let $\mathcal{A}$ be a two-dimensional array. If all rows and all columns of $\mathcal{A}$ satisfy a second order spectral null constraint at dc then we say that $\mathcal{A}$ satisfies the constraint *horizontally* and *vertically*, respectively. If an array satisfies a second order spectral null constraint both horizontally and vertically then we say that the array satisfies a *two-dimensional second order spectral null constraint*.

III. Outline of Coding Rule

We assume that the channel symbol alphabet is $\{-1, 1\}$. Let $\mathcal{A}_0$ be a two-dimensional array of size $m \times n$.

Step 1 First we encode $\mathcal{A}_0$ into a two-dimensional array $\mathcal{A}$ which satisfies a second order spectral null constraint at dc horizontally by using the Henry-Knuth method [4] and a method by Tallini et. al. [5]. Then the length of each row of $\mathcal{A}$ is $n_1 = n + 4\lceil \log n \rceil$.

Step 2 Let $\boldsymbol{p}_i$ be the i-th row of $\mathcal{A}$ and let $\{\boldsymbol{q}_1, \boldsymbol{q}_2, \ldots, \boldsymbol{q}_N\}$ be the set of all distinct code words appearing as rows in $\mathcal{A}$ where we identify $\boldsymbol{p}$ with $\boldsymbol{p}'$ if $\boldsymbol{p} \equiv \boldsymbol{p}'$. Without loss of generality we assume that the first symbol of $\boldsymbol{q}_i$ is 1 for $i = 1, 2, \ldots, N$. We define $L(i)$ to be the number of elements in $\{j : \boldsymbol{p}_j \equiv \boldsymbol{q}_i\}$. We define $\ell(i,j)$, $i = 1, 2, \ldots, N$ so that $\boldsymbol{p}_{\ell(i,j)} \equiv \boldsymbol{q}_i$ for $j = 1, 2, \ldots, L(i)$ and $\ell(i,j) < \ell(i, j+1)$ for $j = 1, 2, \ldots, L(i) - 1$.

Step 3 We extend $\mathcal{A}$ vertically ($L(i)$ and $\ell(i,j)$ are also extended at the same time) by duplicating rows so that $L(i)$ is a multiple of 4. Let J be the number of rows of the resulting array.

Step 4, Step 5 and Step 6 We invert rows so that the absolute values of the second order running digital sums of columns can be bounded from above by $2^{n_1} J$.

Step 7, Step 8 and Step 9 We add rows so that the second order running digital sum of each column of the resulting array is 1, -1 or 0. This can be accomplished by adding at most $2^{n_1}\left\lceil 2\sqrt{J} \right\rceil$ rows. We also add rows to the resulting array in order that all columns satisfy the second order spectral null constraint. The number of extra rows is constant.

Step 10 Let $b(i)$, $i = 1, \ldots, m$ be a sequence such that $b(i) = 1$ if the i-th row in $\mathcal{A}_0$ is inverted and $b(i) = -1$ otherwise. We concatenate the resulting array we get above and $b(1), b(2), \ldots, b(m)$ so that they satisfy the two dimensional second order spectral null constraint.

IV. Code Rate

The number of columns of $\mathcal{A}$ is n_1. In step 4 we add at most 2^{n_1} rows to $\mathcal{A}$. In step 8 we add at most $W 2^{n_1}$ rows where W is the smallest multiple of 4 with $4(m + 2^{n_1})2^{n_1} \le W^2$. In step 9 we add at most $4 \cdot 2^{n_1}$ rows. In step 10 we add at most $4\left\lceil \frac{4m}{n_1} \right\rceil$ rows. Therefore the code rate of our algorithm is bounded from below by

$$\frac{mn}{n_1\left(m + 2^{n_1} + \left\lceil \sqrt{4(m+2^{n_1})2^{n_1}} \right\rceil + 4 + 4 \cdot 2^{n_1} + 4\left\lceil \frac{4m}{n_1} \right\rceil\right)}.$$

We consider a rectangular array of size $2^{2n} \times n$. Then the above rate tends to 1 as $n \to \infty$.

References

[1] A. Kato and K. Zeger, "On the Capacity of Two-Dimensional Run-Length Constrained Channels", *IEEE Trans. Inform. Theory*, vol. IT-45, pp. 1527–1540, 1999.

[2] A. Vardy, M. Blaum, P. H. Siegel, and G. T. Sincerbox, "Conservative arrays: Multidimensional modulation codes for holographic recording", *IEEE Trans. Inform. Theory*, vol. IT-42, pp. 227–230, 1996.

[3] R. Talyansky, T. Etzion, and R. Roth, "Efficient Code Constructions for Certain Two-Dimensional Constraints", *IEEE Trans. Inform. Theory*, vol. IT-45, pp. 794–799, 1999.

[4] D. E. Knuth, "Efficient balanced codes," *IEEE Trans. Inform. Theory*, vol. IT-32, pp. 51–53, 1986.

[5] L. G. Tallini and B. Bose, "Efficient high-order spectral-null codes," *IEEE Trans. Inform. Theory*, vol. IT-45, pp. 2594–2601, 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Convolutional Code and 2-Dimensional PRML Class IV for Multi-track Magnetic Recording System

Naoto KOGO
Faculty of Engineering
Yokohama National University

Norimichi HIRANO
Faculty of Engineering
Yokohama National University

Ryuji KOHNO
Faculty of Engineering
Yokohama National University

Abstract — **This paper proposes a method of joint decoding for combined system between 2-Dimensional Partial Response (2-D PR) system and convolutional codes for the purpose of high density magnetic recording. Since both 2-D PR system and convolutional code can be represented with trellis diagrams, decoding performance can be improved by joint decoding with their overall trellis diagram. Moreover, a method of decoding which can achieve low amount of calculation is also investigated.**

I. Channel Model

If ITI is known in advance, 2-D PR system (3 track - 3 head) can be shown in figure 1. "α" is the amount of ITI.

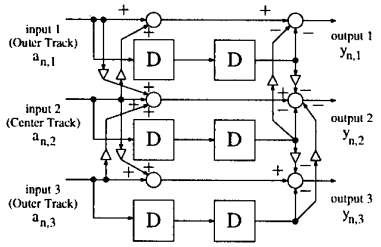


Figure 1: 2-D PR4 (3 Tracks - 3 Heads)

From figure 1, we assume that ITI from the outer track existing on the center track is larger than the ITI from the center track on the outer track. By computer simulation, we confirmed worse BER performance of center track than BER performance of outer tracks (figure 2).

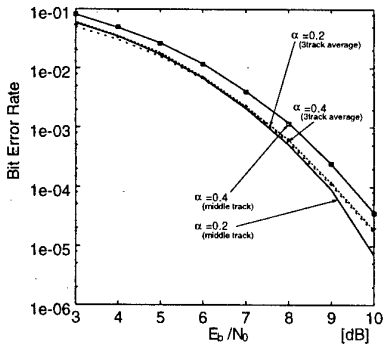


Figure 2: BER performance

II. Convolutional Code and 2-D PR4

Since BER of the center track is worse than that of the outer tracks, it is useful to use error correcting codes for 2-D PRML in which the data in the center track are protected against a greater number of errors than the data in the outer tracks. As we described, both 2-D PR system and convolutional code can be represented with trellis diagrams. Moreover, decoding performance can be improved by joint decoding with their overall trellis diagram.Therefore, we consider joint decoding system with convolutional codes and 2-D PR4 system. The system model is shown in figure 4.

We consider that the contents of memory elements are $a_{n,l}$ (memory elements in convolutional codes) and $b_{n,l}$ (memory elements in PR4 system), where n is the time instant and l is the track number. In this system, outputs are affected by 3 bits and 2 time instances, so the state of the system, S_p, is defined as a $3\times n$ matrix as

$$S_p = \begin{bmatrix} a_{n-1,1} & a_{n-2,1} & \cdots & b_{n-1,1} & b_{n-2,1} \\ a_{n-1,2} & a_{n-2,2} & \cdots & b_{n-1,2} & b_{n-2,2} \\ a_{n-1,3} & a_{n-2,3} & \cdots & b_{n-1,3} & b_{n-2,3} \end{bmatrix} \quad (1)$$

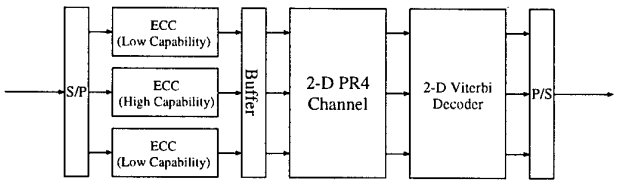


Figure 3: System model

III. Algorithm for Low Amount of Calculation

Next, the algorithm for low amount of calculation of joint decoder is described. As an example, we consider the simplest case applies a $(7,5)_8$ convolutional code to the only center track. By using buffer, the number of input bits of each tracks is same, even the code rate of the center track and that of the outer track is different. Therefore, 6 bits are necessary for 1 path in the trellis diagram. Since the number of memory elements of both PR4 system and $(7,5)_8$ convolutional code is the same, the number of states in the Viterbi decoder will decrease.

References

[1] Emina Soljanin and Costas N. Georghiades, "Coding for Two-Head Recording Systems," *IEEE Trans. Inform. Theory*, Vol.41, No.3, pp.747–755, May 1995.

[2] Y.Yamamoto, R.Kohno: "2-Dimentonal Partial Response Maximum-Likelihood System for Higher-Density Digital Magnetic Recording," Proc. of IEEE ICT'97, pp.183-187, 1997.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Demodulation Techniques for Full-Surface Data

William Weeks IV[1]
University of Illinois
1308 W. Main St.
Urbana, IL 61801
e-mail: w-weeks@uiuc.edu

Abstract — **A comparison of various full-surface demodulation algorithms is presented. Algorithms based on an iterative approach achieve highest data storage density at reasonable complexity and fixed bit error rate.**

I. Introduction

Consider information transmission using a full-surface paradigm. The user data, $\mathbf{u}$, is represented as a one-dimensional signal over a two-dimensional index set, i.e. a matrix of data values, $u_{i,j} \in \{0,1\}$. The noise-free output of the channel, denoted $\mathbf{v}$, may be modeled as the two-dimensional convolution of the user data, $\mathbf{u}$, and the channel model, $\mathbf{c}$, written $\mathbf{v} = \mathbf{c} * \mathbf{u}$. Additive white gaussian noise, $\mathbf{n}$, corrupts the noise-free output, $\mathbf{v}$, which results in the received signal, $\mathbf{r} = \mathbf{v}+\mathbf{n}$. The full-surface maximum-likelihood (ML) demodulator minimizes the expression $||\mathbf{r} - \hat{\mathbf{v}}||^2 = \sum_i \sum_j (r_{i,j} - \hat{v}_{i,j})^2$, where $\hat{\mathbf{v}}$ denotes the noise-free channel output due to channel input $\hat{\mathbf{u}}$, i.e. $\hat{\mathbf{v}} = \mathbf{c} * \hat{\mathbf{u}}$, and $||*||$ denotes the L_2 norm.

In the full-surface optical data storage problem, the channel may be modeled as the truncation of a bivariate gaussian blur, i.e. $c_{i,j} = \exp \frac{-((i-i_c)\delta_x)^2}{2\sigma_c^2} \exp \frac{-((j-j_c)\delta_y)^2}{2\sigma_c^2}$, where δ_x and δ_y denote separation of bits in the vertical and horizontal directions and σ_c is the physical variance of the channel point-spread function. The unitless storage density, D, of such a system is given by $D = \frac{\sigma_c^2}{\delta_x \delta_y}$, where dividing D by σ_c^2 produces a physical density measurement. Finally, the signal-to-noise ratio (SNR) is given by $\text{SNR} = 10 \log_{10} \frac{||\mathbf{c}||^2}{4\sigma_n^2}$, where σ_n is the variance of the noise.

II. Comparison

Figure 1 gives a performance comparison of several full-surface demodulators. For a given point on the graph, data is stored at density given by the vertical axis with SNR given by the horizontal axis and demodulator output that achieves a bit error rate of 10^{-2}.

To date, no ML full-surface demodulator with reasonable complexity has been found. The curve of asterisks is an upper bound to the ML demodulator and is computed using a brute-force ML search over data blocks of size four by four.

The other algorithms perform at sub-ML levels. The solid curve shows the performance of the multitrack Viterbi algorithm (MVA) due to Krishnamoorthi [1]. The curve with "x" is MVA applied to received data that has been filtered using a full-surface equalizer. This equalizer allows for density improvement only at high SNR when colored noise has a negligible effect on the ML demodulation criterion.

The combination of ML image processing methods with threshold decision yields the dashed curve. This is improved

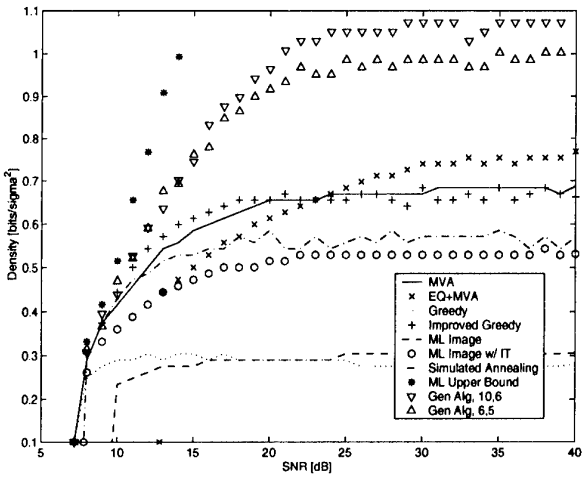


Figure 1: Comparison of Full-Surface Demodulators

to the curve with circles by applying iterative thresholding, an idea developed by Kau [2].

The next class of algorithms is based upon a greedy algorithm. The dotted curve in Figure 1 shows the performance of a greedy algorithm that iteratively chooses data bits to minimize a local metric. It uses a single-point optimization, changing bits one at a time. This algorithm is improved significantly by using techniques of simulated annealing that avoid local minima (the dot-dash curve). Expanding the greedy algorithm to perform multipoint optimizations of likely error sequences produces the curve of plus signs. Finally, a genetic algorithm based upon the improved greedy demodulator achieves the best results. The curve of triangles uses an initial population of five estimated user data matrices and six generations of combining three individuals by majority decision. The curve of upside-down triangles improves on this by using a larger initial population of six and ten generations of natural selection based upon the ML metric.

Acknowledgments

The author would like to thank Prof. Richard Blahut for many helpful discussions.

References

[1] Raghuraman Krishnamoorthi, "Two-Dimensional Viterbi-Like Algorithms," Master's thesis, University of Illinois, Urbana-Champaign, 1998.

[2] Yi-Ming Kau, "Two-Dimensional Data Demodulation from an Image Restoration Approach," Master's thesis, University of Illinois, Urbana-Champaign, 1999.

[1]This work was supported by a JSEP Fellowship

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Two-Dimensional Interleaving Schemes with Repetitions: Constructions and Bounds

Tuvi Etzion
Technion — Israel Institute of Technology
Haifa 32000, Israel
etzion@cs.technion.ac.il

Alexander Vardy
University of California at San Diego
La Jolla, CA 92093–0407, U.S.A.
vardy@kilimanjaro.ucsd.edu

The most common approach for dealing with one-dimensional error bursts is interleaving. For example, to implement the correction of bursts of length 4, one can use four different codewords drawn from a code that corrects τ errors, while encoding, or *interleaving*, the one-dimensional data sequence as follows: 123412341234 $\cdots$. An alternative way to correct any τ bursts of length up to 4 is to use two different codewords from a code that corrects 2τ errors, while interleaving the one-dimensional data sequence as follows: 112211221122 $\cdots$. This is an interleaving scheme with two *repetitions*, in that the same integer appears (at most) twice within a burst of length 4.

While the optimal one-dimensional interleaving schemes, both with and without repetitions, are straightforward, in two dimensions, it is not at all obvious how to interleave a minimal number of codewords so that any burst of size up to t can be corrected. Most two-dimensional burst-correcting codes that have been studied in the literature so far correct error bursts of a given rectangular shape, say $t_1 \times t_2$ rectangular arrays. In this work, we assume that a *cluster of errors* can have an arbitrary shape, as long as it maintains horizontal/vertical connectivity. Important applications where the correction of such two-dimensional error clusters is required are optical recording and holographic storage [2].

Given the foregoing notion of a cluster, one may define a two-dimensional *interleaving scheme* $A(t,r)$ of strength t with r repetitions as an infinite array of integers characterized by the property that every integer appears at most r times in any cluster of size t. The *interleaving degree* of $A(t,r)$, denoted $\deg A(t,r)$, is the total number of distinct integers contained in the array. An interleaving scheme $A(t,r)$ is said to be *optimal* if $\deg A(t,r)$ is the minimum possible for the given t and r.

Blaum, Bruck, and Vardy [2] constructed optimal two-dimensional interleaving schemes without repetitions for all t. Blaum, Bruck, and Farrell [1] generalized the two-dimensional interleaving schemes of [2] in such a way that each integer appears at most twice in any cluster of size t. However, the methods developed in [1] are limited in their scope and applicability. On the other hand, it is obvious from the work of [1, 2] that the problem of constructing $A(t,r)$ to minimize $\deg A(t,r)$ becomes much more challenging for $r \geqslant 2$.

In this work, we introduce the notion of *r-dispersion* that turns out to be crucial in the design of two-dimensional interleaving schemes with repetitions. The r-dispersion may be thought of as a generalization of the L_1-distance to a quantity that reflects a property of r points for $r \geqslant 2$. For $r = 3, 4$, we refer to the corresponding r-dispersion as *tristance* and *quadristance*; efficient methods for computing these dispersions are presented. We also introduce a special class of interleaving schemes based on two-dimensional lattices, which we call *lattice interleavers*. Lattice interleavers are akin to linear codes in coding theory: both classes are distinguished by the fact that a certain linearity property is imposed on their structure. So far, *all* the best-known interleaving schemes, with or without repetitions, belong to the class of lattice interleavers.

We construct lattice interleavers $A(t,2)$ for all t, and compute the corresponding tristance. We also derive lower bounds which show that our constructions are optimal for even t. Finally, we develop the methodology for an elaborate computer search that produces optimal lattice interleavers with two repetitions for all $t \leqslant 161$. These results support our conjecture that the lattice interleavers $A(t,2)$ constructed in this work are, in fact, optimal for all values of t, both even and odd.

We present analogous constructions, bounds, and computer search for lattice interleavers with three repetitions, and prove that our constructions are optimal for $t \equiv 0 \bmod 9$, and asymptotically optimal for other t. The computer search yields optimal lattice interleavers $A(t,3)$ for $t \leqslant 180$. We conjecture that for all higher values of t, optimal lattice interleavers may be obtained from our construction.

For $r = 4$, we construct lattice interleavers for all t. and compute their 5-dispersion. Although we do not have lower bounds in this case, we conjecture that these lattice interleavers are optimal, except for $t = 4, 5, 8, 53, 70$. The computer search confirms this conjecture up to $t = 221$. For higher values of r, we exhibit certain infinite families of lattice interleavers, such as $A(rk, r)$ and $A(r^2k, r)$ for all $k \in \mathbb{Z}^+$, and compute the interleaving degree in each case. These families make it possible to establish general asymptotic results for large r.

We also consider interleaving schemes for an alternative cluster connectivity model. Namely, we assume that two elements in an array are connected if they are adjacent horizontally, vertically, or *diagonally*. We show that there is a tight relation between interleaving schemes for this connectivity model and interleaving schemes for the standard horizontal/vertical connectivity model.

Finally, we consider the following problem: What is the largest shape $\mathcal{S} \subset \mathbb{Z}^2$ such that the tristance between any three points of $\mathcal{S}$ is at most t? Our solution to this problem leads to lower bounds on the interleaving degree of $A(t,2)$ for general (nonlattice) interleavers. These bounds improve substantially upon the earlier results of Blaum, Bruck, and Farell [1].

[1]This work was supported in part by the National Science Foundation, the David and Lucile Packard Foundation, and by grant No. 95–522 from the U.S.–Israel Binational Science Foundation.

References

[1] M. Blaum, J. Bruck, and P.G. Farrell, "Two-dimensional interleaving schemes with repetitions," *IBM Technical Report*, RJ 10047 (90543), 1996.

[2] M. Blaum, J. Bruck, and A. Vardy, "Interleaving schemes for multidimensional cluster errors," *IEEE Trans. Inform. Theory*, vol. 44, pp. 730–743, 1998.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Space-Time Precoding with Imperfect Feedback

Eugene Visotsky[1]
Coordinated Science Laboratory
University of Illinois at
Urbana-Champaign
Urbana, IL, 61801 USA
e-mail: visotsky@uiuc.edu

Upamanyu Madhow
Department of Electrical and
Computer Engineering
University of California
Santa Barbara, CA, 93106 USA
e-mail: madhow@ece.ucsb.edu

Abstract — **This paper provides an information-theoretic perspective on the use of transmit antenna arrays when the transmitter has imperfect channel feedback. The gains obtained are found to be substantial, in contrast with the meager gains due to feedback reported in previous work on single antenna systems.**

I. Introduction

Antenna arrays at the transmitter are widely recognized as an effective means of improving the capacity and reliability of a wireless communication link. There are two key techniques that have been proposed in the literature for exploiting transmit antenna arrays: space-time coding, which requires no knowledge of the spatial channel on the part of the transmitter, and transmit beamforming techniques, which assume that the transmitter has accurate knowledge of the channel through feedback from the receiver. For a typical time-varying channel, however, the feedback available to the transmitter will be of intermediate quality, and one would expect that the transmitter strategy in such situations would be some blend of space-time coding and beamforming. Our purpose in this paper is to make this intuition precise by providing information-theoretic insights into the appropriate transmitter strategies when the channel feedback available to the transmitter is imperfect.

II. Problem Statement

It is assumed that the transmit antenna has M elements, and that the receive antenna has a single element. Consider a discrete time system, where the channel coefficients from the M transmit elements to the receive element at time t are denoted by the $M \times 1$ complex vector $\mathbf{h}(t)$. We consider the following abstraction to model partial knowledge of the channel at the transmitter.

Problem Set-Up: *The transmitter knows that the channel* $\mathbf{h}$ *has a complex Gaussian distribution with mean* $\boldsymbol{\mu}$ *and covariance* $\boldsymbol{\Sigma}$*, denoted by* $\mathcal{N}(\boldsymbol{\mu}, \boldsymbol{\Sigma})$*. The input to the channel is* $\mathbf{x}$*. The receiver knows* $\mathbf{h}$*, and receives*

$$y = \mathbf{x}^H \mathbf{h} + n$$

where $n \sim \mathcal{N}(0, \sigma^2)$ *is circular complex Gaussian noise with variance* $\sigma^2/2$ *per dimension.*

Problem: *What is the input distribution* $p(\mathbf{x})$ *that maximizes the mutual information* $I(\mathbf{x}; y)$*, subject to* $E\{||\mathbf{x}||^2\} \leq P$.

The preceding abstraction can be related to a specific model for channel feedback considered recently in the literature [1], for which the maximizing input distribution achieves the Shannon capacity of the forward link.

[1]This work was supported by Motorola under the University Partnerships in Research Program.

It can be shown [2] that the maximizing input distribution is complex *special* Gaussian, $\mathbf{x} \sim \mathcal{N}(\mathbf{0}, \mathbf{Q})$. The optimization problem is now one of finding the optimum choice of the covariance matrix $\mathbf{Q}^\circ$ maximizing the mutual information for power constraint P, and the optimization problem can be restated as follows:

$$\max_{\mathbf{Q}} E_{\mathbf{h}} \left\{ \log \left(\frac{\mathbf{h}^H \mathbf{Q} \mathbf{h}}{\sigma^2} + 1 \right) \right\} \tag{1}$$

subject to the power constraint $trace\{\mathbf{Q}\} = P$, where σ^2 is variance of the additive circular complex Gaussian noise. The expectation in (1) is computed using the $\mathcal{N}(\boldsymbol{\mu}, \boldsymbol{\Sigma})$ distribution for $\mathbf{h}$.

III. Overview of Results

Presently, the solution to the optimization problem in (1) for the general form of $\mathbf{h} \sim \mathcal{N}(\boldsymbol{\mu}, \boldsymbol{\Sigma})$ is not known. In this work, the optimum distribution is characterized in the following two cases:

1. Mean Feedback: In this case, the channel distribution is modeled at the transmitter as $\mathbf{h} \sim \mathcal{N}(\boldsymbol{\mu}, \alpha \mathbf{I})$, so that the feedback provides noisy information regarding the current channel realization. It is shown that the optimum solution is to use beamforming along $\boldsymbol{\mu}$ ($\mathbf{Q}$ is unit rank) when the feedback SNR is larger than a threshold, and to use M-fold diversity ($\mathbf{Q}$ is full rank) otherwise. In the latter case, the most power is put in the direction $\boldsymbol{\mu}$, while the remaining $M-1$ orthogonal directions receive equal (but lower) powers.
2. Covariance Feedback: The channel distribution known to the transmitter is $\mathbf{h} \sim \mathcal{N}(\mathbf{0}, \boldsymbol{\Sigma})$. This models a situation in which the channel may be varying too rapidly for the feedback to give an accurate estimate of the current channel value. However, the relative geometry of the propagation paths changes more slowly, and is reflected in the covariance matrix $\boldsymbol{\Sigma}$. The optimum solution here is shown to consist of independent Gaussian inputs along (a subset of) the M eigenvectors of $\boldsymbol{\Sigma}$. The solution resembles water pouring, in that eigenvectors corresponding to larger eigenvalues receive more power.

References

[1] G. Caire and S. Shamai, On the capacity of some channels with channel state information, *IEEE Transactions on Information Theory*, vol. 45, pages 2007–2019, September 1999.

[2] I. E. Telatar, Capacity of multi-antenna Gaussian channels, Tech. Rep. BL0112170-950615-07TM, AT&T Bell Labs, 1995.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Space-Time Autocoding: Arbitrarily Reliable Communication in a Single Fading Interval

Thomas L. Marzetta, Bertrand Hochwald and Babak Hassibi
Mathematical Sciences Center
Lucent Technologies
600 Mountain Avenue
Murray Hill, NJ 07974
e-mail: {tlm,hochwald,hassibi}@research.bell-labs.com

Abstract — **Prior treatments of space-time communications in Rayleigh flat fading generally assume that channel coding covers either one fading interval—in which case there is a nonzero "outage capacity"—or multiple fading intervals—in which case there is a nonzero Shannon capacity. However, we establish conditions under which channel codes span only one fading interval and yet are arbitrarily reliable. In short, space-time signals are their own channel codes. We call this phenomenon *space-time autocoding*, and the accompanying capacity the *space-time autocapacity*.**

Let an M-transmitter-antenna, N-receiver-antenna Rayleigh flat fading channel be characterized by an $M \times N$ matrix of independent propagation coefficients, distributed as zero-mean, unit-variance complex Gaussian random variables. This propagation matrix is unknown to the transmitter, remains constant during a T-symbol coherence interval, and there is a fixed total transmit power. Let the coherence interval and number of transmitter antennas be related as $T = \beta M$ for some β. A $T \times M$ matrix-valued signal, associated with $R \cdot T$ bits of information for some rate R is transmitted during the T-symbol coherence interval. Then there is a positive space-time autocapacity C_a such that for all $R < C_a$, the block probability of error goes to zero as the pair $(T, M) \to \infty$ such that $T/M = \beta$. The autocoding effect occurs whether or not the propagation matrix is known to the receiver, and $C_a = N \log(1 + \rho)$ in either case independently of β, where ρ is the expected SNR at each receiver antenna. Lower bounds on the cutoff rate derived from random Unitary Space-Time signals suggest that the autocoding effect manifests itself for relatively small values of T and M. For example within a single coherence interval of duration $T = 16$, for $M = 7$ transmitter antennas and $N = 4$ receiver antennas, and an 18 dB expected SNR, a total of 80 bits (corresponding to rate $R = 5$) can theoretically be transmitted with a block probability of error less than 10^{-9}, all without any training or knowledge of the propagation matrix.

A complete copy of this paper is available on the web at `http://mars.bell-labs.com`.

References

[1] B. Hochwald, T. Marzetta and B. Hassibi, "Space-time autocoding," submitted to *IEEE Trans. Info. Theory*. Also Bell Labs. tech. report, Nov. 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

A Rank Criterion for QAM Space-Time Codes[1]

Youjian Liu
liuy@eemail.eng.ohio-state.edu

Michael P. Fitz
fitz.7@osu.edu

Oscar Y. Takeshita
takeshita.3@osu.edu

The Ohio State University

Abstract — **Sufficient conditions to ensure QAM space-time codes achieve full space diversity in quasi-static fading channel are presented. The conditions are on code words or generator matrices instead of on every code word pair. This greatly simplifies the construction of full space diversity codes.**

I. Introduction

For wireless communication, the design goal of so called "space–time" codes [1] is to take advantage of both the spatial diversity provided by multiple antennas and the temporal diversity available with time–varying fading.

In quasi-static Rayleigh fading channel, in order for a space-time code to achieve full space diversity, the rank of every code symbol difference matrix need to be full rank over complex number field. However, the code is not linear over complex number field. This discrepancy causes a serious obstacle in the design. The paper by Hammons and El Gamal [2] represents an important first step to bridge this discrepancy by providing a binary rank criteria for binary BPSK codes and $\mathbb{Z}_4$ QPSK codes to ensure full space diversity.

We provide a theory for the design of space-time codes in quasi-static Rayleigh fading channel with higher order of constellation (2^{2k} QAM) [3]. It includes the BPSK binary rank criterion in [2] as a special case. For QPSK constellation, it is applicable to GF(4) codes instead of $\mathbb{Z}_4$ codes.

Applications of the theory, such as analysis of existing space-time codes, constructions of new space-time codes from traditional codes and turbo codes will be presented. Only the main theorems are given in this abstract.

II. Σ_o-Rank Criterion

The full space diversity rank criteria developed in [3] are for codes defined on the ring $\mathbb{Z}_{2^k}(j)$, the ring $\mathbb{Z}_{2^k}$ adjoined with the element j which satisfies $j^2 = \ominus 1$. In the sequel, $\oplus$ is used to denote the modulo 2^k addition.

Definition 1 *(**Linear $\mathbb{Z}_{2^k}(j)$ Code with Translation Mapping**) A linear $\mathbb{Z}_{2^k}(j)$ code C is a set of code words which form an additive group. Each code word $\mathbf{J}$ is an N_c by L_t matrix with elements in the ring $\mathbb{Z}_{2^k}(j)$. Each code word matrix $\mathbf{J}$ is mapped to a complex code symbol matrix $\mathbf{D}$ by the translation, $D_i(j) = J_i(j) - \left((2^k-1)/2 + j(2^k-1)/2\right)$, on the element of i^{th} column and j^{th} row for all i and j. It results in a 2^{2k} QAM constellation.*

Definition 2 *(**Σ_o-Coefficients**) Coefficients, α_1, α_2, ..., α_L, in $\mathbb{Z}_{2^k}(j)$ are said to be Σ_o-coefficients if there exists i^* such that $a_{i^*} + b_{i^*}$ is odd, where $a_{i^*} \oplus jb_{i^*} = \alpha_{i^*}$.*

Definition 3 *(Column Σ_o-Rank) A matrix $\mathbf{V}$ over the ring $\mathbb{Z}_{2^k}(j)$ has column Σ_o-rank L if L is the maximum number of column vectors of $\mathbf{V}$, such that*

$$\exists \mathcal{V} = \{\vec{V}_{i_1}, \ldots, \vec{V}_{i_L}\}, \ \bigoplus_{l=1}^{L} \alpha_l \vec{V}_{i_l} \neq \vec{0},$$

for any Σ_o-coefficients, $\alpha_1, \alpha_2, \ldots, \alpha_L$.

The row Σ_o-rank can be similarly defined. Since column Σ_o-rank and row Σ_o-rank are equal [3], they are called Σ_o-rank.

Definition 4 *(**Full Σ_o-Rank**) An m by n matrix $\mathbf{V}$ over ring $\mathbb{Z}_{2^k}(j)$ is said to be of full Σ_o-rank if it has Σ_o-rank equal to the minimum of m and n.*

The sufficient conditions on code words are given first.

Theorem 1 *(**Σ_o-Rank Criterion**) Let C be a linear $\mathbb{Z}_{2^k}(j)$ code with translation mapping to 2^{2k} QAM constellation. If every nonzero code word $\mathbf{J} \in C$ has full Σ_o-rank, then C achieves full space diversity.*

For linear codes, the conditions can be translated into the conditions on the generator matrices.

Theorem 2 *Let C be a linear $\mathbb{Z}_{2^k}(j)$ code. The i^{th} column of the code word matrix is defined as*

$$\vec{J}_i = \mathbf{G}_i \vec{I}, \tag{1}$$

where $\vec{I}$ is the information sequence in $\mathbb{Z}_{2^k}(j)$, $\mathbf{G}_i$ is the generator matrix for i^{th} antenna. If for all Σ_o-coefficients, $\alpha_1, \alpha_2, \ldots, \alpha_{L_t}$, and for all nonzero information sequence, $\vec{I}$,

$$\left(\bigoplus_{i=1}^{L_t} \alpha_i \mathbf{G}_i\right) \vec{I} \neq \vec{0}, \tag{2}$$

then $\forall$ nonzero $\mathbf{J} \in C$, $\mathbf{J}$ is of full Σ_o-rank. Thus, the code achieves full space diversity.

References

[1] V. Tarokh, N. Seshadri, and A. R. Calderbank, "Space-time codes for high data rate wireless communication: performance criterion and code construction," *IEEE Trans. on Info. Th.*, vol. 44, no. 2, pp. 744–765, Mar. 1998.

[2] A. R. Hammons Jr. and H. El Gamal, "On the theory of space-time codes for PSK modulation," *IEEE Info. Theory*, vol. 46, no. 2, pp. 524–542, Mar. 2000.

[3] Y. Liu, M. P. Fitz, and O. Y. Takeshita, "A rank criterion for QAM space-time codes," *submitted to IEEE Trans. on Info. Theory*, Mar. 2000.

[1]This work was supported by National Science Foundation under Grant NCR-9706372.

Y. Liu, M. P. Fitz, and O. Y. Takeshita are with Department of Electrical Engineering, The Ohio State University, 205 Dreese Lab, 2015 Neil Ave., Columbus OH 43210, USA.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

EM-Based Sequence Estimation for Space-Time Codes Systems

Y. Li, C.N. Georghiades, G. Huang
Electrical Engineering Department,
Texas A&M University,
College Station, TX 77843-3128

Abstract — **An EM-based algorithm is introduced for decoding space-time trellis codes without assuming channel knowledge. Its complexity is much smaller than a direct evaluation of the log-likelihood function, and simulation results indicate it receiver achieves a performance close to that of a receiver that knows the channel perfectly.**

I. Introduction and System Model

Tarokh, Seshadri and Calderbank recently proposed trellis-based space-time codes [1] which combine signal processing at the receiver and coding appropriate to multiple transmit antennas. These so-called space-time codes perform well in slowly-fading channels, assuming perfect channel state information (CSI) at the receiver. With the presence of channel mismatch, however, system performance suffers a significant degradation [2]. In this paper we look at the problem of maximum-likelihood sequence estimation for space-time coded systems without assuming channel knowledge. An expectation-maximization (EM) algorithm [3] is derived for the sequence estimation problem and is shown by simulations to perform close to the performance of a maximum likelihood decoder that assumes perfect CSI.

We consider N transmit and M receive antennas. Data blocks of length L are encoded by a space-time encoder. The transmitted code block can be described by a matrix $\mathbf{D}$, whose entry, d_{ln}, is the complex symbol transmitted by the n-th antenna during the l-th symbol time and whose row-vectors are denoted by $\mathbf{D}_l$. The fading channel between the transmit and receive antenna arrays is described by a matrix $\mathbf{\Gamma}$ whose entry γ_{ij} denotes the complex, Gaussian, fading gain in the path from the i-th transmit to the j-th receive antenna. We assume the fading processes of different paths (transmit and receive antenna pairs) are independent. Its column-vectors are denoted by $\mathbf{\Gamma}_j$, which represents the vector of fading coefficients viewed by the j-th receive antenna. The complex matched-filter outputs over the length-L transmitted block at each of the M receive antennas is represented by a matrix $\mathbf{Y}$, whose entry y_{lj} denotes the output at jth antenna at l time instant: $\mathbf{Y} = \mathbf{D}\mathbf{\Gamma} + \mathcal{N}$, where $\mathcal{N}$ is the AWGN term. We denote the column-vectors of $\mathbf{Y}$ by $\mathbf{Y}_j$.

II. The EM-Based Receivers

To apply the EM algorithm, we choose the fading parameter vector $\mathbf{\Gamma}_j^{(l)}$ as the missing data. Thus the expectation step of EM algorithm yields

$$\mathrm{Q}(\mathbf{D}|\mathbf{D}^k) = \sum_{l=1}^{L}\sum_{j=1}^{M}\left[\Re\left(\overline{y_{lj}}\mathbf{D}_l\hat{\mathbf{\Gamma}}_j^k\right) - \frac{1}{2}\mathbf{D}_l\hat{\mathbf{\Omega}}_j^k\mathbf{D}_l^*\right],$$

where

$$\hat{\mathbf{\Gamma}}_j^k = \left((\mathbf{D}^k)^*\mathbf{D}^k + \frac{\mathbf{I}}{\mathrm{SNR}}\right)^{-1}(\mathbf{D}^k)^*\,\mathbf{Y}_j,$$

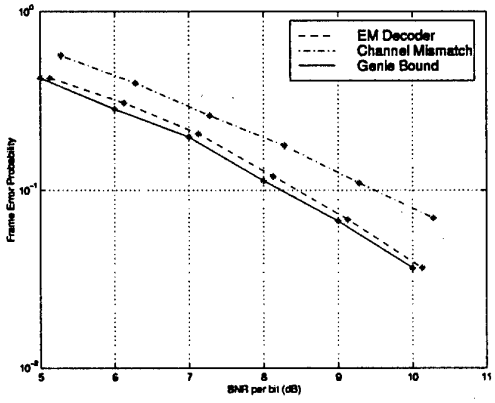


Figure 1: The EM and "genie" decoders: $N = 2$, $M = 2$, $L = 128$, 8-state code, 4 pilot symbols, 3 iterations

$$\hat{\mathbf{\Omega}}_j^k = \mathbf{I} - \left((\mathbf{D}^k)^*\mathbf{D}^k + \frac{\mathbf{I}}{\mathrm{SNR}}\right)^{-1}(\mathbf{D}^k)^*\mathbf{D}^k + \hat{\mathbf{\Gamma}}_j^k(\hat{\mathbf{\Gamma}}_j^k)^*$$

The maximization step yields

$$\mathbf{D}^{k+1} = \arg\max_{\mathbf{D}} \sum_{l=1}^{L}\sum_{j=1}^{M}\left[\Re\left(\overline{y_{lj}}\mathbf{D}_l\hat{\mathbf{\Gamma}}_j^k\right) - \frac{1}{2}\mathbf{D}_l\hat{\mathbf{\Omega}}_j^k\mathbf{D}_l^*\right].$$

III. Performance

We use the 8-state QPSK code introduced in [1] to study the performance of the EM-based algorithm. Pilot symbols are inserted into the data stream to initialize the algorithm. The maximization step of the EM algorithm is efficiently performed using the Viterbi algorithm. Figure 1 shows simulation results for the frame-error probability for the EM-based algorithm, the "genie" receiver that assumes perfect channel knowledge, and a receiver that first estimates the channel. In the simulations for the channel mismatch case, eight pilot symbols were inserted in each frame to estimate the channel. It is clear that the EM decoder performs close to the "genie bound", while in the channel mismatch case, about 1dB loss occurs at a frame error rate of 0.1. At higher SNR, performance loss becomes even larger.

References

[1] V. Tarokh, N. Seshadri, and A. R. Calderbank, "Space-time codes for high data rate wireless communication: Performance criterion and code construction," *IEEE Transactions on Information Theory*, vol. 44, pp. 744–765, March 1998.

[2] V. Tarokh, A. F. Naguib, N. Seshadri, and A. R. Calderbank, "Space-time codes for high data rate wireless communication: Mismatch analysis," *Proceedings of ICC '97*, pp. 309–313, 1997.

[3] A. Dempster, N. M. Laird, and D. B. Rubin, "Maximum-likelihood from incomplete data via the EM algorithm," *Journal of the Royal Statistical Society*, vol. 39, pp. 1–17, 1977.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

The Turbo Decoding Algorithm and Its Phase Trajectories

Dakshi Agrawal
Coordinated Science Laboratory
University of Illinois at Urbana-Champaign
Urbana, IL 61801, U.S.A.
dakshi@csl.uiuc.edu

Alexander Vardy
Department of Electrical Engineering
University of California at San Diego
La Jolla, CA 92093-0407, U.S.A.
vardy@montblanc.ucsd.edu

Abstract — **We analyze phase trajectories of the turbo decoding algorithm as a function of the signal-to-noise ratio (SNR). We prove the existence of fixed points not only at asymptotically high SNRs but also at asymptotically low SNRs. Fixed points at practical SNRs are empirically divided into two classes: indecisive fixed points which usually lead to numerous erroneous decisions and unequivocal fixed points which usually correspond to correct decisions. The waterfall region in the performance curve of turbo decoding is characterized as the region of transition from convergence to indecisive fixed points to convergence to unequivocal fixed points.**

I. Introduction

We consider classical turbo codes, transmitted over an additive white Gaussian noise channel using binary phase-shift-keying modulation. The corresponding turbo decoding algorithm can be viewed as a discrete dynamical system [3]. This dynamical system iteratively updates two probability densities on information bits — commonly known as the *extrinsic information* — provided by the two constituent decoders of the turbo decoding algorithm.

As a dynamical system, the turbo decoding algorithm can have a variety of phase trajectories. A phase trajectory may converge to a fixed point, reach a well-defined invariant set, or simply wander in the high-dimensional space of extrinsic information. At present, preciously little is known about the characteristics of these phase trajectories. For example, in many cases, the turbo decoding algorithm does not converge after a fixed number (say 18) of iterations. Is it possible that in the majority of such cases the decoding algorithm actually converges, albeit only after a large number of iterations? Or is the opposite true: in the majority of such cases, the decoding will never converge. It has been observed that the turbo decoding algorithm always converges at high SNRs. What happens at (asymptotically) low SNRs: Does the algorithm converge or does it wander ad infinitum? These are some of the basic questions answered in this work.

II. Fixed Points at Asymptotic SNRs

Using a set of sufficient conditions provided by Richardson [3], we show [1] that at asymptotically low SNRs, with high probability, the turbo decoding algorithm has a unique fixed point. The extrinsic information that corresponds to this fixed point is close to the uniform distribution on information bits. That is, the fixed point votes almost equally in favor of the two possible values for each transmitted information bit.

On the other hand, we show that at asymptotically high SNRs, with high probability, the turbo decoding algorithm has fixed points that correspond to the transmitted codeword. Moreover, starting from unbiased initialization, the turbo decoding algorithm will converge to one of these fixed points. The derivation of this result indicates that extrinsic information corresponding to such fixed points is concentrated on the transmitted information bits.

III. Fixed Points at Practical SNRs

The existence of certain fixed points at *asymptotic* SNRs raises interesting questions. Does the turbo decoding algorithm, starting from unbiased initialization, converge to these fixed points? If so, what are the threshold values of SNR beyond which the turbo decoding algorithm converges?

To answer these questions, we performed extensive simulations. Empirically, we found that the turbo decoding algorithm converges to two types of fixed points: *indecisive* fixed points and *unequivocal* fixed points. The algorithm converges to indecisive fixed points for SNRs that are below the waterfall region, and to unequivocal fixed points for SNRs above the waterfall region. The empirically observed characteristics of indecisive and unequivocal fixed points match closely the characteristics predicted by our analysis for asymptotically low and asymptotically high SNRs, respectively.

For SNRs in the waterfall region, the decoding algorithm may or may not converge, and in some cases, the phase trajectory may become quasi-period or periodic.

IV. Continuation of Fixed Points

For sufficiently long turbo codes, we can treat the turbo decoding algorithm as a single-parameter dynamical system, parameterized (approximately) by the SNR. This allows us to trace the movement of fixed points (more precisely, obtain the *equilibrium curves* of fixed points) as the SNR is changed.

The equilibrium curves, parameterized (approximately) by the SNR, reveal that unequivocal fixed points barely move as the SNR is changed from very high to very low values. However, starting from the very low values, indecisive fixed points move substantially as the SNR is increased while becoming less and less stable. Ultimately, for SNRs in the waterfall region, indecisive fixed points bifurcate and disappear. All three types of bifurcation, studied in classical bifurcation theory [2], occur in turbo decoding. This explains the quasi-periodic and periodic behavior of the phase trajectories in the waterfall region.

Acknowledgment

The authors benefited tremendously from many lively discussions with Tom Richardson and Ralf Kötter.

References

[1] D. Agrawal and A. Vardy, "The turbo decoding algorithm and its phase trajectories," submitted to *IEEE Trans. Inform. Theory*, available at http://www.comm.csl.uiuc.edu/~dakshi.

[2] Y.A Kuznetsov, *Elements of Applied Bifurcation Theory*, New York: Springer-Verlag, 1998.

[3] T. Richardson, "The geometry of turbo-decoding dynamics," *IEEE Trans. Inform. Theory*, vol. 46, pp. 9–23, January 2000.

[1]This work was supported in part by the National Science Foundation and by the David and Lucile Packard Foundation.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Thresholds for Turbo Codes

Thomas Richardson
Bell Labs, Murray Hill, NJ
tjr@lucent.com

Rüdiger Urbanke
EPFL-DSC, Lausanne, CH
Rudiger.Urbanke@epfl.ch

Abstract — **We prove the existence of thresholds for turbo codes [1] and we prove concentration of the performance of turbo codes within the ensemble determined by the random interleaver. In effect, we show that the results obtained in [2] and [3] for low-density parity-check codes extend to turbo codes. The main technical innovation is to rigorously show that dependence of output extrinsic information on input priors decays with distance along the trellis. In an infinitely long turbo code the densities of the extrinsic information fulfill a certain symmetry condition which we call the *consistency condition*. This condition provides the basis for an efficient Monte-Carlo algorithm for the determination of thresholds for turbo codes. Thresholds of all symmetric parallel concatenated codes of memory up to 6 have been determined.**

I. Introduction

We determine the asymptotic (in length) performance of turbo-codes under *iterative decoding*. The analysis is based on the techniques introduced in [2, 3, 4] in the context of low-density parity check (LDPC) codes extended here to turbo codes.

Assume we have the following setup.

1. A family of binary-input output-symmetric memoryless channels ordered by physical degradation and indexed by a real parameter σ, e.g., the class of binary symmetric channels (BSC), the class of additive white Gaussian noise channels (AWGNC) or the class of Laplace channels (LC).
2. For every integer n we define an ensemble of turbo codes $\mathcal{C}_n$ in the following manner. We first fix the two rational functions $G_1(D) = \frac{p_1(D)}{q_1(D)}$ and $G_2(D) = \frac{p_2(D)}{q_2(D)}$ which describe the recursive convolutional encoding functions. For $x \in \{\pm 1\}$ let $\gamma_i(x)$, $i = 1, 2$, denote the corresponding encoding functions. Then for a given permutation π on n letters the unpunctured codewords of a standard parallel turbo code have the form $(x, \gamma_1(x), \gamma_2(\pi(x)))$. We will assume a uniform probability distribution on the set of such permutations.

There exists a threshold σ^* with the property that if n is large enough then for almost any code from the ensemble $\mathcal{C}_n$ the probability of bit error is below any desired level if transmission takes place over a channel with $\sigma < \sigma^*$ and the bit error probability is bounded away from zero if we transmit over a channel with $\sigma > \sigma^*$.

We use a result from the theory of products of positive random matrices to prove that dependencies in the trellis decay with distance. This implies that constituent decoding is essentially *local* in the trellis and can be appoximated arbitrarily well by finite window turbo decoding [5]. Once one restricts to windowed decoding the proof goes through much as for LDPC codes: An edge exposure martingale argument proves concentration of performance around the mean. For any fixed number of iterations the graph determining output extrinsic information is asymptotically a tree with high probability so the mean converges to the performance of such a tree. By taking limits one obtains the corresponding result for non-windowed, standard, turbo decoding.

To date we know of no numerical algorithm to calculate thresholds which has efficiency comparable to the LDPC code case. To determine thresholds we simulate, in effect, an infinitely long turbo code. If P is the distribution of the priors then the one-sided state distributions, usually denoted α and β converge to steady state distributions along an infinitely long trellis. The output extrinsic information is determined by the these steady state distributions and the distribution of the channel data. We use Monte-Carlo techniques to estimate the various distributions. These calculations are significantly improved in both speed of convergence and accuracy by exploiting a provable symmetry property of extrinisic information distributions in infinitely long turbo codes. Let $f(x)$ be a distribution of extrinsic information in log-likelihood representation for an infinitely long turbo code assuming the all 0 codeword. Then $f(x) = f(-x)e^x$. This consistency condition implies that $f(x)$ is determined by the distribution of $|x|$, which is much easier to accurately estimate via direct simulation.

m	code	σ^*
2	$(5, 7)$	0.883
3	$(11, 13)$	0.93
4	$(17, 31)$	0.94
5	$(31, 45)$	0.94
6	$(41, 107)$	0.941

Table 1: The highest threshold of standard parallel concatenated codes of rate $\frac{1}{2}$ up to memory 6 for the AWGNC: $y = x + n$ where $x = \pm 1$ and n is $\sigma N(0, 1)$.

References

[1] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding," in *Proceedings of ICC'93*, (Geneve, Switzerland), pp. 1064–1070, May 1993.

[2] T. Richardson and R. Urbanke, "The Capacity of Low-Density Parity-Check Codes under Message Passing Decoding," submitted IEEE IT, 1999.

[3] T. Richardson, A. Shokrollahi and R. Urbanke, "Design of Provably Good Low-Density Parity-Check Codes," submitted IEEE IT, 1999.

[4] M. Luby, M. Mitzenmacher, A. Shokrollahi and D. Spielman, "Analysis of low density codes and improved designs using irregular graphs," in *Proceedings of the 30th Annual ACM Symposium on Theory of Computing*, pp. 249-258, 1998.

[5] N. Wiberg, "Codes and Decoding on General Graphs", Linköping University, S-581 83, Linköping, Sweden, 1996.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Gaussian Approximation for Sum-Product Decoding of Low-Density Parity-Check Codes

Sae-Young Chung
Laboratory for Information and Decision Systems, M.I.T.
e-mail: sychung@lids.mit.edu

Rüdiger Urbanke
Communications Theory Lab, EPFL, Lausanne, Switzerland
e-mail: Rudiger.Urbanke@epfl.ch

Thomas J. Richardson
Lucent Technologies, Murray Hill, NJ
e-mail: tjr@lucent.com

Abstract — **We use a Gaussian approximation (GA) for analyzing the sum-product algorithm for low-density parity-check (LDPC) codes and memoryless binary-input continuous-output additive white Gaussian noise (AWGN) channels. This simplification allows us to calculate the threshold quickly and to understand the behavior of the decoder better. We have also designed high rate LDPC codes using the GA that have thresholds less than 0.05 dB from the Shannon limit.**

I. Introduction

For many interesting channels and iterative decoders, LDPC codes exhibit a threshold phenomenon: an arbitrary small bit error probability can be achieved if the noise level is smaller than a certain threshold and the probability of bit error is larger than a positive constant for a noise level above the threshold as the block length tends to infinity [1].

In this paper, we present a simple method to estimate the thresholds of randomly constructed irregular LDPC codes for memoryless binary-input continuous-output AWGN channels under sum-product decoding. This method is based on approximating densities of log-likelihood ratio (LLR) messages as Gaussian mixtures. We assume for each variable node the graph is a tree up to a certain depth as validated by the general concentration theorem [2].

II. Gaussian Approximation

If all incoming messages of a variable node are Gaussian, then the resulting extrinsic information distribution is also Gaussian because it is the sum of independent Gaussian random variables. Numerical results using density evolution (DE) [1] show that the extrinsic information distributions from both variable and check nodes are very close to Gaussian even though the inputs are not. From now on, we assume all extrinsic information distributions are Gaussian. By enforcing the *consistency condition* [2] at each iteration, we can greatly improve the accuracy of the approximation and reduce the DE problem to a one-dimensional one.

Let $\lambda(x) = \sum_{i=2}^{d_l} \lambda_i x^{i-1}$ and $\rho(x) = \sum_{i=2}^{d_r} \rho_i x^{i-1}$ be the degree sequences for the variable and check nodes, respectively. For $0 < s < \infty$ and $0 \le t < \infty$, we define $f(s,t)$ as

$$f(s,t) = \sum_{j=2}^{d_r} \rho_j \psi^{-1}\left(\left[\sum_{i=2}^{d_l} \lambda_i \psi\left(s + (i-1)t\right)\right]^{j-1}\right),$$

where $\psi(x)$ is defined by

$$\psi(x) = \begin{cases} \frac{1}{\sqrt{4\pi x}} \int_{\mathbf{R}} \tanh\frac{u}{2} e^{-\frac{(u-x)^2}{4x}} du & \text{if } x > 0 \\ 0 & \text{if } x = 0. \end{cases}$$

The message update rule becomes now $t_l = f(s, t_{l-1})$, where $s = m_{u_0}$ is the mean of u_0 and t_l is the ensemble mean of the output messages of check nodes at l-th iteration. The initial value t_0 is 0. Note that since $t_1 = f(s,0) > 0$ for $s > 0$, the iteration will always start.

We define the threshold s^* as the infimum of all s in $\mathbf{R}^+$ such that $t_l(s)$ converges to ∞ as $l \to \infty$. By finite induction, we conclude that if $s > s^*$, $t_l(s)$ converges to ∞. The following lemma shows an alternative interpretation of the threshold.

Lemma 1 *$t_l(s)$ will converge to ∞ iff*

$$t < f(s,t), \quad \forall t \in \mathbf{R}^+. \tag{1}$$

As in the case of DE [2] we can derive a stability condition:

Theorem 1 *If $\lambda_2 < \lambda_2^*$, then t will converge to infinity if the initial value of t is large enough. If $\lambda_2 > \lambda_2^*$, then t cannot converge to infinity for any initial value of t, where $\lambda_2^* = e^{1/2\sigma_n^2} / \prod_{j=2}^{d_r} (j-1)^{\rho_j}$.*

For this model it is even possible to derive expressions for the convergence rate of the probability of error P_l. In particular, for $\lambda_2 < \lambda_2^*$, P_l behaves asymptotically as the following as $l \to \infty$:

$$P_l \approx \frac{a}{\sqrt{b+l}} \left(\frac{\lambda_2}{\lambda_2^*}\right)^{2l},$$

where a and b are constants that depend on $\lambda(x), \rho(x)$ and s. These predictions fit well with the actual results using DE.

III. Optimization of Degree Sequences

For given $\rho(x)$ and rate, we can find optimal $\lambda(x)$ that maximizes the noise threshold. This can be performed by maximizing the rate subject to the normalization and the inequality constraint in (1), which can be done using linear programming. Optimization of $\rho(x)$ can be done similarly. We show when we consider only low error probability regions, the optimal form of $\rho(x)$ is concentrated in 1 or 2 consecutive degrees. We have successfully optimized degree sequences using these methods up to within 0.05 dB from the Shannon limit for rates greater than 0.99. Good degree sequences were also obtained for lower rates. Online demonstration of degree sequence optimization using the GA and more results are available at `http://truth.mit.edu/~sychung`.

IV. Acknowledgments

The authors would like to express their appreciation to Prof. G. D. Forney, Jr. for his many helpful comments on this paper.

References

[1] T. J. Richardson and R. Urbanke, "The Capacity of Low-Density Parity Check Codes under Message-Passing Decoding," November 1998, submitted to IEEE IT.

[2] T. J. Richardson, A. Shokrollahi and R. Urbanke, "Design of Provably Good Low-Density Parity Check Codes," April 1999, submitted to IEEE IT.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Analyzing the Turbo Decoder Using the Gaussian Approximation

Hesham El Gamal
Advanced Development Group
Hughes Network Systems
e-mail: helgamal@hns.com

A. Roger Hammons, Jr
Advanced Development Group
Hughes Network Systems
e-mail: rhammons@hns.com

Abstract — **In this paper, we introduce a simple technique for analyzing the iterative decoder that is broadly applicable to different classes of codes defined over graphs in certain fading as well as AWGN channels. The technique is based on the observation that the extrinsic information from constituent MAP decoders is well approximated by Gaussian random variables when the inputs to the decoders are Gaussian. The independent Gaussian model implies the existence of an iterative decoder threshold that statistically characterizes the convergence of the iterative decoder. Despite the idealization of the model and the simplicity of the analysis technique, the predicted threshold values are in excellent agreement with the waterfall regions observed experimentally in the literature when the code word lengths are large.**

I. Introduction

This paper is based on a simple but powerful technique originally developed by the first author in his Ph.D. thesis [1] to evaluate the convergence characteristics of the iterative decoder for various graphical codes. Independently and at roughly the the same time as [1], Richardson and Urbanke [2] developed a rigorous method of analysis for iterative decoding of Gallager low density parity check codes (GLDPCCC). Their approach entails computation of density functions as they evolve from one iteration to the next. The analysis technique proposed in this paper is simpler to evaluate than the density evolution technique and provides insights into the decoder operation that would be difficult to extract using the density evolution approach. Furthermore, despite the idealization of the mathematical model and the simplicity of the analysis technique, the close agreement between its predictions and the simulation results available in the literature, including [2], is striking.

II. Decoder Convergence

Iterative decoding on graphs can be viewed as a multi-stage decoding operation where soft information is exchanged between the different stages. The algorithm performed in each iteration can be either the sum-product or the min-sum algorithms [3]. It was observed in [3] that, if inputs to the sum product algorithm are independent Gaussian random variables, then the output can be tightly approximated by a Gaussian random variable. The independent Gaussian approximation allows for complete characterization of the turbo decoder convergence in terms of a single parameter: the extrinsic information signal-to-noise ratio.

In this paper, we only consider the sum-product algorithm. Therefore, we assume that the constituent codes are decoded by a soft-input/soft-output (SISO) maximum a posteriori (MAP) decoder. The model developed in [4] is intended to cover graphical codes that enjoy some symmetry in their structure; however, with minor modifications the proposed technique can be extended to handle certain irregular codes. In [4], we use this model to show that it is sufficient to characterize the extrinsic information SNR input/output relation of the basic constituent decoder(s) to determine if the turbo decoder will converge or not at any E_b/N_0 [4]. This characterization is generally possible via simple simulations. We only need to simulate on constituent decoder, assuming symmetry, with Gaussian extrinsic and intrinsic inputs and measure the output extrinsic information bit error rate.

III. Application to Different Code Constrcutions

In [4], we analyze in detail the effect of the iterative decoder convergence characteristics on the performance of various graphical codes. For all of the cases considered, the convergence results predicted by the proposed technique are within a small fraction of a dB from the simulation results reported in the literature. [4] also includes an interesting asymmetric parallel concatenated code designed based on convergence considerations.

IV. Conclusions

The main result established in this paper is that the performance of graphical codes in the low SNR region is governed by the convergence characteristics of the iterative decoder independent of the distance spectrum of the code. Thus, traditional optimization of the code parameters with respect to the distance spectrum will not in general improve the performance in the low SNR region. The simple method developed in this paper to analyze the iterative decoder convergence is based on the Gaussian approximation and yields very accurate results compared with the literature.

References

[1] H. El Gamal. On the theory and applications of space-time and graph based codes. *Ph.D Dissertation, University of Maryland at College Park*, May 1999.

[2] T. Richardson and R. Urbanke. The capacity of low density parity check codes under message passing decoding. *submitted to IEEE Trans. Info. Theory.*

[3] N. Wiberg. Codes and decoding on general graphs. *Linkoping Studies in Sci and Technol., dissertations no. 440*, 1996.

[4] H. El Gamal and A. R. Hammons Jr. Analyzing the turbo decoder using the Gaussian approximation. *submitted to IEEE Trans. Info. Theory*, Jan 2000.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Performance Improvement in ATR from Dimensionality Reduction

Natalia A. Schmid[1]
ESSRL, EE Department
Washington University
St. Louis, MO 63130
e-mail: nar@ee.wustl.edu

Joseph A. O'Sullivan[1]
ESSRL, EE Department
Washington University
St. Louis, MO 63130
e-mail: jao@ee.wustl.edu

Abstract — **A thresholding method for reduction of dimensionality applied to test statistics of an M-ary composite hypothesis testing problem, with the maximum likelihood (ML) estimates incorporated instead of the true parameters, is developed. The ML estimates are obtained from training sets of small size. The thresholding method selects only the entries in the testing vector that contain a large amount of information for discriminating among M hypotheses. The information measure is a plug-in version of the relative entropy with one of two distributions known. The method is promising for the exponential family. The performance of the test with a reduced number of dimensions is analyzed by applying a theory of asymptotic expansions of integrals.**

I. Modified Test

Consider an M-ary hypothesis testing problem with populations modeled to belong to a parametric family with an h-dimensional vector of parameters θ in an open subset $\Theta \subset \mathcal{R}^h$. Assume that the vectors of parameters θ_m, $m \in \mathcal{M} = 1, ..., M$, are unknown and distinct. Suppose that M independent sets $\mathcal{S}_m$, one for each population, are available to estimate the unknown parameters. Each set $\mathcal{S}_m$ consists of a collection of N, i.i.d. realizations of a random vector of length $n > N$ sampled from the m-th parametric distribution. Maximum likelihood (ML) estimation often has low complexity and is often preferred for practical pattern recognition systems (see [1]).

Independent data $\mathbf{R}$ drawn equiprobably from one of the M populations are tested using the composite Bayes test with ML estimates in the test statistics. When the entries in the vectors of observations are independent, the test is

$$\hat{m} = \arg \max_{m \in \mathcal{M}} \sum_{l=1}^{n} \log \left\{ p(R(l) : \hat{\theta}_m(l)) \right\}, \qquad (1)$$

where $\hat{\theta}_m(l)$, are the ML estimated parameters obtained using the training set $\mathcal{S}_m$. Tests of this kind are known as plug-in tests [1]. Plug-in tests with ML estimates often exhibit degraded performance and even a so-called peaking phenomenon, which results from nonoptimal use of ML estimates in the test statistics.

A method used in pattern recognition to improve performance of the test with the plug-in test statistics is to apply a method of dimensionality reduction [2, 3]. We take this approach and develop a hard thresholding method to select informative variables (features). First, define a null hypothesis, under which the testing data have a parametric distribution from the same family as the hypothesized populations but with known vector of h parameters ψ (a design vector-parameter). The distribution of the null hypothesis can be incorporated in the test statistics by applying a chain rule. Further the number of dimensions of the testing vector is reduced by using a thresholding approach. According to the method, only the entries in the testing vector that contain the most information for discrimination among M populations are selected. The discrimination information is measured using the following rule

$$d(\hat{\theta}_m(l), \psi(l)) \geq \kappa, \qquad (2)$$

where κ is a nonnegative parameter, called thresholding level, and $d(\cdot, \cdot)$ is an information measure between two distributions. Note that (2) involves the distribution of the null hypothesis. In this work we choose $d(\cdot, \cdot)$ to be a plug-in version of relative entropy. Invoking the null hypothesis and the thresholding rule (2), we can obtain the test

$$\hat{m} = \arg \max_{m \in \mathcal{M}} \sum_{l=1}^{n} \left\{ \log \frac{p(R(l) : \hat{\theta}_m(l))}{p(R(l) : \psi(l))} \right\} I_{d(\hat{\theta}_m(l), \psi(l)) \geq \kappa}, \qquad (3)$$

where $I_{(\cdot)}$ is an indicator function.

II. Performance Analysis

We analyze the performance of the modified test in (3) by first using Monte-Carlo simulations and then by applying a theory of asymptotic expansions of integrals. If N is a parameter of approximation, the moment generating function of the modified test statistic (assume $M = 2$) is a product of (semidefinite or definite) integrals each with a kernel of exponential type. Under conditions stated in [4], each of these integrals can be asymptotically approximated to an arbitrary order in $(1/N)$ (we consider $O(N^{-2})$) by applying the Mellin transform method. The approximation depends on the location of the true parameters in parameter space relative to the solutions of the equation $d(\theta_m(l), \psi(l)) = \kappa$, $l = 1, ...n$, [5].

The results are applied to complex Gaussian models that appear in automatic target recognition problems [5].

[1]This work was supported in part by Grant DAAH04-95-1-0494, by Grant N00014-98-1-06-06, and by the Boeing McDonnell Foundation.

References

[1] L. Devroye, L. Gyorfi, and G. Lugosi, *A Probabilistic Theory of Pattern Recognition*, Springer, New York, 1996.

[2] A. K. Jain, R. P. W. Duin, and J. Mao, "Statistical Pattern Recognition: A Review," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, v. 22, no. 1, pp. 4-36, January 2000.

[3] M. Ben-Bassat, "Use of Distance Measures, Information Measures and Error Bounds in Feature Evaluation," in *Handbook of Statistics*, v. 2, (P. R. Krishnaiah and L. N. Kanal, eds.), North-Holland Publishing Company, 1982, pp. 773-791.

[4] N. Bleistein and R. A. Handelsman, *Asymptotic Expansions of Integrals*, Dover Publications Inc., Mineola, New York, 1986.

[5] N. A. Schmid, J. A. O'Sullivan, "Thresholding Method for Reduction of Dimensionality," submitted, 2000.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Principal Curves with Bounded Turn[1]

S. Sandilya
Department of Electrical Eng.
Princeton University,
Princeton, NJ 08544
sandilya@ee.princeton.edu

S.R. Kulkarni
Department of Electrical Eng.
Princeton University,
Princeton, NJ 08544
kulkarni@ee.princeton.edu

Abstract — **Principal curves, like principal components, are a tool used in multivariate analysis for ends like feature extraction. Defined in their original form, principal curves need not exist for general distributions. The existence of principal curves with bounded length and a learning algorithm for such curves for any distribution that satisfies some minimal regularity conditions has been shown. We define principal curves with bounded turn, show that they exist, and present a learning algorithm for them.**

I. Introduction

Principal component analysis is a widely used tool in multivariate data analysis for purposes such as dimension reduction and feature extraction. A generalization of the idea of principal components to principal curves was introduced by Hastie and Stuetzle in [2]. Principal curves by their definition in [2], however, are not guaranteed to exist for any distribution. Kegl et. al. [3] provided a new definition for principal curves with bounded length, and showed that such curves exist for any distribution with bounded second moment. They also derive a learning algorithm for such curves. Due to the length constraint, the treatment in [3] does not encompass the case of classical principal component analysis. In this paper, we penalize the turn of a curve instead of its length, and look for principal curves within the class of curves of bounded total turn. The appeal of this approach consists partly in the fact that principal components are a special case of such principal curves wherein the total turn is 0. We define principal curves with bounded turn and show that they exist and also analyze an algorithm for learning such curves. Our approach to the problem follows very closely that in [3].

II. Preliminaries and Notation

Definition 1 *A curve in $\mathbb{R}^d$ is defined as a continuous function $f : I \mapsto \mathbb{R}^d$ where I is an interval on $\mathbb{R}$ (possibly infinite, but a closed subset of $\mathbb{R}$).*

Consider a curve f and a point $x \in \mathbb{R}^d$. We define the projection of x onto f and the distortion due to this projection in the natural way. For a random variable X, we define the distortion $\Delta(f)$ of curve f as the expected distortion due to projection of X on to f.

Definition 2 *Given a random variable X, we say that f is a principal curve for X in a class of curves $\mathcal{C}$ if $f \in \mathcal{C}$ and $\Delta(f) = \inf_{g \in \mathcal{C}} \Delta(g) \triangleq \Delta^*_{\mathcal{C}}$*

We define the turn $\kappa(f)$ of a curve f as in [1] so that it generalizes the notion of total integral curvature of a curve to nonsmooth curves in a natural way.

[1]This work was supported in part by the National Science Foundation under NYI grant IRI-9457645 and grant ECS-9873451.

III. Existence of Principal Curves

The main idea in the construction is to use the compactness property of the set of curves of bounded turn within a compact subset of $\mathbb{R}^d$. We know that for any $\mathcal{C}_K$, there exists a sequence of curves in $\mathcal{C}_K$ whose distortions converge to $\Delta^*_{\mathcal{C}_K}$. From this sequence, we construct a subsequence of curves such that this subsequence converges on any compact subset of $\mathbb{R}^d$. We then obtain a "limiting" curve from this subsequence and show that it achieves the minimum distortion in the class and, therefore, is a principal curve.

We need to impose more stringent regularity conditions on the class of curves we consider to ensure that minimizers of our objective function exist as curves that are permitted to accumulate their turn arbitrarily far from the origin may result in the "limit" of these curves not being a curve, but a union of curves. We take the following approach to circumvent the above problem. Impose a uniform bound on the rate at which the turn accumulated within B_R converges to the total turn of the curve, i.e. fix $\tau(R)$ continuous and decreasing in R and consider the class of curves

$$\mathcal{C}_K = \{f \text{ such that } \kappa(f) \leq K,\ \kappa(f) - \kappa(f|_{B_R}) \leq \tau(R)\} \quad (1)$$

Proposition 1 *Consider the class of curves $\mathcal{C}_K$ as detailed in (1). If $E[||X||^2] < \infty$, then there exists a principal curve in $\mathcal{C}_K$.*

As in [3], we may also derive a result on learning such principal curves from i.i.d. data (imposing some extra regularity on F_X). In order to arrive at the principal curve, we resort to empirical risk minimization. When we have a finite amount of data, we cannot optimize over the entire class $\mathcal{C}_K$ as this may lead to overfitting to the data. Hence, we choose a sequence of classes of increasing complexity within which the optimization is conducted. Just as in [3], we consider classes of polygonal lines with increasing number of segments. A distinction that we make is that we also expand the set in which these polygonal lines lie as the random variable X is not assumed to be bounded.

Proposition 2 *Suppose that $E[||X||^2 1_{B_R^C}(X)] \leq R^{-\alpha}$, then there exists an algorithm to produce a sequence of estimates f_n such that*

$$\Delta(f_n) - \Delta(f^*) \sim O(n^{-\frac{\alpha}{6+3\alpha}})$$

References

[1] A.D. Alexandrov, Yu.G. Reshetnyak, *General Theory of Irregular Curves*, Mathematics and Its Applications (Soviet Series), Kluwer vol. 29, 1989.

[2] T. Hastie, W. Stuetzle, "Principal Curves", *Journal of the Amer. Stat. Ass.*, pp. 502-16, 1989.

[3] B. Kegl, A. Krzyzak, T. Linder, K. Zeger, "Learning and Design of Principal Curves", *IEEE Trans. PAMI*, to appear.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Reduced-State BCJR-type Algorithms

G. Colavolpe, G. Ferrari and R. Raheli
Dipartimento di Ingegneria dell'Informazione, Università di Parma, Parco Area delle Scienze 181/A, I-43100 Parma, Italy

Abstract — **In this paper, we propose a technique to reduce the number of trellis states in BCJR-type algorithms, i.e., algorithms with a structure similar to that of the well-known algorithm by Bahl, Cocke, Jelinek and Raviv (BCJR). This work is inspired by reduced-state sequence detection (RSSD). The key idea is the construction, during one of the recursions, of a "survivor map," relative to the reduced-state trellis, to be used in the other recursion.**

I. BCJR-type algorithms

We assume that a source emits a sequence of independent and identically distributed information symbols $\{a_k\}$ which is transmitted through a channel modeled as having a finite memory, possibly by means of some approximations as in [1]. Denoting by $x_1^K = \{x_k\}_{k=1}^K$ the sequence of samples at the input of the receiver, where K is the transmission length and x_k is the observation vector at the k-th signaling interval, and by $e_k(m',m)$ the branch which connects state $S_k = m'$ to state $S_{k+1} = m$, we assume that the BCJR algorithm [2] can be generalized as

$$P(a_k = i|x_1^K) = P\{a_k = i\} \sum_{e_k : a(e_k)=i} \gamma_k(e_k)\alpha_k(e_k)\beta_k(e_k)P\{S^-(e_k)\}$$

where $S^-(e_k)$ is the beginning state of transition e_k. The sum in the above formula is extended over all transitions of epoch k associated to information symbol $a(e_k) = i$. Similarly to the BCJR algorithm, we assume that we can compute the probability density functions $\alpha_k(e_k)$ and $\beta_k(e_k)$ by means of a forward and backward recursion [1, 2, 3].

II. Principle of a reduced-state BCJR-type algorithm

A single transition in the full state trellis can be related to V information symbols, that is $e_k \equiv (a_{k-V+1}, \ldots, a_k)$. Without going into the details as done in [4], indicating by s_k a state in the reduced-state trellis, we simply identify the state reduction by assuming that a transition $\epsilon_k \equiv (s_k, s_{k+1})$ in the new trellis is equivalent to a sequence $(a_{k-Q+1}, \ldots, a_k)$ of information symbols, with $Q < V$. In the reduced-state trellis we may define by $\hat{e}_{k-j}^{(i)}(\epsilon_k)$ the sequence of the most likely transitions $(\hat{e}_{k-j-i+1}, \ldots, \hat{e}_{k-j}) \equiv (\hat{a}_{k-j-i-Q+2}, \ldots, \hat{a}_{k-j-Q+1})$ along the survivor that ends in ϵ_k. As $\alpha_k(e_k)$ can be calculated through a forward recursion in the full state trellis, a similar recursion holds for $\alpha_k(\epsilon_k)$ in the reduced-state trellis. In the logarithmic domain, we may write

$$\bar{\alpha}_k(\epsilon_k) \simeq \max_{\epsilon_{k-1} : s^+(\epsilon_{k-1}) = s^-(\epsilon_k)} \left\{ \bar{\psi}_k(\epsilon_{k-1}, \epsilon_k) + \bar{\alpha}_{k-1}(\epsilon_{k-1}) + \ln P\{a_{old}(\epsilon_{k-1})\} \right\}$$

where $\bar{\psi}_k(\epsilon_{k-1}, \epsilon_k)$ is a suitable logarithmic probability density function and $a_{old}(\epsilon_{k-1})$ indicates the information symbol lost in the transition ϵ_{k-1}. For each transition ϵ_k, the transition ϵ_{k-1}^{max} that maximizes the partial metric $\bar{\psi}_k(\epsilon_{k-1}, \epsilon_k) + \bar{\alpha}_{k-1}(\epsilon_{k-1}) + \ln P\{a_{old}(\epsilon_{k-1})\}$ should be stored (equivalently, we could store $s^-(\epsilon_{k-1}^{max})$ or a_{old}^{max}, the symbol discarded in the transition ϵ_{k-1}^{max}). Keeping track of the survivors associated to each transition in the forward recursion, we build a "survivor map" to be used in the backward recursion.

This work was supported in part by Ministero dell'Università e della Ricerca Scientifica e Tecnologica (MURST), Italy.

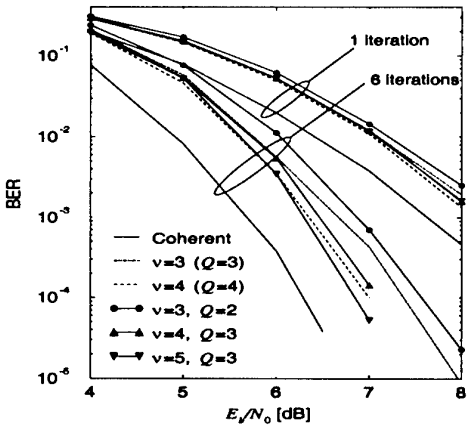


Fig. 1: Application of the proposed technique to iterative detection, through linear prediction, over a flat-fading channel.

The proposed reduced-state technique can be successfully applied to various cases where iterative decoding can be employed: coherent detection over channels affected by intersymbol interference (ISI) (assuming perfect knowledge of the ISI channel coefficients), noncoherent detection as proposed in [1] and fading channels.

In Fig. 1, we consider iterative detection, based on linear prediction, over a Rayleigh flat-fading channel, referring to the concatenated scheme (outer convolutional code and inner differential code) proposed in [5]. The performance for various levels of complexity (in terms of prediction order ν and reduced-state parameter Q of the inner differential detector) is shown. The considered numbers of iterations are 1 and 6 in all cases. The performance in the case of decoding with perfect knowledge of the fading coefficients is also shown (solid lines). The normalized fading rate is $f_{D_{max}} T_s = 0.01$.

References

[1] G. Colavolpe, G. Ferrari and R. Raheli, "Noncoherent iterative (turbo) decoding," *IEEE Trans. Commun.*, to appear, 2000.

[2] L. R. Bahl, J. Cocke, F. Jelinek, and R. Raviv, "Optimal decoding of linear codes for minimizing symbol error rate," *IEEE Trans. Inform. Theory*, vol. 20, pp.284-284, March 1974.

[3] C. Berrou and A. Glavieux, "Near optimum error correcting coding and decoding: turbo-codes," *IEEE Trans. Commun.*, vol. 44, pp.1261-1271, October 1996.

[4] M. V. Eyuboğlu and S. U. H. Qureshi, "Reduced-state sequence estimation with set partitioning and decision feedback," *IEEE Trans. Commun.*, vol. 36, pp.13-20, January 1988.

[5] P. Hoeher and J. Lodge, ""Turbo-DPSK": iterative differential PSK demodulation and channel decoding," *IEEE Trans. Commun.*, vol. 47, pp. 837-843, June 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On Model Selection and Concavity for Finite Mixture Models

Igor V. Cadez and Padhraic Smyth[1]
Dept. of Information and Computer Science
University of California Irvine,
Irvine, CA 92697-3425, U.S.A.
e-mail: {icadez,smyth}@ics.uci.edu

I. Introduction

In this paper we show that the log-likelihood of finite mixture models is approximately concave as a function of the number of mixture components k. A corollary of this result is that the penalized log-likelihood will also be approximately concave (as a function of k) if the penalty term is itself strictly concave or linear in k (true, for example, for BIC [1]). These results have a number of significant practical implications for parameter estimation [2] and model selection [3, 4] in a mixture context

II. Necessary Conditions on the Mixture Components

Our results require three assumptions on the functional form of the components in the finite mixture models being used to fit the data (assumptions which are commonly met in mixture models used in practice):

1. Each model of complexity k contains each model of complexity $k' < k$ as a special case (i.e., it can be reduced to a model of lower complexity by a suitable choice of parameters).
2. Any two models of complexities k_1 and k_2 can be combined as a convex weighted sum in any proportion to yield a valid model of complexity $k = k_1 + k_2$.
3. Each model of complexity $k = k_1 + k_2$ can be decomposed into a convex weighted sum of two valid models of complexities k_1 and k_2 respectively, for each valid choice of k_1 and k_2.

III. Concavity

We wish to fit a finite mixture model probability density function (PDF) to the data U consisting of data points x_i, $U = \{x_1, x_2, \ldots, x_n\}$, of the form: $f(x;\theta) = \sum_{j=1}^{k} \alpha_j \Phi_j(x;\theta_j)$ where Φ_j are basis functions of the mixture model, each with a corresponding set of parameters θ_j. Assuming that the x_i are independent (conditioned on the model f) the log-likelihood is defined as: $l(\theta|U) = \sum_{i=1}^{n} \ln f(x_i;\theta)$.

Theorem 1:
Assuming a mixture model that satisfies the three assumptions from Section II, the log-likelihood is first-order concave, i.e.,

$$l_{k+1} - 2l_k + l_{k-1} \leq 0, \qquad (1)$$

within first-order, where the quantities l_k and $l_{k\pm1}$ are log-likelihoods of the best k and $k \pm 1$ -component models, i.e., the models with k and $k \pm 1$ components which achieve the maximum of the likelihood function.

[1]This work was supported by NSF CAREER award IRI-9703120 and by the University of California MICRO program.

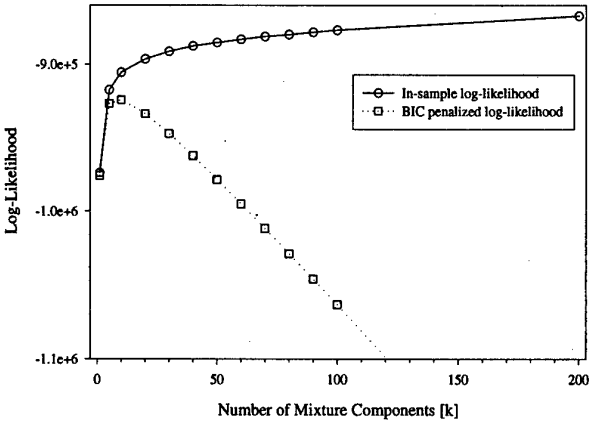


Fig. 1: Maximum log-likelihood and BIC as a function of k for Markov mixtures fitted to sequences from a Web data set.

From the theorem above an obvious corollary is that if an additive penalty term to the log-likelihood is strictly concave or linear in k, then this implies first-order concavity of this penalized log-likelihood (BIC being such an example).

Figure 1 shows an empirical example of apparent concavity for a mixture of Markov chains fitted to over 100,000 page-request sequences from a large commercial Web site. Note that BIC as a function of k is unimodal, as predicted within first-order by theory. This unimodality is a useful practical property in searching for the best model within a large model family as in this example.

Li and Barron [5] have shown in related work that the log-likelihood for any k is bounded above by a function of the form C/k where C is a constant which is independent of k. The results presented here are complementary in the sense that we show that the actual maximizing log-likelihood itself is concave to first-order as a function of k.

References

[1] Schwarz, G., 'Estimating the dimension of a model,' *Annals of Statistics*, 6, 461–462, 1978.

[2] Titterington, D. M., A. F. M. Smith, U. E. Makov, *Statistical Analysis of Finite Mixture Distributions*, Chichester, UK: John Wiley and Sons, 1985.

[3] Fraley, C. and A. E. Raftery, 'How many clusters? Which clustering method? Answers via model-based cluster analysis,' *Computer Journal*, 41, 578–588, 1998.

[4] Smyth, P., 'Model selection for probabilistic clustering using cross-validated likelihood,' *Statistics and Computing*, 9, 63–72, 2000.

[5] Li, J. Q., and Barron, A., 'Mixture density estimation,' preprint, May 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

A Generalized Minmax Bound for Universal Coding

J. Rissanen
IBM ARC, 650 Harry Rd, San
Jose, Ca 95120; and
University of London, Royal
Holloway, Egham, Surrey TW20
OEX, UK
e-mail: jormarissanen@msn.com

Abstract — **The normalized maximum likelihood distribution as a code minimizes the mean code length distance to the ideal target, defined by the negative logarithm of the maximized likelihood of a parametric class of models, where the mean is taken with respect to the worst case model outside the parametric class. The same minmax bound is in essence the lower bound for all codes when the mean is taken with respect to almost all distributions that minimize the mean ideal target. These results strengthen the known bound when the mean is restricted to the parametric class.**

I. Introduction

Two fundamental types of universal code defining distributions for a parametric model class $\mathcal{M}_k = \{P(x^n;\theta)\}$, where θ ranges over a subset Ω of the $k-$dimensional Euclidean space, are the mixture

$$P_w(x^n) = \int_\Omega P(x^n;\theta)w(\theta)d\theta \tag{1}$$

and the Normalized Maximum Likelihood *NML* distribution [4]

$$\hat{P}(x^n) = \frac{P(x^n;\hat{\theta}(x^n))}{\sum_{y^n} P(y^n;\hat{\theta}(y^n))}. \tag{2}$$

Here, w is a density function on the parameters, often called a 'prior' although no prior knowledge in the Bayesian sense is required, and $\hat{\theta}(x^n)$ is the ML estimate. The mixture for a special prior minimizes the worst case redundancy, [2], $\min_q \max_\theta E_\theta \log(P(X^n;\theta)/q(X^n))$, which also defines the capacity of a related channel. In [5] this was generalized to minimizing the worst case *relative* redundancy

$$\min_q \max_g E_g \log(P(X^n;\theta_g)/q(X^n)), \tag{3}$$

where θ_g minimizes $-E_g \log P(X^n;\theta)$ and where the expectation is to be taken with respect to a distribution outside the model class $\mathcal{M}_k$ satisfying certain conditions. Asymptotically the minmax relative redundancy was reached by a modified Jeffreys' mixture.

The normalized ML distribution, too, solves a minmax problem due to Shtarkov, [4], but of a very different kind,

$$\min_q \max_{x^n} \log \frac{P(x^n;\hat{\theta}(x^n))}{q(x^n)}. \tag{4}$$

The first contribution of this paper is to show that the normalized ML distribution also solves the following minmax problem

$$\min_q \max_{g\in G} E_g \log \frac{P(X^n;\hat{\theta}(X^n)}{q(X^n))} = \log C_n(k), \tag{5}$$

where the expectation is taken with respect to virtually any nonsingular distribution $g(x^n)$.

We then have a nice symmetrical situation in that the two universal distributions, the modified Jeffreys' mixture and the normalized ML distribution, are solutions to their closely related minmax problems, (3) and (5), respectively. These are indeed close, since for iid models $\hat{\theta}(x^n)) \to \theta_g$ with $g-$probability 1. As in [1] for the case where $G = \mathcal{M}_k$ one can interpret $-E_g \log P(X^n;\hat{\theta}(X^n))$ as the mean of an ideal but unreachable target code length, and the minimizing q as the reachable distribution that is closest to the ideal target in the mean code length sense.

In [3] this result was strengthened as follows. Let $G_\theta = \{g : \theta_g = \theta\}$, and define

$$g(\theta) = \min_{g\in G_\theta} E_g \log 1/f(X^n;\hat{\theta}(X^n))$$

as the most 'benevolent' distribution for model $f(X^n;\theta)$ giving the shortest mean ideal target.

Theorem 1 *Let $\mathcal{M}_k$ be an exponential family. Then*

$$\log C_n(k) = \frac{k}{2}\log\frac{n}{2\pi} + \log\int_\Omega |I(\theta)|^{1/2}d\theta + o(1), \tag{6}$$

where $|I(\theta)|$ is the Fisher information. Moreover, for any distribution $q(x^n)$ and any ϵ

$$E_{g(\theta)} \log 1/q(X^n) \geq E_{g(\theta)} \log 1/\hat{f}(X^n;\hat{\theta}(X^n)) + \frac{k-\epsilon}{2}\log n$$

except for $\theta \in A_n$, where the volume of A_n goes to zero as $n \to \infty$.

References

[1] Barron, A.R., Rissanen, J., and Yu, B. (1998) 'The MDL Principle in Modeling and Coding', special issue of *IEEE Trans. Information Theory* to commemorate 50 years of information theory, Vol. **IT-44**, No. 6, October 1998, pp 2743-2760

[2] Davisson, L.D. (1983), 'Minimax Noiseless Universal Coding for Markov Sources', *IEEE Trans. Information Theory*, Vol. **IT-29**, No. 2, 211-215, 1983

[3] Rissanen, J. (2000), 'Strong Optimality of Normalized ML models as Ideal Codes', (submitted to IEEE Trans. on Information Theory), http://www.cs.tut.fi/ rissanen/

[4] Shtarkov, Yu. M. (1987), "Universal Sequential Coding of Single Messages", Translated from Problems of Information Transmission, Vol. 23, No. 3, 3-17, July-September 1987.

[5] Takeuchi, Jun-ichi and Barron, Andrew R. (1998), 'Robustly Minimax Codes for Universal Data Compression', *The 21'st Symposium on Information Theory and Its Applications*, Gifu, Japan, December 2-5, 1998.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Universal Noiseless Codes for Sources of Arbitrary Entropy

Abraham Wyner
Department of Statistics
Wharton School
University of Pennsylvania
Philadelphia, PA, USA
ajw@wharton.upenn.edu

Dean Foster
Department of Statistics
Wharton School
University of Pennsylvania
Philadelphia, PA, USA
foster@wharton.upenn.edu

Bob Stine
Department of Statistics
Wharton School
University of Pennsylvania
Philadelphia, PA, USA
stine@wharton.upenn.edu

Abstract — **We offer two noiseless codes for representing blocks of n integers X^n generated independently by a source characterized by an unknown monotone probability function. Though assumed monotone, the source is allowed arbitrary entropy $H \geq 0$, including zero. Our first coding procedure is illustrative, yet universal in the strong sense that the expected value of the code length $L(X^n)$ is dominated by a linear function of the source entropy, $E\,L(X^n) \leq c_0 + c_1\, n\, H$. Our second procedure is asymptotically optimal in the sense that $E\,L(X^n) \leq n\,H + o(n\,H)$. We discuss the implications of these coding procedures for model selection using *MDL*.**

I. Introduction

Consider the problem of encoding a finite collection of n positive integers, $X^n = (X_1, \ldots, X_n)$ into a prefix code of shortest expected length. The component terms $X_i \geq 1$ are independent, integer-valued random variables that share the common, unknown monotone probability distribution F. If $X \sim F$ denotes a random variable with distribution F, then $\Pr(X = i) = p_i \geq p_{i+1},\ i = 1, 2, \ldots$, but are otherwise arbitrary. In particular, the entropy

$$H = -\sum_i p_i \log p_i$$

can be 0, in which case all $X_i = 1$.

We wish to encode X^n as efficiently as possible for the given sample size n, regardless of the entropy of the underlying source. Given F, one can construct an arithmetic coder whose code length $L_F(X^n)$ is on average within one bit of the minimum attainable length,

$$n\,H \leq E\,L_F(X^n) \leq 1 + n\,H\,.$$

If F is unknown, we seek a universal code whose loss relative to this utopian performance is limited. In particular, we seek to encode X^n so that the length of the resulting prefix code $L(X^n)$ is bounded in expectation by a linear function of the entropy of the source,

$$E\,L(X^n) \leq c_0 + c_1 H(X^n) = c_0 + c_1\, n\, H\,,$$

where the constants c_0 and $c_1 \geq 1$ are invariant of n and F. Such a code is universal in the sense described by Elias [1]; the ratio of the expected code length to the minimum attainable message length is bounded for all allowed sources,

$$\frac{E\,L(X^n)}{\max(1, H(X^n))} \leq c_0 + c_1\,.$$

We also want to use codes that are optimal in the sense of having small values for the constants c_0 and c_1.

II. Results

Our first result is to show that a simple modification of the concatenation of scalar universal codes produces a universal code with $c_0 = 3$ and $c_1 = \frac{9}{2}$. Surprisingly, the only modification is the optional compression of the leading bits of each universal code so that the code is competitive when the source entropy is near 0. Our second result is to extend this approach significantly to produce an asymptotically optimal code for sources with arbitrary entropy. Specifically, we prove:

Theorem 1. *There exists a uniquely decodable prefix code for X^n whose length function $L(X^n)$ satisfies*

$$\lim_{nH \to \infty} \frac{EL(X^n)}{nH} \leq 1 + \frac{2\log\log(nH)}{\log(nH)} + O\left(\frac{1}{\log nH}\right)\,.$$

Thus, the relative redundancy goes to 0, asymptotically, as the *minimum* expected number of bits goes to infinity. Our final goal is to provide a firm upper bound on the code length for all sequences. To this end we prove:

Theorem 2. *There exists a uniquely decodable prefix code for X^n whose length function $L(X^n)$ satisfies*

$$E\,L(X^n) \leq 1 + H(X^n)\,\left[1 + O\left(\frac{\log\log\log n}{\log\log n}\right)\right]\,.$$

This code has a particular goal in mind: model selection using the minimum description length (*MDL*). In that setting, the X_i represent the absolute value of rounded, standardized parameter estimates in a statistical model, such as the coefficients in a multiple regression equation.

References

[1] Elias, P. (1975). Universal codeword sets and representations of the integers. *IEEE Trans on Information Theory*, **IT-21**, 194-203.

[2] Wyner, A. D. (1972). An upper bound on the entropy series. *Inform. Contr.*, **20**, 176-181.

[3] Rissanen, J. (1983). A universal prior for integers and estimation by minimum description length. *Annals of Statistics*, **11**, 416-431.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On the Redundancy of Universal Lossless Coding for General Piecewise Stationary Sources[1]

Gil I. Shamir[2] and Daniel J. Costello, Jr.[2]

Abstract — **A lower bound on the achievable redundancy for universal lossless coding of parametric sources with abruptly changing statistics is derived. Unlike the previously known bound for a problem that assumes a fixed number of changes in the statistics, the new bound is general and can be used even if the number of changes increases with the data length.**

The universal lossless coding problem of *Piecewise Stationary Sources* (PSS's), namely, sources with abruptly changing statistics, has significant practical importance. This results from the fact that data sequences from a large family of practical applications can be modeled as being emitted from a source in this class.

A PSS is uniquely defined by the parameter $\psi \triangleq (\boldsymbol{\theta}, \boldsymbol{t})$. The vector $\boldsymbol{\theta} \triangleq (\theta_1, \theta_2, \ldots, \theta_q)$ is the set of k-dimensional parameters that govern the statistics in each of q stationary statistically independent *segments*. The vector $\boldsymbol{t} \triangleq (t_1, t_2, \ldots, t_{q-1})$ represents the set of transition times between stationary segments. The *redundancy* of a code with length function $L(\cdot)$ for n-sequences governed by ψ is defined as

$$R_n(L, \psi) \triangleq \frac{1}{n} E_\psi L(X^n) - H_\psi(X^n), \tag{1}$$

where X^n is a random sequence, E_ψ is the expectation for the given PSS, and H_ψ is the per-letter average entropy of ψ.

In [1], Merhav derived a lower bound on the redundancy of any universal lossless code for a somewhat artificial particular case, where it is assumed that q remains fixed even if n grows. Merhav showed that for every code with length function $L(\cdot)$, the average universal coding redundancy over all sequences of n letters, drawn from almost every PSS ψ with a *fixed* number of stationary segments q, is lower bounded by

$$R_n(L, \psi) \geq (1-\varepsilon)\left(\frac{1}{2}kq + q - 1\right)\frac{\log n}{n}, \tag{2}$$

where $\varepsilon > 0$ can be arbitrarily small.

In various recent works, different approaches were used to develop low complexity, strongly sequential, compression algorithms specifically designed to code memoryless PSS's. Recently (see [3]), it was shown that even if q grows, there exist such coding schemes that achieve redundancy of

$$R_n(L, \psi) \leq (1+\varepsilon)\left(\frac{1}{2}kq + q - 1\right)\frac{\log m}{n} \tag{3}$$

for every PSS, where $m \triangleq n/q$ is the average segment length and $\varepsilon > 0$ can be arbitrarily small.

In this work we show that in the general case, where q is allowed to grow with n (but at a slower rate), there exists a lower bound that asymptotically meets the upper bound in (3). First, let Λ_q be the class of all PSS's with q segments. Then, define a subclass $\Lambda_\varepsilon \subseteq \Lambda_q$ as follows: If $q \to \infty$, Λ_ε contains all $\psi \in \Lambda_q$ for which *almost all* segments are sufficiently long (at least $m^{1-\epsilon}$ time units) and *almost all* transitions are sufficiently large (at least of Euclidean distance of $m^{-\epsilon}$). Otherwise, Λ_ε contains all $\psi \in \Lambda_q$ for which *all* segments are sufficiently long and *all* transitions sufficiently large. It can be shown that in either case, Λ_ε contains almost all sources in Λ_q in the sense that under the uniform *prior* (distribution) $\mu(\cdot)$ over all possible sources in Λ_q, $\mu(\Lambda_\varepsilon) \to 1$ as $n \to \infty$.

Next, partition the subclass Λ_ε into *disjoint* sets $\boldsymbol{\varphi} \triangleq \left(\psi^1, \ldots, \psi^{M_\varphi}\right)$, each with $M_\varphi \geq M$ points $\psi^i \in \Lambda_\varepsilon$, such that any set $\boldsymbol{\varphi}$ contains the largest possible number of sources ψ, *distinguishable* by X^n, for which the parameters for all short segments and small transitions are identical. A set $\boldsymbol{\varphi}$ is distinguishable by X^n if for any source $\psi^i \in \boldsymbol{\varphi}$, the probability that an X^n generated by ψ^i appears to be generated by $\psi^j \in \boldsymbol{\varphi}$ for $j \neq i$ goes to zero.

By the random coding version of the *redundancy-capacity theorem* (see [2]), if $\mu(\Lambda_\varepsilon) \to 1$, and all possible sets $\boldsymbol{\varphi}$ are distinguishable by X^n, then the redundancy of every code for *almost* every source $\psi \in \Lambda_q$, except for a set of sources B for which $\mu(B) \to 0$, is lower bounded by

$$R_n(L, \psi) \geq (1-\varepsilon)\frac{\log M}{n}, \tag{4}$$

where $\varepsilon > 0$ can be arbitrarily small. Lower bounding the maximum M_φ that satisfies the above condition, and using (4), the redundancy for almost all $\psi \in \Lambda_q$ is lower bounded by

$$R_n(L, \psi) \geq (1-\varepsilon)\left(\frac{1}{2}kq + q - 1\right)\frac{\log m}{n} \tag{5}$$

for any parametric PSS of practical interest. If $q \gg m$, in order for all sources ψ in a set $\boldsymbol{\varphi}$ to be distinguishable, the choices of δq long segments, and δq large transitions, for a $\delta > 0$ that can be arbitrarily small, are constrained by the choices of the other parameters for any source $\psi \in \boldsymbol{\varphi}$. This reduces M_φ, but negligibly, resulting in the same lower bound as in (5). The lower bound above confirms the optimality of schemes that achieve the redundancy in (3).

Acknowledgments

We gratefully acknowledge N. Merhav for helpful suggestions.

References

[1] N. Merhav, "On the minimum description length principle for sources with piecewise constant parameters," *IEEE Trans. Inform. Theory*, Vol. 39, No. 6, pp. 1962-1967, November 1993.

[2] N. Merhav and M. Feder, "A strong version of the redundancy-capacity theorem of universal coding," *IEEE Trans. Inform. Theory*, Vol. 41, No. 3, pp. 714-722, May 1995.

[3] G. I. Shamir and D. J. Costello, Jr., "Asymptotically optimal threshold based low complexity sequential lossless coding for piecewise stationary memoryless sources," in *Proceedings of the 1999 IEEE Information Theory and Networking Workshop*, pp. 32, Metsovo, Greece, June 27 - July 1, 1999.

[1]This work was supported by NSF Grant NCR95-22939 and NASA Grant NAG5-8355.

[2]G. I. Shamir and D. J. Costello, Jr. are with Dept. EE, University of Notre Dame, Notre Dame, IN 46556, USA. Emails: gshamir@nd.edu, Daniel.J.Costello.2@nd.edu

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On the Performance of Recency-Rank and Block-Sorting Universal Lossless Data Compression Algorithms

Jun Muramatsu
NTT Communication Science Laboratories
2-4, Hikaridai, Seika-cho, Soraku-gun, Kyoto 619-0237, Japan. e-mail:pure@cslab.kecl.ntt.co.jp

Abstract — **We present bounds of the redundancy of the recency-rank [2] and the block-sorting [1] universal lossless data compression algorithms for finite-length sequences.**

I. Recency-Rank Algorithm

We call the mapping $\xi : \mathcal{A}^n \to \mathcal{A}^n$ *k-block permutation* if there exists a permutation $\pi_{x^n} : \{1,2,\dots,q\} \to \{1,2,\dots,q\}$ such that $\xi(x^n) = \left[*_{j=1}^{q} x_{[\pi_{x^n}(j)-1]k+1}^{\pi_{x^n}(j)k}\right] * x_{qk+1}^n$, where $q \equiv \lfloor n/k \rfloor$ and $n = qk + r$. We assume that both the encoder and the decoder have ξ. For $y^n \in \mathcal{A}^n$, we encode y_1^{qk} by the recency-rank algorithm with k-symbol extension and y_{qk+1}^n using some fixed-length lossless code. Let φ_k be the encoder and $H(p_k(x^n))$ be the non-overlapping k-block empirical entropy function estimated from x^n.

Theorem 1 *Let ξ be a k-block permutation. Then*

$$\frac{1}{n}\ell(\varphi_k(\xi(x^n))) \le \frac{1}{k}H(p_k(x^n)) + \frac{1}{k}\log_2 k + \frac{1}{k}\log_2\left[1+\frac{2k|\mathcal{A}|^k}{n}\right] + \frac{1}{k}\log_2\log_2\left[1+\frac{2k|\mathcal{A}|^k}{n}\right] + O\left(\frac{\log_2\log_2 k}{k}\right) + O\left(\frac{k}{n}\right).$$

When $k(n)$ satisfies $k(n)|\mathcal{A}|^{k(n)} \le n < [k(n)+1]|\mathcal{A}|^{k(n)+1}$,

$$\frac{1}{n}\ell(\varphi_{k(n)}(\xi(x^n))) \le \frac{1}{k}H(p_k(x^n)) + \frac{[\log_2|\mathcal{A}|]\log_2\log_2 n}{\log_2 n} + O\left(\frac{\log_2\log_2\log_2 n}{\log_2 n}\right).$$

When ξ is the identity map, this theorem is the results in [2]. It follows from the theorem that the algorithm is asymptotically optimal for an infinite-length sequences, stationary ergodic sources in the almost-sure sense, and Asymptotically Mean Stationary (AMS) sources in the average and almost-sure sense.

Next theorem tells us the lower bound of the redundancy.

Theorem 2 *Let ξ be a bijective k-block permutation. Then there exist $0 < h < \log_2|\mathcal{A}|$ and x^n such that*

$$\frac{1}{n}\ell(\varphi_k(\xi(x^n))) \ge \frac{1}{k}H(p_k(x^n)) + \frac{1}{k}\log_2 k - O\left(\frac{2^{hk}\log_2 n}{n}\right) - O\left(\frac{k2^{hk}}{n}\right) - O\left(\frac{1}{k}\right).$$

When $k(n)$ satisfies $k(n)|\mathcal{A}|^{k(n)} \le n < [k(n)+1]|\mathcal{A}|^{k(n)+1}$,

$$\frac{1}{n}\ell(\varphi_k(\xi(x^n))) \ge \frac{1}{k}H(p_k(x^n)) + \frac{[\log_2|\mathcal{A}|]\log_2\log_2 n}{\log_2 n} - O\left(\frac{1}{\log_2 n}\right).$$

II. Block-Sorting Algorithm

Let σ_k be the Burrows-Wheeler Transform (BWT) of x^{qk} with k-symbol extension and $\alpha_k(x^{qk})$ be the pointer of the sequence. We use the recency-rank algorithm φ_k with k-symbol extension to encode $\sigma(x^{qk})$ and a lossless encoder δ_q to encode $\alpha(x^{qk})$. Then the block-sorting algorithm Φ_k is defined by

$$\Phi_k(x^n) \equiv \varphi_k(\sigma_k(x^{qk}) * x_{qk+1}^n) * \delta_q(\alpha_k(x^{qk})).$$

Since BWT is a k-block permutation, we do not need the BWT to perform the universal asymptotic optimality when the lossless encoder is the recency-rank algorithm with the extension of alphabet. However, due to sorting in the lexicographical order, symbols with the same context are gathered by the BWT. This provides the good performance for the block-sorting algorithms. We construct the code $\widehat{\Phi}_k$ defined by

$$\widehat{\Phi}_k(x^n) \equiv \varphi_k(\sigma_k(T^{\widehat{s}}x^{qk}) * x_{qk+1}^n) * \delta_q(\alpha_k(T^{\widehat{s}}x^{qk})) * \delta_k(\widehat{s}),$$

where $\widehat{s} \equiv \arg\min_{0\le s\le k-1}\ell(\varphi_k(\sigma_k(T^s x^{qk}))$ and T is the rotation of the sequence. Let $H(\widehat{p}^m(x^n))$ be the empirical m-step Markov entropy function estimated from x^n. We have the following theorem.

Theorem 3

$$\frac{1}{n}\ell(\widehat{\Phi}_k(x^n)) \le H(\widehat{p}^m(x^{qk})) + \frac{1}{k}\log_2 k + \frac{1}{k}\log_2\left[1+\frac{2k|\mathcal{A}|^m|\mathcal{A}|^k}{n}\right] + \frac{1}{k}\log_2\log_2\left[1+\frac{2k|\mathcal{A}|^m|\mathcal{A}|^k}{n}\right] + O\left(\frac{\log_2\log_2 k}{k}\right) + O\left(\frac{\log_2 n}{n}\right) + O\left(\frac{k}{n}\right).$$

When $k(n)$ satisfies $k(n)|\mathcal{A}|^{k(n)} \le n < [k(n)+1]|\mathcal{A}|^{k(n)+1}$,

$$\frac{1}{n}\ell(\widehat{\Phi}_{k(n)}(x^n)) \le \min_{0\le m<k(n)}\left[H(\widehat{p}^m(x^{qk(n)})) + \frac{m[\log_2|\mathcal{A}|]^2}{\log_2 n}\right] + \frac{[\log_2|\mathcal{A}|]\log_2\log_2 n}{\log_2 n} + O\left(\frac{\log_2\log_2\log_2 n}{\log_2 n}\right).$$

It should be noted here that m is automatically optimized by the BWT and we don't need to select it.

References

[1] M. Barrows and D. J. Wheeler, "A block-sorting lossless data compression algorithm," *SRC Research Report 124*, Digital Systems Research Center, Palo Alto, CA., May 1994.

[2] P. Elias, "Interval and recency rank source coding: two online adaptive variable-length schemes," *IEEE Trans. Inform. Theory*, vol.IT-33, pp.3–10, Jan. 1987.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

A new family of ternary sequences with ideal two-level autocorrelation function

Tor Helleseth[1]
Department of Informatics
University of Bergen
Høyteknologisenteret
N-5020 Bergen, Norway
e-mail: torh@ii.uib.no

Vijay Kumar[1]
Communications Science Institute
Electrical Engineering-Systems
USC, Los Angeles
CA 90089-2565, USA
e-mail: vijayk@usc.edu

Halvard Movik Martinsen[1]
Department of Informatics
University of Bergen
Høyteknologisenteret
N-5020 Bergen, Norway
e-mail: halvard@ii.uib.no

Abstract — **Let α be a primitive element of F_{3^n}. Let $d = 3^{2k} - 3^k + 1$ where $n = 3k$. We show that the ternary sequence $\{s(t)\}$ given by $s(t) = Tr_n(\alpha^t + \alpha^{dt})$ has a two-level ideal autocorrelation function.**

I. Introduction

Given a sequence $\{s(t)\}$ of period ϵ and with elements from a finite field F_p. The autocorrelation of the sequence at shift τ is defined by

$$a(\tau) = \sum_{t=0}^{\epsilon-1} \omega^{s(t+\tau)-s(t)}$$

where ω is a complex pth root of unity.

An important problem in sequence design is to find sequences with two-level ideal autocorrelation, i.e., where $a(\tau) = -1$ for any $\tau \neq 0$. Recently, much progress has been obtained for binary sequences of period $\epsilon = 2^n - 1$. These are of considerable interest also because of their close connections to difference sets. For recent work on binary sequences with two-level ideal autocorrelation function the reader is referred to [3], [6], [7], [8], [2] and [1].

Motivated by these results we focused our attention to ternary sequences. To our knowledge, the only non-binary sequences over the alphabet F_p of length $p^n - 1$ with ideal autocorrelation are the m-sequences and the GMW-sequences. This paper present one new family of ternary sequences with ideal autocorrelation.

II. Main result

It is known that the crosscorrelation function takes on three values in the case $d = p^{2k} - p^k + 1$ when $n/gcd(n,k)$ is odd. When $p = 2$ this result is usually attributed to Welch even though he never published a proof. In Kasami [5] a proof can be found in the binary case. For $p > 2$ the proof is given in Trachtenberg [11].

The following is the main result.

Theorem 1. *Let $d = 3^{2k} - 3^k + 1$, $n = 3k$ and let $\{s(t)\}$ be the ternary sequence given by*

$$s(t) = Tr_n(\alpha^t + \alpha^{dt})$$

where α is a primitive element of F_{3^n}. Then the sequence $\{s(t)\}$ has ideal two-level autocorrelation.

The autocorrelation of the sequence above will equal the crosscorrelation of two m-sequences that differ by this decimation and thus will be at most three-valued. The purpose of this paper is to show that the autocorrelation of this sequence has only one out-of-phase value, being equal to -1. By observing that the trace function of the sequence can be expressed as a quadratic form over F_{p^k}, we found the number of solutions and thereby proved the theorem.

For further references on the crosscorrelation of m - sequences the reader is referred to [4], [10], [5], [11] and [9].

[1]This work was supported in part by The Norwegian Research Council under grant numbers 127203/410 and 119390/431 and in part by the National Science Foundation under Grant NCR-9612864.

References

[1] J. Dillon, "Multiplicative difference sets via additive characters", *Designs, Codes and Crytopgrahy*, vol. 17, pp. 225-235, 1999.

[2] J. Dillon and H. Dobbertin, "New cyclic difference sets with Singer parameters", submitted for publication.

[3] R. Evans, H. Hollmann, C. Krattenthaler and Q. Xiang, "Gauss sums, Jacobi sums, and p-ranks of cyclic difference sets", *Journal of Combin. Theory Ser. A.*, to appear.

[4] T. Helleseth, "Some results about the cross-correlation function between two maximal linear sequences", *Discrete Math.*, vol. 16, pp. 209-232, 1976.

[5] T. Kasami, "The weight enumerators for several classes of subcodes of the 2^{nd} order Reed-Muller codes", *Information and Control*, vol. 18, pp. 369-394, 1971.

[6] A. Maschietti, "Difference sets and hyperovals", *Designs, Codes and Cryptography*, vol. 14, pp. 89-98, 1998.

[7] J. S. No, H. Chung and M. S. Yun, "Binary pseudorandom sequences of period $2^m - 1$ with ideal autocorrelation generated by the polynomial $z^d + (z+1)^d$", *IEEE Trans. Inform. Theory*, vol. 44, pp. 1278-1282, 1998.

[8] J. S. No, S. W. Golomb, G. Gong, H. K. Lee and P. Gaal, "Binary pseudorandom sequences of period $2^n - 1$ with ideal autocorrelation", *IEEE Trans. Inform. Theory*, vol. 44, pp. 814-817, 1998.

[9] Y. Niho, "Multi-valued cross-correlation functions between two maximal linear recursive sequences", Ph.D. Thesis, University of Southern California, Los Angeles, USA, 1972.

[10] D. V. Sarwate and M. B. Pursley, "Crosscorrelation properties of pseudorandom and related sequences", *Proc. IEEE International Symposium Inform. Theory* vol. 68, pp. 593-619, 1980.

[11] H. M. Trachtenberg, "On the cross-correlation functions of maximal linear sequences", Ph. D. Thesis, University of Southern California, Los Angeles, USA, 1970.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Ternary m-Sequences with Three-Valued Crosscorrelation Function: Two New Decimations

Hans Dobbertin
German Information Security Agency
P.O. Box 20 0363
D-53133 Bonn, Germany
e-mail: dobbertin@skom.rhein.de

Tor Helleseth[1]
Dept. of Informatics
University of Bergen
Høyteknologisenteret
N-5020 Bergen, Norway
e-mail: torh@ii.uib.no

Vijay Kumar
Com. Science Institute
El. Engineering-Systems
USC, Los Angeles
CA 90089-2565, USA
e-mail: vijayk@usc.edu

Halvard M. Martinsen[1]
Dept. of Informatics
University of Bergen
Høyteknologisenteret
N-5020 Bergen, Norway
e-mail: halvard@ii.uib.no

Abstract — **We show that the crosscorrelation between two ternary m-sequences of period 3^n-1 that differ by the decimation $d=2\cdot 3^m+1$, where $n=2m+1$, takes on 3 different values. We conjecture the same result for the decimation $d=2\cdot 3^r+1$, where n is odd and r is defined by the condition $4r+1\equiv 0 \bmod n$. These two new cases form in a sense ternary counterparts of two recently confirmed binary cases, the conjectures of Welch and Niho.**

I. Introduction

Let $\{u(t)\}$ and $\{v(t)\}$ be two sequences of period ϵ with symbols from F_p, the finite field of p elements. The crosscorrelation of the sequence $\{u(t)\}$ and $\{v(t)\}$ is defined as

$$\theta_{u,v}(\tau)=\sum_{t=0}^{\epsilon-1}\omega^{u(t+\tau)-v(t)},$$

where ω is a complex, primitive pth root of unity.

If $\{u(t)\}$ and $\{v(t)\}$ are two cyclically distinct m-sequences of period p^n-1 with symbols from F_p, we may assume without loss of generality that there exists a d such that $\gcd(d,p^n-1)=1$ and that

$$u(t)=Tr_n(\alpha^t) \text{ and } v(t)=Tr_n(\alpha^{dt})$$

for some primitive elements α in the finite field F_{p^n} and where Tr_n denotes the trace function from F_{p^n} to F_p. We use $C_d(\tau)$ to denote the crosscorrelation function between the m-sequence $\{s(t)\}$ and its decimation $\{s(dt)\}$.

It is known for a long time that the crosscorrelations between two F_p-valued m-sequences of period p^n-1 that differ by a decimation d takes on 3 different values for the *Gold type* decimation $d=\frac{1}{2}(p^k+1)$ (which can be replaced by $d=2^k+1$ for $p=2$) and the *Kasami-Welch-Trachtenberg type* decimation $d=p^{2k}-p^k+1$ if $n/\gcd(k,n)$ is odd. We even get a preferred, i.e. three-valued and minimal, crosscorrelation function in these cases if $\gcd(k,n)=1$.

In the binary case old conjectures of Welch [5] and Niho [7] have recently been confirmed in part by [1], [4], [3] and [6], which give two additional decimations with a preferred crosscorrelation function for each odd n. Apart from the above mentioned cases no other decimations for odd n are known to have a preferred crosscorrelation function. Particular, no decimation have been found by computer experiments. Two further cases for even n can be found in [2].

[1]This work was supported in part by The Norwegian Research Council under grant numbers 127203/410 and 119390/431.

II. Main results

Our main result is the following theorem, loosely speaking the "ternary Welch conjecture":

Theorem A. *Let $d=2\cdot 3^m+1$, where $n=2m+1$, then the crosscorrelation function $C_d(\tau)$ is preferred, i.e. it takes on the following three values:*

$$\begin{array}{lll} -1+3^{m+1} & \text{occurs} & \frac{1}{2}(3^{n-1}+3^m) \text{ times} \\ -1 & \text{occurs} & 3^n-3^{n-1}-1 \text{ times} \\ -1-3^{m+1} & \text{occurs} & \frac{1}{2}(3^{n-1}-3^m) \text{ times.} \end{array}$$

Our proof of Theorem A follows in principle the same basic steps as the proof of the binary case. We were not able to prove the following "ternary Niho conjecture".

Conjecture B. *Let $d=2\cdot 3^r+1$, where $n=2m+1$ and*

$$r=\begin{cases} \frac{n-1}{4} & \text{if } n\equiv 1 \pmod 4, \\ \frac{3n-1}{4} & \text{if } n\equiv 3 \pmod 4, \end{cases}$$

then the crosscorrelation function $C_d(\tau)$ is preferred.

References

[1] A. Canteaut, P. Charpin, H. Dobbertin, "Binary m-sequences with three-valued crosscorrelation: a proof of Welch's conjecture", *IEEE Trans. Inform. Theory*, to appear.

[2] T. W. Cusick and H. Dobbertin, "Some new three-valued crosscorrelation functions for binary m-sequences", *IEEE Trans. Inform. Theory*,vol. 42, pp. 1238-1240, 1996.

[3] H. Dobbertin, "Almost perfect nonlinear power functions on $GF(2^n)$: the Welch case", *IEEE Trans. Inform. Theory* vol. 45, pp. 1271-1275.

[4] H. Dobbertin, "Almost perfect nonlinear power functions on $GF(2^n)$: the Niho case", *Information and Computation*, to appear.

[5] S.W. Golomb, "Theory of transformation groups of polynomials over GF(2) with applications to linear shift register sequences", *Information Sciences 1*, pp. 87-109, 1968.

[6] H.D.L. Hollmann and Q. Xiang, "A proof of the Welch and Niho conjectures on crosscorrelation of binary m-sequences", *Finite Fields and Their Applications*, submitted.

[7] Y. Niho, "Multi-valued cross-correlation functions between two maximal linear recursive sequences", Ph.D. Thesis, University of Southern California, 1972.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Reverse–Complement Similarity Codes for DNA Sequences[1]

Arkadii G. D'yachkov, Pavel A. Vilenkin
Moscow State University
Faculty of Mechanics & Mathematics
Department of Probability Theory
Moscow, 119899, Russia
e-mails: dyachkov@nw.math.msu.su
paul@vilenkin.dnttm.ru

David C. Torney, P. Scott White
MS K710, Los Alamos National Laboratory
Los Alamos, NM, 87545, USA
e-mails: dct@lanl.gov
swhite@telomere.lanl.gov

Abstract — **We introduce three definitions of quaternary codes which are based on a biologically motivated measure of sequence similarity for quaternary n-sequences, extending Hamming similarity. The corresponding codes are used in bio-molecular experiments with DNA sequences. One of the codes is based on a distance function, extending Hamming distance. We discuss upper and lower bounds on the rates of these codes.**

I. Notations

Consider the *quaternary alphabet* $\mathsf{A} \triangleq \{0,1,2,3\}$ and denote by A^n the set of words $\mathbf{w} = (w_1,\ldots,w_n)$, $w_i \in \mathsf{A}$. For any two words $\mathbf{x},\mathbf{y} \in \mathsf{A}^n$, we define a *similarity function*

$$\mathcal{S}(\mathbf{x},\mathbf{y}) \triangleq \sum_{i=1}^{n} \varsigma(x_i,y_i), \tag{1}$$

where *alphabetic similarities* $\varsigma(0,0) = \varsigma(3,3) = 3$, $\varsigma(1,1) = \varsigma(2,2) = 2$ and $\varsigma(x,y) = 0$ for $x \neq y$.

The value $\mathcal{S}(\mathbf{x},\mathbf{x})$ is called a *self-similarity* of the word $\mathbf{x}$, and the value $\mathcal{S}(\mathbf{x},\mathbf{y})$ for $\mathbf{x} \neq \mathbf{y}$ is called a *cross-similarity* between sequences $\mathbf{x}$ and $\mathbf{y}$.

Using (1), we define a *DNA distance* on $\mathsf{A}^n \times \mathsf{A}^n$:

$$\mathcal{D}(\mathbf{x},\mathbf{y}) \triangleq \frac{\mathcal{S}(\mathbf{x},\mathbf{x}) + \mathcal{S}(\mathbf{y},\mathbf{y})}{2} - \mathcal{S}(\mathbf{x},\mathbf{y}). \tag{2}$$

For any $\mathbf{x} = (x_1,\ldots,x_n) \in \mathsf{A}^n$, we introduce its *reverse complementary* word

$$\widetilde{\mathbf{x}} \triangleq (\bar{x}_n, \bar{x}_{n-1}, \ldots, \bar{x}_1),$$

where *alphabetic complementaries* have the form $\bar{0} = 3$, $\bar{1} = 2$, $\bar{2} = 1$ and $\bar{3} = 0$.

II. Definitions

Definition 1. A set of words $\mathcal{C} \subset \mathsf{A}^n$ is called a *reverse-complement code* of *DNA distance* D if the following two conditions hold:

1) for any word $\mathbf{x} \in \mathcal{C}$, its reverse complementary word $\widetilde{\mathbf{x}} \neq \mathbf{x}$ and $\widetilde{\mathbf{x}} \in \mathcal{C}$;
2) $\mathcal{D}(\mathbf{x},\mathbf{y}) \geq D$ for any $\mathbf{x} \neq \mathbf{y}$, $\mathbf{x},\mathbf{y} \in \mathcal{C}$.

Definition 2. A set of words $\mathcal{C} \subset \mathsf{A}^n$ is called a *reverse-complement code* with *similarity parameters* (S_1,S_2) if the reverse-complement condition 1) holds and

2') $\mathcal{S}(\mathbf{x},\mathbf{x}) \geq S_1$ for any $\mathbf{x} \in \mathcal{C}$ and $\mathcal{S}(\mathbf{x},\mathbf{y}) \leq S_2$ for any $\mathbf{x} \neq \mathbf{y}$, $\mathbf{x} \in \mathcal{C}$, $\mathbf{y} \in \mathcal{C}$.

Definition 3. A set of words $\mathcal{C} \subset \mathsf{A}^n$ is called a *reverse-complement code* with *similarity threshold* Δ if the reverse-complement condition 1) holds and

2") $S_1 - S_2 \geq \Delta$, where S_1 is the least self-similarity and S_2 is the largest cross-similarity in the set $\mathcal{C}$, see 2').

III. Bounds on the Rate

Denote by $t(n,D)$, $t'(n,S_1,S_2)$ and $t''(n,\Delta)$ the maximum possible sizes of codes defined above. Let $n \to \infty$, $D \sim nd$, $S_1 \sim ns_1$, $S_2 \sim ns_2$ and $\Delta \sim n\delta$, where d, s_1, s_2 and δ are fixed. Introduce the rates of these codes

$$R(d) \triangleq \limsup_{n\to\infty} \frac{\log_2 t(n,D)}{n},$$

$$R'(s_1,s_2) \triangleq \limsup_{n\to\infty} \frac{\log_2 t'(n,S_1,S_2)}{n},$$

$$R''(\delta) \triangleq \limsup_{n\to\infty} \frac{\log_2 t''(n,\Delta)}{n}.$$

Theorem 1 (Plotkin bound). *If* $d \geq 1.9$, *then* $R(d) = 0$. *If* $0 \leq d < 1.9$, *then*

$$R(d) \leq \overline{R}(d) \triangleq 2\left(1 - \frac{10}{19}d\right).$$

Let $m(p) \triangleq 1 + 6p - 10p^2 \leq m(3/10) = 1.9$, $0 < p \leq 1/2$,

$$\mu(h,p) \triangleq \log_2\left(2p^2(1+2^{3h}) + 2q^2(1+2^{2h}) + 8pq2^{2.5h}\right),$$

where $q \triangleq \frac{1}{2} - p$. For the fixed $p \in (0,1/2)$, consider the function $E(p,d) > 0$, $0 \leq d < m(p)$, defined by the parametric equations

$$E(p,d) = h\frac{\partial\mu(h,p)}{\partial h} - \mu(h,p), \quad d = \frac{\partial\mu(h,p)}{\partial h}, \quad h \leq 0.$$

Theorem 2 (random coding bound). *If* $0 \leq d < 1.9$, *then*

$$R(d) \geq \underline{R}(d) \triangleq \max_{m(p)\geq d} E(p,d) > 0,$$

where the maximum is taken over p, $0 < p < 1/2$, *for which* $0 \leq d \leq m(p)$.

References

[1] R. G. Gallager, *Information Theory and Reliable Communication*, New York: J. Wiley, 1968.

[2] J. L. Massey, "Reversible Codes," *Information and Control*, no. 7, pp. 369-380, 1964.

[3] A. G. D'yachkov and D. C. Torney, "On Similarity Codes," paper, submitted for publication.

[1]This paper was supported by the US Department of Energy through OBER. The work of A.D'yachkov and P.Vilenkin was supported in part by the Russian Foundation of Basic Research, grant 98-01-00241.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Golay Complementary Sequences for OFDM with 16-QAM

Cornelia Rößing[1]
Department of Mathematics
Ohio University
Athens, OH 45701, USA
e-mail: roessing@math.ohiou.edu

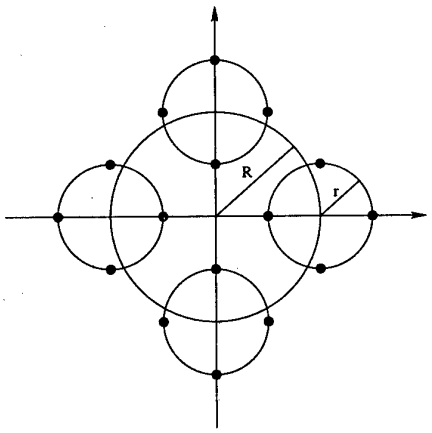
Abstract — **Orthogonal frequency division multiplexing (OFDM) is a common technique in multicarrier communications. Whereas most results so far relate 4-PSK-based OFDM, this contribution introduces a new approach using the 16-QAM scheme.**

I. Basics

The transmission of a signal in an OFDM system is based on equally spaced, phase-shifted sinusoidal carriers. In a 4-PSK modulation e.g. there are four distinct phase shifts used, and the OFDM signal of a word $x \in \mathbb{Z}_4^n$ is given by the real part of the function:

$$S_x(t) := \sum_{j=0}^{n-1} i^{x_j} \exp[2\pi i(f_0 + j\Delta f)\, t]$$

where $f_0 + j\Delta f$ are the carrier frequencies and $i = \sqrt{-1}$. The 16-QAM (quadrature amplitude modulation) is a signal set that allows a convenient representation as a product af two 4-PSK modulations. Here, after a normalization $R = \sqrt{2}$ is



16-QAM as a product of two 4-PSK

the distance between the origin and the center of one 4-PSK circle and $r = \frac{1}{2}\sqrt{2}$ is the radius of the smaller circles. Then the OFDM signal is given by the function

$$S_{x,y}(t) := \sum_{j=0}^{n-1} (Ri^{x_j} + ri^{y_j}) \exp[2\pi i(f_0 + j\Delta f)\, t],$$

where $x, y \in \mathbb{Z}_4^n$. The instantaneous envelope power is defined as $P_{x,y}(t) := |S_{x,y}(t)|^2$, and the peak-to-mean envelope power ratio (PMEPR) of a set $Z \subseteq \mathbb{Z}_4^n \times \mathbb{Z}_4^n$ is given by

$$\mathrm{PMEPR}(Z) := \frac{\sup_{(x,y)\in Z} \sup_t P_{x,y}(t)}{\frac{1}{|Z|}\sum_{(x,y)\in Z} \int P_{x,y}(t)\, dt}.$$

[1]This work was supported by AT&T Labs-Research, Florham Park, NJ

II. Results

The aperiodic autocorrelation of a sequence $x \in \mathbb{Z}_4^n$ at displacement u is the function

$$C_x(u) := \sum_{0\le j, j+u\le n-1} i^{x_j - x_{j+u}}.$$

Two sequences $x, y \in \mathbb{Z}_4^n$ form a *Golay complementary pair* (GCP) if $C_x(u) + C_y(u) = 0$ for each $u \neq 0$. A member of a GCP is called a *Golay sequence*. It is known that $P_x(t) \le 2n$ for a Golay sequence $x \in \mathbb{Z}_4^n$.

Theorem: For a GCP (x, y) of length n there holds $P_{x,y}(t) \le 5n$. If x and y are Golay sequences (not necessarily forming a GCP) then $P_{x,y}(t) \le 10n$.

If $C \subseteq \mathbb{Z}_4^n$ is invariant under the translation by the all-2-sequence, then for $Z := C \times C$ we have

$$\frac{1}{|Z|} \sum_{(x,y)\in Z} \int_0^1 P_{x,y}(t)\, dt = 2.5\, n.$$

Theorem: Let $C \subseteq \mathbb{Z}_4^n$ be a set of Golay sequences that is invariant under the translation by the all-2-sequence. Then the PMEPR for $Z := C \times C$ is bounded by 4.

Acknowledgments

The author is indebted to Vahid Tarokh from AT&T Labs-Research for many inspiring discussions.

References

[1] J. A. C. Bingham, "Multicarrier modulation for data transmission: an idea whose time has come", IEEE Commun. Magazine, pp. 5–14, May 1990.

[2] J. A. Davis and J. Jedwab, "Peak-to-mean power control in OFDM, Golay complementary sequences and Reed-Muller codes," Submitted 1997.

[3] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Solé: "The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes." IEEE Trans. Inform. Theory, 40: 301-319, 1994.

[4] R. D. J. van Nee, "OFDM codes for peak-to-average power reduction and error correction", Proc. IEEE Globecom 1996, pp. 740–744, London, 1996.

[5] H. Ochiai and H. Imai, "Block coding scheme based on complementary sequences for multicarrier signals", IEICE Trans. Fundamentals, pp. 2136–2143, 1997.

[6] K. G. Paterson, "Generalized Reed-Muller codes and power control in OFDM modulation", IEEE Trans. Inform. Theory, submitted.

[7] S. B. Weinstein and P. M. Ebert, "Data transmission by frequency-division multiplexing using the discrete Fourier transform", IEEE Trans. Commun. Technol., vol. 19, pp. 628–634, Oct. 1971.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Linear Parallel Interference Cancellation Using Fixed Weighting Factors for Long-Code CDMA

Dongning Guo
Dept. of Electrical Engineering
Princeton University
Princeton, NJ 08544, USA
email: dGuo@Princeton.EDU

Lars K. Rasmussen
Dept. of Computer Engineering
Chalmers University of Technology
SE-412 96 Göteborg, Sweden
email: larsr@ce.chalmers.se

Abstract — **Linear weighted multistage parallel interference cancellation (PIC) implements exactly the family of polynomial expansion detectors. For long-code CDMA, a set of optimal weights is found which minimizes the ensemble averaged mean squared error (MSE) over random codes. The weights are dependent on moments of the eigenvalues of the correlation matrix, where exact expressions are derived. The loss incurred by averaging rather than using the optimal, time-varying weights is practically negligible.**

I. Introduction

Consider a K-user symbol-synchronous CDMA system with processing gain N. The received signal vector is $\mathbf{r} = \mathbf{A}\mathbf{d} + \mathbf{n}$, where $\mathbf{A} = (\mathbf{a}_1, \mathbf{a}_2, \cdots, \mathbf{a}_K)$ is the matrix containing all users' spreading codes, $\mathbf{d} = (d_1, d_2, \cdots, d_K)^{\mathsf{T}}$ the data vector and $\mathbf{n}$ the AWGN with variance σ^2.

The detailed structure of the ith PIC stage with weight μ_i is depicted here where MF denotes matched filtering. A multistage PIC is a simple cascade of m PIC stages, whose output is

$$\mathbf{y}_m = \left[\mathbf{I} - \prod_{i=1}^{m}(\mathbf{I} - \mu_i(\mathbf{R} + \sigma^2\mathbf{I}))\right](\mathbf{R} + \sigma^2\mathbf{I})^{-1}\mathbf{A}^{\mathrm{H}}\mathbf{r} \quad (1)$$

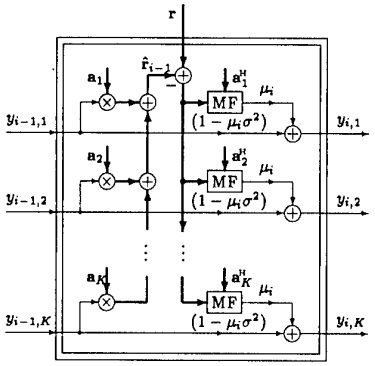
where $\mathbf{R} = \mathbf{A}^{\mathrm{H}}\mathbf{A}$ is the correlation matrix. By choosing an appropriate set of weights, the PIC can implement exactly any detector of the form of a polynomial in $\mathbf{R}$ applied to the code matched-filtered output $\mathbf{A}^{\mathrm{H}}\mathbf{r}$.

It has previously been shown that the PIC is a realization of the steepest descent algorithm used to minimize the MSE. Following this interpretation, a unique set of weights, dependent on the eigenvalues of $\mathbf{R}$, was found to lead to the minimum achievable MSE for a given number of stages in a short-code system [1]. This approach is too complex for long-code systems. Instead, we consider using a set of code-invariant weights designed to give the minimum ensemble averaged MSE over random codes.

The ensemble average of the excess MSE, as compared to the MMSE, is expressed as a function of $\mathbf{u} = (\mu_1, \mu_2, \cdots, \mu_m)$

$$J^{(m)}(\mathbf{u}) = \mathrm{E}\left\{\sum_{k=1}^{K}\frac{\lambda_k}{\lambda_k + \sigma^2}\prod_{i=1}^{m}\left|1 - \mu_i(\lambda_k + \sigma^2)\right|^2\right\} \quad (2)$$

where the λ_k's are the eigenvalues of $\mathbf{R}$ and the expectation is taken over random codes. By an elementary symmetric polynomial transform in $\mathbf{u}$ we can rewrite (2) as a quadratic function in a vector $\mathbf{x}$, which is a function of $\mathbf{u}$. A unique minimum is then obtained where the corresponding μ_k's are found as the inverse polynomial transform.



For an m-stage PIC, the weights depend on the first $2m$ moments of the eigenvalues, defined as $M_r = \mathrm{E}\{\lambda^r\}$, $r = 1, 2, \cdots, 2m$ where λ is an arbitrary eigenvalue of $\mathbf{R}$. Moreover,

$$\begin{aligned} M_r &= \frac{1}{K}\mathrm{E}\{\mathrm{trace}\{\mathbf{R}^r\}\} \\ &= \frac{1}{K}\sum_{k_1=1}^{K}\sum_{k_2=1}^{K}\cdots\sum_{k_r=1}^{K}\mathrm{E}\left\{R_{k_1k_2}R_{k_2k_3}\cdots R_{k_{r-1}k_r}R_{k_rk_1}\right\} \\ &= \frac{1}{K}\sum_{k_1=1}^{K}\sum_{k_2=1}^{K}\cdots\sum_{k_r=1}^{K}\sum_{n_1=1}^{N}\sum_{n_2=1}^{N}\cdots\sum_{n_r=1}^{N} \\ &\qquad \mathrm{E}\{A^*_{n_1k_1}A_{n_1k_2}A^*_{n_2k_2}A_{n_2k_3}\cdots A^*_{n_rk_r}A_{n_rk_1}\}. \end{aligned} \quad (3)$$

Since A_{nk} are all independent random variables, only terms containing all complex conjugate pairs are relevant. M_r is then obtained through evaluation of the summation over all combinations of indices. As the expectation is taken over all code-sets, M_r only depends on N and K, but not on specific codes. In fact it is a polynomial in N and K [2].

With the exact expressions derived, the moments can be evaluated easily and the optimal weights computed. The computational complexity is minor for a moderate number of stages and hence can be implemented on-line. Simulation results show that the penalty of averaging rather than using the optimal weights dependent on the instantaneous spreading codes is negligible in most cases of interest.

This work was supported in part by the Centre for Wireless Communications, National University of Singapore and Oki Techno Centre (S'pore) Pte Ltd.

References

[1] D. Guo, L. K. Rasmussen, S. Sun, and T. J. Lim, "A matrix-algebraic approach to linear parallel interference cancellation in CDMA," *IEEE Trans. Commun.*, vol. 48, Jan. 2000.

[2] D. Guo, L. K. Rasmussen, and T. J. Lim, "Linear parallel interference cancellation in long-code CDMA multiuser detection," *IEEE J. Selected Areas Commun.*, vol. 17, Dec. 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On CDMA Transmission over Mismatched Fading Channels employing MMSE–Receivers and Successive Cancellation

Alexander Lampe
Universität Erlangen-Nürnberg, Cauerstraße 7/NT, 91058 Erlangen, Germany
Phone: +49-9131-85 27114, Fax: +49-9131-85 28919, Email: alampe@LNT.de

Abstract — **Recently, a closed solution to the capacity of synchronous CDMA for fading channels supposing exact channel knowledge at the receiver and infinite spreading factor, i.e., $N\to\infty$ has been derived by Shamai and Verdú [1]. On the other hand, considering imperfect channel state information Evans and Tse [2] derived analytical solutions to the signal to noise ratio provided by linear multiuser receivers and could also give results for the error variance resulting from linear channel estimation. Here, lower and upper bounds on the users' SIR reachable by means of a nonlinear MMSE–receiver applying successive cancellation while assuming a certain channel estimation accuracy are given. Note that due to imperfect channel estimation the interference from previously decoded users cannot be cancelled completely even if no decoding errors occur.**

I. Lower and Upper Bound on SIR

We consider the synchronous transmission of K users over frequency selective fading channels to a common receiver and model the shifted replicas of the kth user's random spreading sequence arriving over the L resolved paths as L independently chosen random spreading sequences $\boldsymbol{s}_{k,1}[\mu],\ldots,\boldsymbol{s}_{k,L}[\mu],\forall k$, with spreading factor N [2] (Note, this model holds exactly for the equivalent case of K users transmitting with L antennas over flat fading channels to a single receiver). Assuming imperfect channel knowledge at receiver site, the path weights are modeled as sum of a Gaussian distributed MMSE path weight estimate $\hat{h}_{k,l}[\mu]$ with variance $1/L-J$ and orthogonal estimation error $\hat{n}_{k,l}[\mu]$ with power J. For sake of simplicity, we suppose that channel estimation is performed with equal accuracy for all users $1\le k\le K$, paths $1\le l\le L$ and time slots. Now, considering user k the signal employed for subsequent processing in a specific time interval $[\mu]$ after cancellation of user $k+1,\ldots,K$ based on their perfectly decoded symbols is

$$\begin{aligned}\boldsymbol{y}_k[\mu] &= \sum_{\kappa=1}^{k}\sum_{l=1}^{L}\boldsymbol{s}_{\kappa,l}[\mu](\hat{h}_{\kappa,l}[\mu]+\hat{n}_{\kappa,l}[\mu])x_\kappa[\mu]\\ &\quad+\sum_{\kappa=k+1}^{K}\sum_{l=1}^{L}\boldsymbol{s}_{\kappa,l}[\mu]\hat{n}_{\kappa,l}[\mu]x^d_{\kappa,l}[\mu]+\boldsymbol{n}[\mu],\end{aligned}$$

where the N dimensional vector $\boldsymbol{n}$ represents the additive channel noise. The i.i.d. components of $\boldsymbol{n}$ are zero mean complex Gaussian with variance σ_n^2. Further, the users' channel symbols are denoted as $x_k\in\mathcal{X}$, $1\le k\le K$, having equal power σ_x^2 and the superscript d marks the already known channel symbols of previously decoded users. Assuming uncorrelated channel estimation errors for the different users as well as paths and time slots, a lower bound on the resulting signal to interference ratio $\mathrm{SIR}_k[\mu]$ at the output of an MMSE filter extracting the signal of user k from $\boldsymbol{y}_k[\mu]$ can be solved for $N\to\infty$ with $|\hat{\boldsymbol{h}}_k[\mu]|^2\triangleq\sum_{l=1}^{L}|\hat{h}_{k,l}[\mu]|^2$ as

Theorem: For arbitrarily long spreading sequences and constant load β the normalized signal to interference ratio $\mathrm{SIR}(\alpha=k/N,\beta=K/N)\triangleq\mathrm{SIR}_k[\mu]/|\hat{\boldsymbol{h}}_k[\mu]|^2$ is in probability lower bounded by

$$\mathrm{SIR}(\alpha,\beta)[\mu]\ge\frac{\gamma^{\mathrm{L}}(\alpha,\beta)}{1+J\gamma^{\mathrm{L}}(\alpha,\beta)},$$

where

$$\gamma^{\mathrm{L}}(\alpha,\beta)=\left(\frac{\sigma_n^2}{\sigma_x^2}+\frac{\alpha(L-1)J}{1+\gamma^{\mathrm{L}}(\alpha,\beta)J}+\right.$$
$$\left.+(\beta-\alpha)L\int_0^\infty\frac{\zeta f_{J|X|^2}(\zeta)}{\sigma_x^2+\gamma^{\mathrm{L}}(\alpha,\beta)\zeta}\mathrm{d}\zeta+\alpha\int_0^\infty\frac{\zeta f_{|\hat{h}|^2+J}(\zeta)}{1+\gamma^{\mathrm{L}}(\alpha,\beta)\zeta}\mathrm{d}\zeta\right)^{-1}.$$

Here, $f_{|\hat{h}|^2+J}(\zeta)$ as well as $f_{a|X|^2}(\zeta)$ denote the pdf of $|\hat{\boldsymbol{h}}|^2+J$, as well as the pdf of the squared absolute value of the transmit symbols $x\in\mathcal{X}$ multiplied by a, respectively.

In addition, for single path fading channels an upper bound can be given resulting from the assumption of correlated channel estimation errors.

Lemma: For a single path fading channel $\mathrm{SIR}(\alpha,\beta)$ is for $N\to\infty$ upper bounded by

$$\mathrm{SIR}(\alpha,\beta)\le\frac{\gamma^{\mathrm{U}}(\alpha,\beta)}{1+J\gamma^{\mathrm{U}}(\alpha,\beta)},$$

where $\gamma^{\mathrm{U}}(\alpha,\beta)=\left(\frac{\sigma_n^2}{\sigma_x^2}+\alpha\int_0^\infty\frac{\zeta f_{|\hat{h}|^2+J}(\zeta)}{1+\gamma^{\mathrm{U}}(\alpha,\beta)\zeta}\mathrm{d}\zeta\right)^{-1}$

Based on the above formulas as well as results on iterative channel estimation we can show that successive cancellation yields considerable gains compared to linear interference suppression even if the channel state is not know exactly at receiver site. It turns out that this advantage depends heavily on the system load as well as number of propagation paths. Moreover, we can show that also in this case nonorthogonal multiple access can reach a higher spectral efficiency than orthogonal schemes. Finally, it is worth noting that other nonlinear receivers, systems with multiple transmit and receive antennas as well as the problem of imperfectly known reference symbols for channel estimation can be treated analytically in the same way.

References

[1] S. Shamai (Shitz) and S. Verdú,"The effect of frequency–flat fading on the spectral efficiency of CDMA", submitted to IEEE Trans. on IT, Nov. 1999.

[2] J. S. Evans and D. N.C. Tse,"Linear Multiuser Receivers for Multipath Fading Channels", submitted to IEEE Trans. on IT, 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On Linear Parallel Interference Cancellation

Mehul Motani, D.R. Brown, C.R. Johnson[1]
Cornell University
Ithaca, NY 14850
{motani,browndr,johnson}@ee.cornell.edu

H.V. Poor
Princeton University
Princeton, NJ 08544
poor@ee.princeton.edu

Abstract — **The performance of the linear parallel interference cancellation (LPIC) receiver in a synchronous multiuser CDMA system with binary signaling is studied. We show that there exist conditions under which the LPIC receiver underperforms other receivers and characterize its asymptotic behavior.**

I. Introduction and Motivation

The linear parallel interference cancellation (LPIC) receiver has been been studied in the literature recently due to its low computational complexity and good performance under certain operating conditions. In this paper, we compare the performance of the LPIC receiver to the hard parallel interference cancellation (HPIC) and conventional matched filter (MF) receivers.

We assume the standard discrete synchronous CDMA system model [1] with K users using binary (± 1) spreading sequences of length N and binary signaling over an additive white Gaussian noise (AWGN) channel with variance σ^2. Let $\boldsymbol{R}$ be the $K \times K$ normalized spreading sequence cross-correlation matrix and $\boldsymbol{A}$ be the $K \times K$ diagonal matrix of positive real amplitudes. If the spreading sequences are chosen randomly, we resort to large system techniques [2, 3] to get analytical results. By "large system", we mean that $K \to \infty$ and $N \to \infty$ but $K/N \to \beta$, for some constant β.

In parallel interference cancellation (PIC), the desired user's decision statistic is formed by subtracting an estimate of the multiple access interference (MAI) from the original observation of the desired user. PIC lends itself to a multistage implementation in which M stages can be used to generate the final decision statistics. The HPIC receiver generates hard bit decisions at each stage to be used in subsequent stages, while the LPIC receiver passes on soft information.

The goal of this paper is to develop a better understanding of the behavior and performance of the LPIC receiver. Some authors have previously noted the performance limitations of the LPIC and others have suggested improvements. We do not propose to fix the LPIC receiver but rather to understand it better so that we can bound the operating regions where the LPIC receiver exhibits good or bad performance. In that spirit, we present a collection of related analytical results which expose the behavior of the LPIC receiver. We refer to [4] for detailed proofs.

II. Results and Conclusions

Our main results are as follows:

1. Let $\mathrm{MSE}_{\mathsf{LPIC}}^{(\ell)}$ and $\mathrm{MSE}_{\mathsf{HPIC}}^{(\ell)}$ be the mean squared error of the ℓ^{th} user's MAI estimate for the two stage LPIC and two stage HPIC receivers respectively. Let $\mathrm{AMSE}_{\mathsf{HPIC}}^{(\ell)}$ be the approximate MSE derived by using a Gaussian approximation for the MAI. Then for any $\boldsymbol{R}$, σ, $\boldsymbol{A}$, K, and ℓ, we show that $\mathrm{MSE}_{\mathsf{LPIC}}^{(\ell)} > \mathrm{AMSE}_{\mathsf{HPIC}}^{(\ell)}$.

2. Let $P_{\mathsf{LPIC}}^{(k)}(M)$ and $P_{\mathsf{MF}}^{(k)}$ be the error probabilities for the M-stage LPIC and the MF respectively for the k^{th} user. Then for any k, M, $\boldsymbol{R} \neq \boldsymbol{I}$, $\sigma > 0$, and interfering user amplitudes $a^{(\ell)}$ $\forall \ell \neq k$, there exists an amplitude threshold $a^* < \infty$ such that $P_{\mathsf{LPIC}}^{(k)}(M) > P_{\mathsf{MF}}^{(k)}$ for $a^{(k)} > a^*$.

3. For any user k in a system with $K > 2$ users, odd M, equal amplitude users such that $\boldsymbol{A} = a\boldsymbol{I}$ and $\frac{a}{\sigma} > 0$, there exists $\boldsymbol{R}$ such that $P_{\mathsf{LPIC}}^{(k)}(M) > 0.5$. We say that the k^{th} user *suffers*.

4. Consider the behavior of the LPIC for large M. Let $\rho(\boldsymbol{R})$ be the spectral radius of $\boldsymbol{R}$, i.e., the maximum magnitude of all eigenvalues of $\boldsymbol{R}$. It is well known that if $\rho(\boldsymbol{R}) < 2$, the LPIC converges to the decorrelating detector. Our result is as follows. If $\rho(\boldsymbol{R}) > 2$, there exists M^* and *at least one* k such that $P_{\mathsf{LPIC}}^{(k)}(M) > 0.5$ for all odd integer values of $M \geq M^*$.

5. An extra constraint on $\boldsymbol{R}$ allows us to show that all users can suffer. Suppose $\rho(\boldsymbol{R}) > 2$ and $\boldsymbol{R}$ has an eigenvector, associated with an eigenvalue greater than two, with all nonzero entries. Then there exists M^* such that *for all* k, $P_{\mathsf{LPIC}}^{(k)}(M) > 0.5$ for all odd integer values of $M \geq M^*$.

6. For randomly chosen spreading sequences and large systems, we show that for any σ, $\boldsymbol{A}$, and ℓ, $E[\mathrm{MSE}_{\mathsf{LPIC}}^{(\ell)}] > E[\mathrm{MSE}_{\mathsf{HPIC}}^{(\ell)}]$. Note that, unlike Result 1, we need not rely upon the Gaussian approximation for the MAI.

7. For randomly chosen spreading sequences and large systems, we show that if $\beta = K/N > (\sqrt{2}-1)^2 \approx 0.17$, then $\rho(\boldsymbol{R}) > 2$ almost surely. Result 4 then indicates that at least one user will suffer in each bit interval for large odd M. More precisely, we note that the misperforming user may be different for each realization of $\boldsymbol{R}$, and so no one user need suffer on average. Numerical experiments suggest that, on average, all users may indeed suffer as $M \to \infty$, but a proof of this conjecture is left as an open problem.

The results in this paper, which indicate that the LPIC has the potential to misperform, are intended to fill in some of the gaps in our understanding of PIC receivers. We hope they can serve as cautionary guidelines concerning the application of LPIC receivers to CDMA communication systems.

[1]This research is supported in part by NSF Grants CCR-9805885, MIP-9811297, EEC-9872436, ECS-9528363, and in part by the Intel Foundation Fellowship.

References

[1] S. Verdu, *Multiuser Detection*, Cambridge Univ. Press, 1998.

[2] S. Verdu and S. Shamai, "Spectral Efficiency of CDMA with Random Spreading", *IEEE Trans. Inform. Th.*, vol. IT-45, pp. 622 - 640, Mar. 1999.

[3] D. Tse and S. Hanly, "Linear Multiuser Receivers: Effective Interference, Effective Bandwidth and User Capacity," *IEEE Trans. Inform. Th.*, v.45, No. 2, pp. 641-657, Mar. 1999.

[4] D.R. Brown, M. Motani, V.V. Veeravalli, H.V. Poor, and C.R. Johnson, Jr., "On the Performance of Linear Parallel Interference Cancellation," submitted to *IEEE Trans. Inform. Th.*, Oct. 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Adaptive Multiuser Parallel-Decision-Feedback with Iterative Decoding

Michael L. Honig[1]
Dept. of ECE
Northwestern University
2145 Sheridan Road
Evanston, IL 60208

Graeme Woodward
Southern-Poro Communications
355A Young St.
Annandale, NSW 2038,
Australia

Paul D. Alexander
Southern-Poro Communications
355A Young St.
Annandale, NSW 2038,
Australia

I. Summary

We combine the *adaptive* (Least Squares) Parallel-Multiuser Decision Feedback Detector for CDMA with short spreading sequences, presented in [1], with iterative (turbo) decoding and soft cancellation, presented in [2]. The resulting receiver requires only a training sequence and (coarse) timing for estimation of all filter coefficients, and performs close to the single-user bound with relatively low E_b/N_0. Prior knowledge of spreading codes and channels is unecessary.

For simplicity, we consider a synchronous CDMA system. The extension to an asynchronous CDMA system with multipath can be achieved by using an expanded observation window [1]. A block diagram of the receiver is shown in Figure 1. Each user's information bits are convolutionally encoded and interleaved before transmission. The received vector of N samples during symbol interval i is $\mathbf{r}(i) = \mathbf{P}\mathbf{d}(i) + \mathbf{n}(i)$ where $\mathbf{P}$ is the matrix of spreading codes, $\mathbf{d}$ is the binary vector of coded symbols across users, and $\mathbf{n}$ is noise. The sequence of vectors $\mathbf{r}(1), \cdots, \mathbf{r}(M)$, corresponding to a packet, is the input to the iterative receiver. Referring to the figure, the output of the DFD is

$$\mathbf{y}^{(m)}(i) = (\mathbf{F}^{(m)})^\dagger \mathbf{r}(i) - (\mathbf{B}^{(m)})^\dagger \bar{\mathbf{d}}^{(m)}(i).$$

where $\mathbf{F}^{(m)}$ and $\mathbf{B}^{(m)}$ are the feedforward and feedback filters, respectively, and $\bar{\mathbf{d}}^{(m)}$ is the vector of soft decisions, all corresponding to the mth iteration.

For purposes of MAP decoding, we assume that the residual interference plus noise at the output of the DFD is Gaussian. It is then possible to estimate the *a priori* probabilities $\Pr\left(y_k^{(m)}(i) | d_k(i) = \pm 1\right)$ without additional side information. These are deinterleaved and input to the MAP decoder for the convolutional code. The MAP decoder generates the *a posteriori* probabilities $\Pr[d_k(i) = \pm 1]$, which are used to compute the input to the feedback filter $\bar{\mathbf{d}}^{(m)} = E[\mathbf{d}]$.

The filters $\mathbf{F}^{(m)}$ and $\mathbf{B}^{(m)}$ are selected to minimize the Least Squares (LS) cost function

$$\mathcal{E}_{LS} = \sum_{i=0}^{M} \|\mathbf{d}(i) - (\mathbf{F}^{(m)})^\dagger \mathbf{r}(i) + (\mathbf{B}^{(m)})^\dagger \bar{\mathbf{d}}^{(m)}(i)\|^2 \qquad (1)$$

at each iteration m, and are constant over the duration of the packet. The symbols $\mathbf{d}$ are obtained either from a training sequence or in decision-directed mode. In the latter case, simulation results show that using soft decisions gives better performance than using hard decisions.

Figure 2 shows a plot of *packet* error rate vs. E_b/N_0 for different receivers. For the MMSE Parallel (P)-DFD curve, the filters $\mathbf{F}^{(m)}$ and $\mathbf{B}^{(m)}$ are computed assuming *perfect* feedback ($\bar{\mathbf{d}} = \mathbf{d}$). The "approximate" LS P-DFD curve is based on minimizing (1), but with soft decisions for $\mathbf{d}$. The results are averaged over random spreading sequences. Data packets contain 500 information symbols and 200 training symbols.

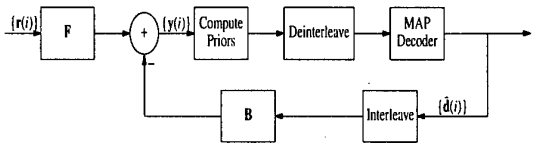


Figure 1: Iterative P-DFD receiver

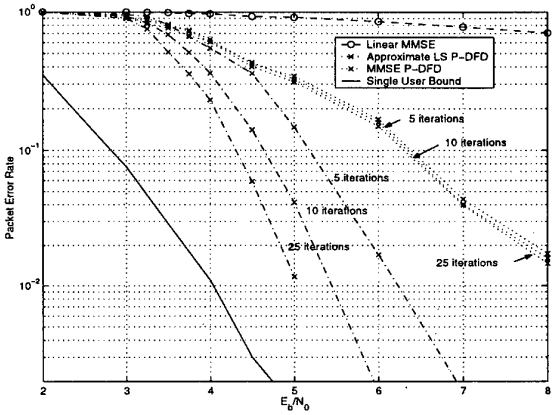


Figure 2: Receiver comparison with $K = 12$ users, $N = 16$, code rate $R = 1/2$ (8 chips per coded bit).

Because of the high load, the linear receiver has a packet error rate near one. The MMSE P-DFD performs *worse* than the LS P-DFD since the latter measures and exploits the joint statistics of the soft estimates with the transmitted symbols. The break point near 3 dB shown in the Figure is close to the fundamental limit based on large system capacity.

References

[1] R. Ratasuk et al, Adaptive multiuser parallel-decision-feedback demodulation. In *Proc. Allerton Conf.*, Monticello, IL, Oct. 1999.

[2] P. D. Alexander et al, Iterative detection in code-division multiple-access with error con trol coding. *European Trans. on Telecomm.*, 9(5):419–425, Sept-Oct 1998.

[1]This work was partially supported by ARO under Grant DAAD19-99-1-0288 and by Southern-Poro Communications

0-7803-5857-0/00/$10.00 ©2000 IEEE.

CDMA Coding and Decoding Methods for Space–Time Block Codes

Jifeng Geng, Li-Chung Chu, Urbashi Mitra and Michael P. Fitz
Department of Electrical Engineering
The Ohio State University, Columbus, OH 43210
E-mail: {gengj, chul, ubli, fitz}@ee.eng.ohio-state.edu

Abstract — **Space-time block code design and decoder design are addressed for Code-Division Multiple-Access (CDMA) systems. Optimal code designs are found by optimizing the Chernoff bound of the probability of decoding error. From this, the diversity gain and the coding gain are determined for the CDMA scenario. The resultant optimal code designs are classified and analyzed. Both optimal and moderate complexity suboptimal decoding algorithms are proposed and evaluated.**

I. Introduction & System Model

Transmit diversity methods have proven effective for combatting fading in wireless communication systems[1, 2, 3, 4]. In this paper, we focus on determining space-time block coding methods for Code-Division Multiple-Access systems. *Due to the assumption of independent fading for different users; the multiuser coding problem decouples to multiple single-user coding problems.* The presence of spreading codes in the CDMA problem yields interesting differences in code designs and code metrics relative to the single-user narrowband case [4].

The up-link between K users and one base station is considered. For each user, k_c information bits are mapped to one of 2^{k_c} Space–Time Block Codes (STBC), D. The codeword D is a matrix of dimension $L_t \times M$; where M is the number of transmit antennae and L_t is the duration, in symbol intervals, of the code. It is assumed that the base station has N receive antennae. We further assume that: the fading processes associated with each transmit antenna are independent; the channel is constant over the duration of the block code (quasi-static) and is known perfectly; and that the transmission is synchronous. For the system under consideration, a different spreading code is employed for each transmit antenna and it is assumed that the receiver has full knowledge of these spreading codes.

II. Performance Criteria & Code Designs

It can be shown that optimizing the upper bound on the probability of decoding error yields two criteria for space-time block code design. Performance is determined by a key matrix $\Phi = \Delta D^H \Delta D \odot R$ [1], where ΔD is a codeword difference matrix and R is the spreading code cross-correlation matrix. The resultant design "metrics" over all pairs of codewords are:

diversity gain $\Delta_H = N r_{min}$, where r_{min} is the minimum rank of Φ.

coding gain $\Delta_p = \left(\prod_{i=1}^{r_{min}} \lambda_i\right)^N$ is the smallest product of all the non-zero eigenvalues of Φ.

These "metrics" are analogous to those obtained in [1] for the narrowband case, but due to the presence of the cross-correlation matrix, R, some new features appear in the resulting optimal codes. The goal of code design is to find 2^{k_c} distinct STBCs such that r_{min} is maximized and given this rank, that Δ_p is also maximized. Codes satisfying these conditions are deemed *optimal.* The following two propositions can be proved regarding diversity gain and coding gain:

PROPOSITION 1 *If ΔD has no zero columns and if R is positive definite, full diversity gain is always achieved.*

PROPOSITION 2 *If $R_{ij} = \rho$ for $i \neq j$, the coding gain is a monotonically decreasing function of ρ.*

Note that for the narrowband case, $\rho = 1$ and R is thus singular. For the CDMA case, due to these two propositions, we focus on maximizing Δ_p. We observe that *non-unitary codes usually outperform unitary codes.* Consider the optimal code sets for BPSK modulation. We discuss the case of $k_c = 2$, $M = 2$ and $L_t = 2$. The resulting optimal codes can be partitioned into three equivalence classes. Each element of the equivalence class can be transformed into another element via simple isometries. Each class has a uniform distance spectrum across codewords. Class 1 and 2 are optimal for all $|\rho| \leq 1$ while Class 3 is optimal for $|\rho| \leq \sqrt{3}/2$. Class 2 is essentially Alamouti's orthogonal code set [3] while Class 1 is non-unitary [4]. Interestingly, for QPSK modulation, we can find an optimal non-unitary code set which outperforms all unitary codes for all $|\rho| \leq 1$. The optimal codes are tabulated below.

symbol	Class	D1		D2		D3		D4	
BPSK	1	1	1	1	-1	-1	1	-1	-1
		1	1	-1	-1	1	-1	-1	1
BPSK	2	1	1	1	-1	-1	1	-1	-1
		1	-1	-1	-1	1	1	-1	1
BPSK	3	1	1	1	-1	-1	1	-1	-1
		1	1	-1	1	1	-1	-1	-1
QPSK		1	1	1	-1	-1	i	-i	-i
		1	i	-1	i	-i	1	i	-i

III. Decoding Algorithms

Three types of decoders are considered: the optimal maxmimum-likelihood (ML) decoder, a joint multiuser minimum mean-squared error decoder and a combined interference cancellation/ML decoder. These algorithms perform as predicted with the ML decoder offering the best performance at the expense of computational complexity. The two suboptimal algorithms offer solid performance with reduced complexity.

[2]This work was supported by NSF Grant ANI-9809018.

[1]Here $\odot$ represents Schur product.

References

[1] V. Tarokh, N. Seshadri, and A. R. Calderbank, "Space-time codes for high data rate wireless communication: Performance criterion and code construction," *IEEE Trans. on Information Theory*, vol. 44, pp. 744–765, March 1998.

[2] C. Papadias, "On the Spectral Efficiency of Space-Time Spreading Schemes for Multiple Antenna CDMA Systems," *Proc. 33rd Asilomar Conference on Signals, Systems and Computers*, Pacific Grove, CA, October 1999.

[3] S. M. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE Trans. on Select Areas in Comm.*, vol. 16, pp. 1451–1458, October 1998.

[4] B. L. Hughes, "Differenctial Space-Time Modulation," in *Proc. IEEE WCNC'99*, New Orleans, LA, September 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Multiple Antennas and Representation Theory

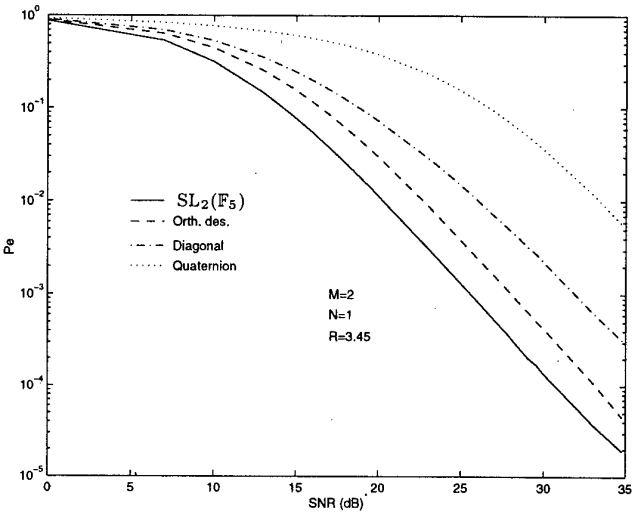
Babak Hassibi, Bertrand Hochwald, Amin Shokrollahi, and Wim Sweldens
Mathematical Sciences Center
Lucent Technology
600 Mountain Avenue
Murray Hill, NJ 07974
e-mail: {hassibi,hochwald,mshokrollahi,wim}@lucent.com

Abstract — **Multiple antennas can greatly increase the data rate and reliability of a wireless communication link in a fading environment, but the practical success of using multiple antennas depends crucially on our ability to design high-rate space-time constellations with low encoding and decoding complexity. It has been shown that full transmitter diversity, where the constellation is a set of unitary matrices whose differences have nonzero determinant, is a desirable property for good performance.**

We use the powerful theory of fixed-point-free groups and their representations to design high-rate constellations with full diversity. Furthermore, we thereby classify all full-diversity constellations that form a group, for all rates and numbers of transmitter antennas. The group structure makes the constellations especially suitable for differential modulation and low-complexity decoding algorithms.

The classification also reveals that the number of different group-structures with full diversity is very limited when the number of transmitter antennas is large and odd. We therefore also consider extensions of the constellation designs to nongroups. We conclude by showing that many of our designed constellations perform excellently on both simulated and real wireless channels.

A complete copy of this paper is available on the web at `http://mars.bell-labs.com` under the title "Representation Theory for High-Rate Multiple-Antenna Code Design." Other related papers are also available at this web site.



Block-error rate performance of the group $SL_2(\mathbb{F}_5)$ compared with constellations from other constructions for $M = 2$ transmitter antennas and $N = 1$ receiver antenna. The channel is known at the receiver. The solid line is $SL_2(\mathbb{F}_5)$, which has 120 unitary matrices (rate $R \approx 3.45$). The dashed line is an orthogonal design with 11th roots of unity ($R \approx 3.46$). The dashed-dotted line is the best diagonal (Abelian group) construction ($R \approx 3.45$). The dotted line is the quaternion group with 128 matrices ($R = 3.5$).

I. An Example of a High-Rate Code

As an example of a high-rate group code that we find, we plot the performance of $SL_2(\mathbb{F}_5)$, the group of 2×2 matrices over the field $\mathbb{F}_5$ with determinant one. This group has a representation as 120 complex 2×2 unitary matrices suitable for transmission over a two-antenna fading channel. The group is fixed-point-free which means that its constellation has full diversity. We also plot the performance of the best cyclic group with the same rate [2], a 2×2 orthogonal design [4] (which is not a group) and a generalized quaternion group code [3] with similar rates. All of these codes can be used with a known channel (as shown), or they can be used differentially when the channel is unknown and with a performance loss of approximately 3 dB.

References

[1] B. Hassibi, B. Hochwald, A. Shokrollahi and W. Sweldens, "Representation theory for high-rate multiple-antenna code design," Bell Labs. tech. report, Mar. 2000.

[2] B. Hochwald and W. Sweldens, "Differential unitary space-time modulation," submitted to *IEEE Trans. Comm.*, Also, Bell Labs. tech. report, Mar., 1999.

[3] B. Hughes, "Differential Space-Time Modulation," submitted to *IEEE Trans. Info. Theory*, 1999.

[4] V. Tarokh, H. Jafarkhani and A. R. Calderbank, "Space-time block codes from orthogonal designs," *IEEE Trans Info. Theory*, vol. 45, pp. 1456–1467, July 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

The Expectation-Maximization Algorithm for Space-Time Communications

Carmela Cozzo and Brian L. Hughes [1]
Center for Advanced Computing and Communication
Department of Electrical and Computer Engineering
North Carolina State University
Raleigh, NC 27695-7914
{ccozzo,blhughes}@eos.ncsu.edu

Abstract — **This paper investigates the application of the expectation-maximization algorithm for systems with multiple transmit and/or receive antennas in presence of fast fading channels.**

I. Introduction

The use of space-time coding and modulation techniques can improve system performance and combat the damaging effects due to the presence of fading. Most work has assumed that accurate estimates of current channel fading conditions are available at the receiver [4, 5, 6]. When channel estimation becomes very challenging, e.g. in fast fading channels, it is of interest to explore joint channel estimation and data detection methods in order to approach coherent performance with a minimum of pilot symbols.

For single-antenna channels, suboptimal receivers based on the expectation-maximization (EM) algorithm have been shown to perform well under fast fading [2] and multipath fading [3] conditions. The EM algorithm is a general two-steps procedure for iterative maximum likelihood estimation. The algorithm was first formalized in the statistics literature by Dempster, Laird, and Rubin [1], and has since been applied to a variety of communications problems.

We consider a system with multiple transmit and receive antennas, and propose a suboptimal space-time receiver based on the EM algorithm, which performs iterative joint channel estimation and data sequence detection in alternating steps. We derive simple expressions for these steps and evaluate the performance of the resulting receiver for several modulation techniques.

II. Receiver Structure

Consider a wireless channel with t transmit and r receive antennas. The signal sample taken by receive antenna i at time k can be modeled, for $i = 1, \ldots, r$, $k = 1, \ldots, n$, as

$$y_{ik} = \sum_{j=1}^{t} h_{ij}(k) c_{jk} \sqrt{\rho_t} + n_{ik} , \qquad (1)$$

where c_{jk} is the constellation point transmitted, $h_{ij}(k)$ is the fading path gain, ρ_t is the signal-to-noise ratio and n_{ik} are noise samples. In matrix form, (1) can be rewritten as

$$Y = \sqrt{\rho_t} H_v C_v + N , \qquad (2)$$

where $H_v = [H_1 : H_2 : \cdots : H_n]$ is $r \times nt$, C_v is the $nt \times n$ block-diagonal matrix, ρ_t is the signal-to noise ratio and N is the noise matrix. Each row of H_v is iid with covariance matrix S.

The receiver performs iteratively two steps: Expectation step and Maximization step. The E-step can be evaluated as

$$\begin{aligned} Q(C_v|C_v^i) &= \mathcal{E}\left[\log p(Y|H_v, C_v) \mid Y, C_v^i\right] \\ &= -\mathrm{Tr}\{(Y - \sqrt{\rho_t}\hat{H}_v^i C_v)^\dagger (Y - \sqrt{\rho_t}\hat{H}_v^i C_v) \\ &\quad + r\rho_t C_v^\dagger \Sigma_v^i C_v\} - rn \log \pi , \end{aligned} \qquad (3)$$

where $\hat{H}_v^i = \sqrt{\rho_t} Y C_v^{i\dagger} \Sigma_v^i$ and $\Sigma_v^i = (S^{-1} + \rho_t C_v^i C_v^{i\dagger})^{-1}$ are the channel estimate and the error covariance matrix, respectively, at the i-th iteration.

The M-step calculates the next estimate by $C_v^{i+1} = \arg\max_{C_v} Q(C_v|C_v^i)$. The expression (3) can be recursively maximized by using the Viterbi Algorithm with a modified metric which consists of the Euclidean distance metric plus a quadratic term that depends on the previous decoded sequence C_v^i. Thus, each iteration consists of an estimation phase followed by a detection phase.

The initial estimate C^0 for the iterative receiver will generally be derived using a pilot-symbol-assisted modulation scheme.

Simulations suggest that the receiver can often achieve near-coherent performance with only two iterations and using a very small number of pilot symbols under fast fading conditions.

[1] This work was supported in part by the National Science Foundation under grants CCR-9903107, and by the Center for Advanced Computing and Communication.

References

[1] A. P. Dempster, N. M. Laird and D. R. Rubin, "Maximum likelihood from incomplete data via the EM algorithm," *Journal of the Royal Statistical Society*, Series B (Methodological), vol. 39, no. 1, pp. 1-38, 1977.

[2] C. N. Georghiades and Jae Choong Han, "Sequence estimation in the presence of random parameters via the EM algorithm," *IEEE Trans. on Comm.*, vol. 45, no. 3, pp. 300-308, Mar. 1997.

[3] G. Kaleh, "Joint parameter estimation and symbol detection for linear and nonlinear unknown channels," *IEEE Trans. on Comm.*, vol. 42, no. 7, pp. 2406-2413, July 1994.

[4] V. Tarokh, H. Jafarkhani and A. R. Calderbank, "Space-time block codes from orthogonal designs," *IEEE Trans. on Info. Theory*, vol. 45, no.5, pp. 1456-1467, July 1999.

[5] V. Tarokh, N. Seshadri and A. R. Calderbank, "Space-time codes for high data rate wireless communication: performance criteria and code construction," *IEEE Trans. on Info. Theory*, vol. 44, no. 2, pp. 744-765, Mar. 1998.

[6] A. Wittneben, "A new bandwidth efficient transmit antenna modulation diversity scheme for linear digital modulation," *Proc. IEEE ICC*, pp. 1630-1634, Mar. 1993.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Further Results on the Algebraic Design of Space-Time Codes

A. Roger Hammons Jr.
Hughes Network Systems
Germantown, MD, USA
e-mail: rhammons@hns.com

Hesham El Gamal
Hughes Network Systems
Germantown, MD, USA
e-mail: helgamal@hns.com

Abstract — **Recently, the authors presented a new threaded space-time architecture [1][2] combining generalized layered transmission, advanced iterative multi-user detection techniques, and space-time code design that provides superior performance compared to the layered architectures proposed by Foschini *et al.* [3] and Tarokh *et al.* [7]. In this paper, we discuss the design of algebraic space-time codes for layered and non-layered architectures.**

I. Introduction

Two essentially different approaches have been proposed for exploiting the spatial diversity available to systems with multiple transmit and receive antennas operating over fading channels. In the first, channel coding is performed using so-called "space-time codes" [4][6][5]. In the second, conventionally-encoded data streams are "layered" in space and time by the transmitter and separated at the receiver using interference-cancellation and interference-avoidance signal processing [3]. A new "threaded" space-time architecture, introduced in [1][2], shows that significant gains are possible without undue complexity, however, when the encoding, interleaving, and distribution of transmitted symbols among different antennas are optimized to maximize spatial diversity, temporal diversity, and coding gain in accordance with space-time code design principles.

II. Algebraic Space-Time Code Design

We consider a communication system with n transmit and m receive antennas. A space-time code $\mathcal{C}$ consists of an underlying channel code C together with a spatial modulator function $\mathbf{f}$ that parses the modulated symbols among the transmit antennas. Binary rank criteria developed in [5] made possible the first designs of space-time codes by algebraic means.

Thm 1 (Stacking Construction)[5] *Let $\mathcal{C}$ be the space-time code of dimension k consisting of the $n \times \ell$ code word matrices $\mathbf{c} = \left[\, \bar{x}\mathbf{M}_1 \;\; \bar{x}\mathbf{M}_2 \;\; \cdots \;\; \bar{x}\mathbf{M}_n \,\right]^{\mathrm{T}}$, where $\mathbf{M}_1, \mathbf{M}_2, \ldots, \mathbf{M}_n$ are binary matrices of dimension $k \times \ell$ and $\bar{x}$ denotes the k-tuple of information bits. Then, for BPSK transmission over the quasi-static fading channel, $\mathcal{C}$ achieves full spatial diversity nm provided*

$$\forall a_1, a_2, \ldots, a_n \in \mathsf{F}, \text{ not all zero}: \quad \mathbf{M} = a_1\mathbf{M}_1 \oplus a_2\mathbf{M}_2 \oplus \cdots \oplus a_n\mathbf{M}_n \text{ is of rank } k \text{ over } \mathsf{F}.$$

Furthermore, if $\mathbf{M}_1, \mathbf{M}_2, \ldots, \mathbf{M}_n$ are $\mathbf{Z}_4$-valued matrices whose projections modulo 2 satisfy the above constraint, then the corresponding $\mathbf{Z}_4$ space-time code $\mathcal{C}$ achieves full spatial diversity for QPSK transmission.

In a layered architecture, a similar algebraic construction is applicable to arbitrary signaling constellations Ω of size 2^b.

Thm 2 (Threaded Stacking Construction) *Let L be a layer of spatial span n. Given binary $k \times \ell$ matrices $\mathbf{M}_1, \mathbf{M}_2, \ldots, \mathbf{M}_n$, let C be the binary code consisting of the vectors $c(\bar{x}) = \bar{x}\mathbf{M}_1 \,|\, \bar{x}\mathbf{M}_2 \,|\, \cdots \,|\, \bar{x}\mathbf{M}_n$, where $\bar{x}$ denotes a k-tuple of information bits. Let $\mathbf{f}_L$ be the spatial modulator in which the modulated symbols associated with $\bar{x}\mathbf{M}_j$ are transmitted in the ℓ/b symbol intervals of L that are assigned to antenna j. Then, the space-time code $\mathcal{C}$ consisting of C and $\mathbf{f}_L$ achieves spatial diversity dm in a quasi-static fading channel iff d is the largest integer such that*

$$\forall a_1, a_2, \ldots, a_n \in \mathsf{F}, a_1 + a_2 + \cdots + a_n = n - d + 1: \quad \mathbf{M} = [a_1\mathbf{M}_1 a_2\mathbf{M}_2 \cdots a_n\mathbf{M}_n] \text{ is of rank } k \text{ over } \mathsf{F}.$$

The stacking constructions are general for any number of antennas and apply to trellis as well as block codes. The observation in [5] that the stacking construction is readily satisfied within the class of binary rate $1/n$ convolutional codes is particularly noteworthy. Indeed, most of the well-known convolutional codes of rate $1/n$ with optimal d_{free} can be formatted to achieve full spatial diversity!

Similarly, the natural space-time codes associated with the general class of binary rate k/n convolutional codes are attractive candidates for the layered space-time architecture since they can be easily formatted via periodic bit interleaving to satisfy the generalized layered stacking construction. In this case, a total transmission rate of $b(n-d+1)$ bits per signaling interval can be achieved, which is the maximum possible.

Example. The natural layered space-time code associated with the optimal 8-state, $d_{\text{free}} = 5$ convolutional code (with generators $G_0(D) = 1 + D^2$ and $G_1(D) = 1 + D + D^2$) achieves maximum possible spatial diversity for $n = 2$, 4, and 6 transmit antennas. The achieved diversity levels are $d = 2$, 3, and 4, respectively, in accordance with Theorem 2.

References

[1] H. El Gamal and A.R. Hammons Jr., "New approach to space-time transmitter/receiver design," In *Thirty-Seventh Annual Allerton Conf.*, Sep. 1999.

[2] H. El Gamal and A.R. Hammons Jr., "The layered space-time architecture: a new perspective," Submitted *IEEE Trans. Info. Th.*, September 1999.

[3] G.J. Foschini and M. Gans, "On the limits of wireless communication," *Wireless Personal Comm.*, 1998.

[4] J.-C. Guey *et al.*, "Signal design for transmitter diversity wireless communication," In *1996 IEEE Veh. Tech. Conf.*

[5] A.R. Hammons Jr. and H. El Gamal, "On the theory of space-time codes for PSK modulation," *IEEE Trans. Info. Th.*, Mar. 2000.

[6] V. Tarokh *et al.*, "Space-time codes for high data rate wireless communication," *IEEE Trans. Info. Th.*, Mar. 1998.

[7] V. Tarokh *et al.*, "Combined array processing and space-time coding," *IEEE Trans. Info. Th.*, May 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Best Tailbiting Convolutional Encoders Using a Priori Information

Marc Handlery
Department of Information Technology
Lund University, Box 118
S-221 00 Lund, Sweden
e-mail: marc@it.lth.se

John B. Anderson
Department of Information Technology
Lund University, Box 118
S-221 00 Lund, Sweden
e-mail: anderson@it.lth.se

Abstract — **The bit error rate of tailbiting convolutional encoders is compared for the case that *a priori* source information is available, and for the case that it is not. The set of best encoders depends on the *a priori* information, and is not identical to the set of encoders maximizing minimum distance. Characteristics that govern the BER are analyzed.**

Summary

The bit error rate (BER) is an important encoder criterion. The question arises which encoder to use in a specific environment. We compare the BER performance of tailbiting convolutional (TB) encoders for the BSC and AWGN channel with different noise powers when differing amounts of *a priori* information are available to the decoder.

A TB encoder must end in the same state it started. A codeword can be viewed as a path around a circular trellis. TB codes are an efficient tool to supply error protection for short packets, since they do not suffer any rate loss due to a terminating zero-tail. In general, they achieve the minimum distance ($d_{\min}$) of the best known block codes. Besides, TB codes allow trellis decoding.

The apt decoder is the *symbol-by-symbol maximum a posteriori* algorithm, denoted as MAP decoder. With trellis decoding, the well-known BCJR algorithm computes the *a posteriori* probability (APP) of each data symbol. The data symbol with highest APP is chosen as the MAP decoder output. In order to achieve a lower BER the *a priori* information is taken into account. In [1] we extended the original BCJR algorithm to the TB environment. This algorithm (TB-BCJR) does not quite obtain the true MAP output, but it is a factor 2^m simpler than the true MAP decoder, where m denotes the memory of the TB encoder. Here, the BER of rate 1/2 feedforward TB encoders is measured using the TB-BCJR algorithm.

Let L be the tail-biting length. The ith bit of the data word is denoted by u_i, $1 \le i \le L$. Define the source bit probability $\phi_i = \mathrm{P}\{u_i = 0\}$, $1 \le i \le L$. Assume now that $\phi_i = 1/2$, $\forall i$. A table of best rate 1/2 TB encoders for the BER criterion is shown in [2]. The BERs are listed at three SNR benchmarks for the BSC and AWGN channels. In general, the list of best encoders differs in each of these cases. The main conclusions are as follows.

(i) The BER of the best encoder of memory m does not decrease further with growing L once the ratio L/m exceeds 4–5. Analogously, the BER does not decrease much with growing m and constant L. The critical ratio L/m relates to the decision depth parameter of the encoder, which relates asymptotically to the Gilbert-Varshamov parameter.

(ii) The best encoder in a bad channel is a systematic one. Systematic feedforward codes have asymptotically half the free distance growth with m, compared to general codes. Thus the best encoder in a channel of unknown quality is a feedback systematic one, since these have full distance growth; its BER will be low in both good and bad channels.

(iii) In about half the combinations m, L the best encoders in a BSC differ significantly from those in the AWGN channel.

(iv) Due to the mapping between information and codebits, the best encoders are in general not the ones maximizing $d_{\min}$.

Now, assume an unbalanced information source, i.e., $\phi_i \lesseqgtr 1/2$, $1 \le i \le L$. Some data words and their corresponding codewords have a higher probability than others.

In [3] we present good TB encoders in terms of BER when *a priori* information is available. Their performances are listed for the same channels as before. The main results are:

(i) In general, for BSCs the best encoders for balanced sources perform badly if a lot of *a priori* information is available, e.g., if ϕ_i=0.95, $\forall i$. This is because now the codewords with low Hamming weight are more likely to occur. If the codewords with $d_{\min}$, i.e., the ones which are most likely to be decoded in error for a balanced source, are unlikely to occur, then the *a priori* information will drastically reduce the BER.

(ii) For BSCs the best encoders for ϕ_i=0.5, $\forall i$, are generally also the best when ϕ_i=0.7, $\forall i$. If the source is not strongly unbalanced, the effect described in (i) looses importance.

(iii) The best encoders for ϕ_i=0.95, $\forall i$, perform poorly when used for data with ϕ_i=0.5 or ϕ_i=0.7, compared to the best encoders for those cases, for which the mapping of data to codebits and the distance spectrum play the major role. The best encoders for AWGN channels for ϕ_i=0.5, $\forall i$, also differ from the best encoders for strongly unbalanced sources, but their BER can be almost as good.

(iv) For ϕ_i=0.95, $\forall i$, the best encoders for a BSC are not the best encoders for a AWGN channel, and vice versa, although they also perform sufficiently well for the other channel model.

(v) The encoders maximizing $d_{\min}$ are generally not those with best BER.

(vi) When not all data bits carry the same *a priori* information, the BER depends on the positions of the bits with most *a priori* information. Similar arguments as in (i) explain this effect. In general, the TB encoder and the amount and structure of the *a priori* information must be tuned to each other.

References

[1] J.B. Anderson and S.M. Hladik, "Tailbiting MAP Decoders," *IEEE J. Sel. Areas Commun.*, vol. 16, pp. 297–302, Feb. 1998.

[2] J.B. Anderson, "Best Short Rate 1/2 Tailbiting Codes for the Bit Error Rate Criterion," accepted, *IEEE Trans. Commun.*, 1999.

[3] M. Handlery, "Bit Error Rate Performance of Tailbiting Convolutional Encoders with Unbalanced Source Bit Probabilities," Diploma Thesis, ETH Zürich, and Lund University, Feb. 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Searching for tailbiting codes with large minimum distances

Irina E. Bocharova and
Boris D. Kudryashov
Dept. of Inform. Systems
University on Airspace
Instrumentation
St.-Petersburg, 190000, Russia,
e-mail: {Irina,Boris}@kb.spb.su

Rolf Johannesson and
Per Stâhl
Dept. of Inform. Technology
Lund University
P.O. Box 118
SE-221 00 LUND, Sweden,
e-mail: {Rolf,Per}@it.lth.se

Abstract — **Tailbiting trellis representations of linear block codes with an arbitrary sectionalization of the time axis are studied. A new lower bound on the maximal state complexity of an arbitrary tailbiting code is derived. The asymptotic behavior of the derived bound is investigated. Some new tailbiting representations for linear block codes of rates $R = 1/c$, c = 2,3, 4 are presented.**

I. Introduction

Tailbiting is a technique to terminate a convolutional code into a block code [1]. We focus on constructions and bounds for sectionalized tailbiting trellises since they may have less complexity than non-sectionalized ones.

We consider an $(N, K, d_{\min})$ binary linear block code $\mathcal{C}$ with a generator matrix $\boldsymbol{G} = \{\mathbf{r}_i\}, i = 1, ..., K$. We say that $\boldsymbol{G}$ is given in *tailbiting span form* if it consists of rows such that (circular) start($\mathbf{r}_i$) $\neq$ start($\mathbf{r}_j$) and end($\mathbf{r}_i$) $\neq$ end($\mathbf{r}_j$), $i \neq j$, where start($\mathbf{x}$) and end($\mathbf{x}$) denote the (circular) number of the first and the last nonzero section in the vector $\mathbf{x}$, respectively. The ith section of $\mathbf{r}_j$ is *active* if $i \in [\text{start}(\mathbf{r}_j), \text{end}(\mathbf{r}_j))$. The maximal state complexity or μ-state complexity of the trellis is defined [2] as $\mu = \max_i\{\log_2 |A_i|\}$, where $|A_i|$ denotes the number of rows where the ith section is active.

II. Lower bound on the state complexity for tailbiting codes

Theorem 1 *The state complexity μ of a linear $(N, K, d_{\min})$ tailbiting code is lower-bounded by*

$$\mu \geq \mu_0 = \left\lceil \max_{j=1,\ldots,K} \{RN_{\min}(j, d_{\min}) - j\} \right\rceil .$$

Moreover, if μ_0 is odd $\mu \geq \max\{\mu_0, d_{\min}(K+1)/N - 1\}$.

Denote by $\zeta = \mu/N$ the relative trellis complexity. Then we have the following asymptotic behavior of ζ as $N \to \infty$,

$$\zeta \geq \max_{\theta \in [2\delta, 1]} \{\theta [R - R_{\max}(\delta/\theta)]\},$$

where $\delta = d_{\min}/n$, and $R_{\max}(\cdot)$ is the McEliece-Rodemich-Rumsey-Welch upper bound.

III. Search techniques and results

We have used the bound in Theorem 1 to find an efficient (in sense of state complexity) tailbiting representation for an (N, K) linear block code using time-invariant convolutional codes of rate $R = 1/c$, c = 2,3,4, and state complexity (constraint length) μ. We exploit two kinds of methods to reject weak codes. The first one includes rules for rejecting weak encoders of convolutional codes. The second one rejects those encoders among the accepted ones which generate poor tailbiting codes. Some search results are presented in the following table.

$N, K, d_{\min}(\hat{d}_{\min})$	$\mu(\hat{\mu})$	Generators
56,28,12(12-14)	9(8)	477,1505
58,29,12(12-14)	9(8)	433,1275
60,30,12(12-14)	9(8)	217,1665
62,31,12(12-15)	8(8)	435,657
64,32,12(12-16)	8(8)	235,557
66,33,12(12-16)	8(8)	235,557
68,34,13(13-16)	11(9)	4315,5651
72,36,14(15-18)	13(10)	4473,32611
74,37,14(14-18)	11(10)	1353,7461
76,38,14(14-18)	11(10)	1145,7173
78,39,14(15-18)	10(10)	1473,2275
82,41,14(14-20)	10(10)	1157,3455
84,42,14(15-20)	10(10)	1157,3455
92,46,16(15-22)	13(11)	5447,21675
94,47,16(16-22)	12(11)	5135,14477
96,48,16(16-22)	12(11)	5135,14477
110,55,18(18-25)	15(14)	23077,173255
84,28,22(22-27)	11(10)	2215,5467,7647
96,32,24(24-30)	12(11)	2153,11625,17557
99,33,24(24-32)	11(11)	4467,5725,6373
102,34,24(24-32)	11(11)	4465,5357,6373
105,35,25(24-33)	13(13)	20447,25315,37317
108,36,26(24-34)	13(13)	20465,31327,34773
111,37,26(25-34)	13(13)	20445,31527,35757
114,38,26(26-36)	13(13)	20445,31653,37673
120,40,28(28-37)	14(14)	41127,63663,72575
112,28,32(32-40)	11(11)	4447,5277,6335,7533
116,29,32(32-42)	11(11)	4445,6353,6537,7673

Almost all codes meet the Brower-Verhoeff (BV) lower bound $\hat{d}_{\min}$ on the minimum distance for linear codes and achieve the lower bound $\hat{\mu}$ on the state complexity. All presented codes are new best known quasi-cyclic codes. The code (111,37,26) is better than any previously known linear code with the same length and dimension, and the codes (92,46,16), (105,35,25) and (108,36,26) are better than any previously known codes with the same length and dimension.

References

[1] G. Solomon and H. C. A. van Tilborg, "A connection between block and convolutional codes," *SIAM J. Appl. Math.*, vol. 37, pp. 358-369, 1979.

[2] A. R. Calderbank, G. D. Forney, Jr. and A. Vardy, "Minimal tail-biting trellises: the Golay code and more," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1435-1455, 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Decoding of Codes Based on Their Tail Biting Trellises

Rose Y. Shao
Quantum Corporation
Shrewsbury, MA 01545
rose.shao@quantum.com

Shu Lin
University of California, Davis
Davis, CA 95616
shulin@ece.ucdavis.edu

Marc P.C. Fossorier
University of Hawaii at Manoa
Honolulu, HI 96822 USA
marc@spectra.eng.hawaii.edu

I. Introduction

A tail biting (TB) trellis for a code is a trellis with multiple starting and multiple ending states [1, 2]. Each starting state corresponds to a unique ending state and they are the same state. A path in a TB trellis represents a valid codeword if and only if it starts from a state and ends at the same state. Such a path is called a TB path. In this paper, two new iterative algorithms for decoding codes based on their TB trellises are presented, one is unidirectional and the other is bidirectional. Both algorithms are computationally efficient and achieves virtually optimum error performance with a small number of decoding iterations.

II. The Wrap-Around Viterbi (WA-V) Algorithm

Let T be an L-section TB trellis for a code C with section boundary locations in $\{0, 1, \cdots, L\}$. For $0 \leq t \leq L$, let $\Sigma_t(C) = \{s_t^{(1)}, s_t^{(2)}, \cdots, s_t^{(q_t)}\}$ denote the state space of the trellis at the boundary location(BL)-t. $\Sigma_0(C)$ and $\Sigma_L(C)$ are the starting and ending state spaces, respectively, and $\Sigma_0(C) = \Sigma_L(C)$. For simplicity, we assume that $s_0^{(i)}$ and $s_L^{(i)}$ are the same state for $1 \leq i \leq q_0$(or q_L).

The WA-V algorithm processes T continuously in a round-and-round manner. One round of decoding process is called an iteration. At the beginning of the first iteration, the decoder starts from all the states in $\Sigma_0(C)$ at BL-0 with the same initial state metrics. At the end of each iteration, the decoder attempts to make a decoding decision. If the decoding decision is successful, the decoding process stops; otherwise, the decoder wraps around T and starts another iteration from the states in $\Sigma_0(C)$ with the starting state metrices equal to the metrics of their equivalent states in $\Sigma_L(C)$ at the end of the previous iteration. Suppose the decoder is executing the i-th iteration. For each state $s_t^{(j)}$ in T, the decoder computes two metrics, the accumulative state metric(ASM) and the state metric gain(SMG). The ASM of a state $s_t^{(j)}$ at BL-t in the i-th iteration, denoted $M^{(i)}(t, s_t^{(j)})$, is defined as the total path metric of the survivor that originates from a state $s_0^{(k)}$ at the beginning of the first iteration and terminates at the state $s_t^{(j)}$. The SMG of the state $s_t^{(j)}$ during the i-th iteration, denoted $\Delta^{(i)}(t, s_t^{(j)})$, is defined as the path metric of the survivor $\mathbf{p}^{(i)}(s_0^{(l)}, s_t^{(j)})$ that originates from the state $s_0^{(l)}$ at BL-0 at the beginning of the i-th iteration and terminates at the state $s_t^{(j)}$. Therefore, $\Delta^{(i)}(t, s_t^{(j)}) = M^{(i)}(t, s_t^{(j)}) - M^{(i)}(0, s_0^{(l)})$, where $M^{(i)}(0, s_0^{(l)}) = M^{(i-1)}(L, s_L^{(l)})$ and $M^{(1)}(0, s_0^{(k)})$=constant, for all $1 \leq k \leq q_0$. When the decoder reaches BL-L at the end of the i-th iteration, there are q_L survivors $\mathbf{p}^{(i)}(s_0^{(l)}, s_L^{(j)})$ of length L, each terminates at a different state $s_L^{(j)}$ at BL-L. The path $\mathbf{p}^{(i)}(s_0^{(l_0)}, s_L^{(j_0)})$ with the best metric gain $\Delta^{(i)}(L, s_L^{(j_0)})$ is chosen as the winning path. If the winning path $\mathbf{p}^{(i)}(s_0^{(l_0)}, s_L^{(j_0)})$ is a TB path, decoding stops and $\mathbf{p}^{(i)}(s_0^{(l_0)}, s_L^{(j_0)})$ is the decoded codeword. Otherwise, find the TB path with the best metric (if any), denoted $\mathbf{p}_{T,best}^{(i)}$, and store it. The decoder then starts the $(i+1)$-th iteration. Decoding process continues until either the winning path at the end of an iteration is a TB path or a preset maximum number of iterations I_{max} is reached. For the latter case, the decoder outputs the best TB path $\mathbf{p}_{T,best}$ stored in the memory if it exists; otherwise, it outputs the winning path found at the end of the I_{max}-th iteration.

III. The Iterative Bidirectional Viterbi Decoding (IBVD) Algorithm

This algorithm processes a TB trellis T of a code from opposite directions with two decoders, called the left- and the right-decoder, respectively. Both decoders execute the WA-V algorithm and they collaborate to make a decoding decision. During each iteration, the two decoders start from opposite ends of T, work through the trellis until they reach the other ends of T. For each state in the trellis, two ASM's and two SMG's are computed by the two decoders. At iteration-i, as soon as a state $s_t^{(j)}$ has been visited by both decoders, it has two SMG's, denoted $\Delta_l^{(i)}(t, s_t^{(j)})$ and $\Delta_r^{(i)}(t, s_t^{(j)})$, from the left and the right decoders. The sum of these two SMG's, denoted $\Delta_c^{(i)}(t, s_t^{(j)})$ is called the composite SMG of the state $s_t^{(j)}$ which is simply the path metric of the survivor of length L passing through the state $s_t^{(j)}$ that connects a state at BL-0 with a state at BL-L. This survivor is called a composite path(CP). The CP at BL-t with the best composite SMG is called the best CP at BL-t, denoted BCP_t. If the BCP_t is a TB path, decoding stops; otherwise, find the best composite TB path at BL-t(if any), denoted BCTBP_t, and store it in the decoder memory. The iteration process continues until the BCP at a boundary location is found to be a TB path or a preset maximum number of iterations, I_{max}, is reached. For the latter case, the updated BCTBP in the memory is chosen as the decoded codeword if it exists; otherwise, the BCP stored in the memory is chosen as the decoded codeword.

IV. Performance and Complexity

Both WA-V and IBVD algorithms have been applied for decoding several convolutional and block codes(including the (24,12) Golay code). Simulation results show that both algorithms achieve virtually optimum error performance with a small number of iterations. The IBVD algorithm in all cases always converges to MLD performance in two iterations.

References

[1] G. Solomon and H. C. A van Tilborg, " A connection between block and convolutional codes", *SIAM J. Appl. Math.*, Vol. 37, No. 2, pp. 358-369, Oct. 1979.

[2] A. R. Calderbank, G. D. Forney Jr. and A. Vardy, "Minimal Tail-Biting Trellises: Golay Code and More," *IEEE Trans. Inform. Theory*, Vol.45, No.5, pp. 1435-1455. July 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

The Effect of the Tailbiting Restriction on Feedback Encoders

Per Ståhl[1]
Dept. Information Tech.
Lund University
P.O. Box 118
SE-221 00 LUND, Sweden
email: per.stahl@it.lth.se

John B. Anderson
Dept. Information Tech.
Lund University
P.O. Box 118
SE-221 00 LUND, Sweden
email: anderson@it.lth.se

Rolf Johannesson
Dept. Information Tech.
Lund University
P.O. Box 118
SE-221 00 LUND, Sweden
email: rolf@it.lth.se

Abstract — **It is shown that for short and moderate relative tailbiting lengths and high signal-to-noise ratios systematic feedback encoders have better bit error performance than nonsystematic feedforward encoders. Conditions for when tailbiting will fail are given and it is described how the encoder starting state can be obtained for feedback encoders in both controller and observer canonical form.**

I. Systematic versus Nonsystematic Tailbiting Encoders

Comparing the bit error performance between tailbiting codes encoded by systematic and nonsystematic encoders [1] shows that for a bad channel systematic encoders, feedforward or feedback, give the best performance. Simulations also show that the best encoders to use when the channel quality is unknown are the systematic feedback ones. In a good channel we show that the type of encoder having the best bit error performance depends on the relative tailbiting length, i.e., the tailbiting length/memory. For a good channel, ML-decoding, and a rate $R = b/c$ tailbiting code of length L an upper bound on the bit error probability can be expressed as $P_b \leq \frac{1}{L}\sum_{d=d_{min}}^{cL} b_d P_d$, where b_d is the sum of all bit errors for all codewords of weight d and P_d is the probability that a word of weight d is chosen instead of the allzero word. For a given length L and memory m the encoder giving the lowest bit error probability in a good channel is the one with as large minimum distance as possible and the smallest $b_{d_{min}}$ as possible. For rate $R = 1/2$ a search has been made for these encoders at various lengths and encoder memories. We can identify three regions where different encoder types give the best performance. For very short relative tailbiting lengths the best feedforward encoders are systematic and give the same bit error probability as the best systematic feedback encoders. For short and medium relative tailbiting lengths, systematic feedback encoders are typically a factor of 1.5-2 better than the feedforward ones. For long relative tailbiting lengths feedforward encoders give typically a factor of 2 better performance than the systematic feedback encoders. The explanation for this lies in the type of codeword which leads to the minimum distance. We show that this in turn depends on the relative tailbiting length.

II. Tailbiting failure

A rate $R = b/c$ feedback convolutional encoder of memory m can be viewed as consisting of b linear feedback shift registers (LFSRs), where the longest shift register has length m. For a given LFSR we define the *cycle characteristic* of the LFSR as the set of all possible cycles of its output. Consider first a rate $R = 1/c$ encoder. Assume that the LFSR has a cycle of length p. Then if we are in one of the states that belongs to this cycle and feed the encoder with only zeros at the input, corresponding to an allzero information sequence, the encoder returns to the same state after p steps. If the tailbiting length (number of trellis sections) L is a multiple of p, then we have more than one codeword corresponding to an all-zero input since the allzero codeword corresponds also to the allzero input. This means that for this L, we have no one-to-one mapping between the blocks of information bits and the codewords, and the tailbiting technique cannot work. Every polynomial has at least one cycle of length 1, the zero cycle corresponding to the allzero codeword, which is not a trouble maker, but for any multiple of any other cycle, the tailbiting technique fails. If we have a general rate $R = b/c$ encoder the tailbiting technique does not work for any multiple of the cycles in the cycle characteristic of any of the b LFSRs. See also [2][3][4].

III. Finding the Encoder Starting State

For polynomial convolutional encoders realized in controller canonical form the initial state of the encoder is simply given by the reciprocal of the last m input b-tuples, but for systematic feedback encoders the starting state depends on all of the information bits to be encoded. Several methods are presently known for finding the starting state in the controller canonical form. Certain algebraic equations may be set up and solved to obtain the starting state [2][4]. In some cases the number of delay elements can be reduced by realizing the encoder in observer canonical form. For example, the minimal realization of rate $R = 2/3$ and $R = 3/4$ systematic feedback encoders is the observer canonical form [5]. We give a method for finding the starting state for this form.

[1]This research was supported by the Foundation for Strategic Research - Personal Computing and Communication under Grant PCC-9706-09.

References

[1] J. B. Anderson, "Best Short Rate 1/2 Tailbiting Codes for the Bit Error Rate Criterion", *IEEE Trans. Communication*, vol. 48, Apr. 2000.

[2] P. Ståhl, J. B. Anderson and R. Johannesson, "Systematic Feedback Encoders for Short and Moderate-length Tailbiting Trellises". Submitted to *IEEE Trans. Information Theory*, 1998.

[3] R. Johannesson and J.B. Anderson, "A Condition for Feedback Tailbiting Convolutional Encoders and A Short List of Allowed Feedback Polynomials", *Proceedings of the 32nd Conf. on Information Sciences and Systems*, Princeton University, March 19, 1998.

[4] R. Ramesh, E. Wang and H. Koorapaty, "On Tail-Biting Recursive Systematic Convolutional Encoders". Submitted to *IEEE Trans. Communications*, 1998.

[5] R. Johannesson and K. Sh. Zigangirov, *Fundamentals of Convolutional Coding*, IEEE Press, New York, 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On Instantaneous Codes for Zero-Error Coding of Two Correlated Sources

Ying-On Yan and Toby Berger
School of Electrical Engineering
Cornell University
Ithaca, NY 14853 USA
Email: {yoyan,berger}@ee.cornell.edu

Abstract — **We study the problem of finding zero-error instantaneous codes for the Slepian-Wolf configuration [1]. By a zero-error instantaneous code we mean two encoder maps $f_1 : \mathcal{X} \to \{0,1\}^*$, $f_2 : \mathcal{Y} \to \{0,1\}^*$ and a decoding algorithm which, for any pair of encoder outputs $f_1(x_1)f_1(x_2)f_1(x_3)\ldots$ and $f_2(y_1)f_2(y_2)f_2(y_3)\ldots$, can correctly determine x_1 and y_1 by reading only the first length$(f_1(x_1))$ bits of the X encoder output and the first length$(f_2(y_1))$ bits of the Y encoder output. For $|\mathcal{X}| = 2$, we find a necessary and sufficient condition for the existence of a zero-error instantaneous code with a given set of codeword lengths for Y. Using this condition, we derive an upper bound to the minimum expected codeword length for Y and construct a simple example showing that the coding scheme proposed by Kh, Jabri and Al-Issa [2] is not optimal in general, and more surprisingly, the optimal code may violate the "Morse condition" that the more probable of two symbols never has the longer codeword. For $|\mathcal{X}| = 3$, we find a necessary but not sufficient condition for the existence of a zero-error instantaneous code with a given set of codeword lengths for Y. Moreover, for $|\mathcal{X}| \geq 3$, the existence of such a code is shown to be related to a rectangle packing problem.**

I. Introduction

The variable-length coding scheme proposed by Kh, Jabri and Al-Issa [2], henceforth called KJA coding, is summarized as follows. One of the sources, say X, is encoded by a Huffman code corresponding to the marginal p.m.f. $p(x)$, while for Y, a Huffman code is constructed for $\phi(Y)$ rather than Y, where $\phi : \{0,1,2,\ldots,|\mathcal{Y}|-1\} \to \{0,1,2,\ldots,S-1\}$ and $S \leq |\mathcal{Y}|$. S and ϕ are chosen in such a way that $\phi(y_1) \neq \phi(y_2)$ if $\exists x'$ s.t. $p(x',y_1) > 0$ and $p(x',y_2) > 0$, and the entropy of $\phi(Y)$ attains the minimum over all possible choices of ϕ.

KJA codes operate at rates $R_X \to H(X)$ and $R_Y < H(Y)$ and in general have lower rates than Witsenhausen's codes [3] because they use the nonzero $p(x,y)$ values explicitly, whereas Witsenhausen distinguished only those (x,y) with $p(x,y) = 0$ from those for which $p(x,y) > 0$. However, we notice that it is not necessary for the distinct codewords for Y to satisfy the prefix condition. Therefore, we propose an improved coding scheme as follows.

For X, a Huffman code is used as before. For Y, we abandon the mapping ϕ and encode by f_2 directly, where f_2 has the property that for each $x \in \mathcal{X}$ the set of codewords $\{f_2(y) : p(x,y) > 0\}$ satisfies the prefix condition; we call such a code an admissible f_2. Decoding is done in two steps. X is first decoded in the usual way for Huffman codes. Then the decoded value x will give us a set of codewords $\{f_2(y) : p(x,y) > 0\}$ which can be used to decode Y. The fact that $\{f_2(y) : p(x,y) > 0\}$ satisfies the prefix condition guarantees that as we read the encoder output of Y sequentially, the first match to one of the codewords in $\{f_2(y) : p(x,y) > 0\}$ corresponds to the true value of Y. Therefore, this modified scheme is a zero-error instantaneous code.

II. Main Results

Where $i \in \mathcal{X}$ and $j \in \mathcal{Y}$, let $A_i = \{y : p(i,y) > 0\}$ and $l_j = \text{length}(f_2(j))$.

Theorem 1: For $|\mathcal{X}| = 2$, if f_2 is admissible, then $\sum_{j\in A_i} 2^{-l_j} \leq 1$, for $i = 0,1$. Conversely, if $\{l'_j\}$ satisfies $\sum_{j\in A_i} 2^{-l'_j} \leq 1$, for $i = 0,1$, then there exists an admissible f_2 such that $l'_j = \text{length}(f_2(j))$ for all $j \in \mathcal{Y}$.

Non-optimality of KJA coding: For the joint p.m.f. $\{p(0,0) = 0.201,\ p(0,1) = 0.201,\ p(0,2) = 0.201,\ p(0,3) = 0.1,\ p(1,3) = 0.1,\ p(1,4) = 0.197\}$, the expected codeword length of Y for KJA coding is 2, while that for our code is 1.803.

Theorem 2: For $|\mathcal{X}| = 3$, if f_2 is admissible, then

$$\sum_{j\in A_i} 2^{-l_j} \leq 1 \qquad \text{for } i = 0,1,2 \tag{1}$$

and

$$\sum_{j\in (A_0\cap A_1)\cup(A_1\cap A_2)\cup(A_2\cap A_0)} 2^{-l_j} \leq 1 \tag{2}$$

Unlike the case for $|\mathcal{X}| = 2$, (1) is not a sufficient condition for the admissibility of f_2 when $|\mathcal{X}| = 3$. Furthermore, even with the additional constraint (2), we still do not have a sufficient condition. This can be verified by the following example.

If $|\mathcal{X}| = 3$, $|\mathcal{Y}| = 7$, $A_0 = \{0,2,4,6\}$, $A_1 = \{1,2,5,6\}$, $A_2 = \{3,4,5,6\}$, then (2) and (3) can be satisfied by choosing $\{l_j\}$ s.t. $l_0 = l_1 = l_3 = 2$, $l_2 = l_4 = l_5 = 3$ and $l_6 = 1$. Yet no codeword sets with these lengths can satisfy the admissibility requirement. We will show this by considering a rectangle packing problem.

References

[1] D. Slepian and J. K. Wolf, "Noiseless Coding of Correlated Information Sources," *IEEE Trans. Inform. Theory*, IT-19, No. 4, pp. 471–480, July 1973.

[2] A. Kh, A. Jabri and S. Al-Issa, "Zero-Error Codes for Correlated Information Sources," *Proceedings of the 6th IMA International Conference on Cryptography and Coding*, pp. 17–22, December 1997.

[3] H. S. Witsenhausen, "The Zero-Error Side Information Problem and Chromatic Numbers," *IEEE Trans. Inform. Theory*, IT-22, No. 5, pp. 592–593, September 1976.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Multi-Value Match Length Functions For Data Compression

S.M. Khosravifard ⊥ and M. Nasiri- Kenari *
⊥ Isfahan Univ. of Tech. , * Sharif Univ. of Tech. , IRAN
Email : P7730196 @ sepahan.iut.ac.ir , mnasiri @ sina.sharif.ac.ir

Abstract- In this paper, we propose a new match length function (MLF) called multi-value MLF (MVMLF) to be used with Lempel- Ziv type (LZI) data compression scheme. By restricting the function to five essential constraints, we obtain the most complete and compact dynamic dictionary which is efficiently updated. Based on MVMLF, we present two asymptotically optimal compression schemes.

Summary

With reference to Lempel- Ziv data compression algorithm (LZ1)[1], various modifications have been made to reduce the bits required to encode the match length and match position. In [2], Gavish and lempel describe match length function (MLF), and propose to use MLF to save on encoding the length of a match. As a modification of their approach, in this paper we introduce and employ multi-value MLF (MVMLF) to achieve some desired properties, such as to obtain the most complete and compact dynamic dictionary which is efficiently modified and updated according to the existance redundancy in the window.

The MLF as introduced in [2] associates just one unique nonnegative integer called match length value to each position of the current input data string in the window. MLF is defined as follows.

Let $X_0^{N-1} = x_0 x_1 x_2 ... x_{N-1}$ denote an input sequence of length N over a finite alphabet of size α and n, $0 < n << N$, be the size of the sliding window. Let also $l_i(k)$ denote the value of MLF for the k^{th} position of the window , when the window starts with x_i, the i^{th} symbol of the input string. To determine $l_i(k)$, we look for the largest integer l', $l' \le LMAX$, that satisfies $X_{i+k}^{i+k+l'-1} = X_{i+m}^{i+m+l_i(m)-2}$ $0 \le m < k$, and then we set $l_i(k)$= $\max\{l', LMIN\}$, where $LMIN$ and $LMAX$ indicate the minimum and maximum permissible values of MLF. All strings of the form $X_{i+k}^{i+k+l_i(k)-1}, 0 \le k < n$ are referred to as valid strings , and the set of all valid strings creates the dictionary.

The MVMLF that we propose in this paper may uniquely associate several match length values to some positions in the string , but does not associate any match length value to other positions. That is , numerous valid strings can be started from some positions (called valid positions) , whereas no valid string is started from other positions (called invalid positions). To save the required memory , and also to implement the recursive algorithm for MVMLF evaluation easily, we consider a special from of MVMLF in which the values associated to a valid position are successive. We define three functions $f_i(k), l_{\min_i}(k)$ and $l_{\max_i}(k)$, each associates a value to each position k, for $0 \le k < n$, where $f_i(k) = 0$ implies invalidity of position k and $f_i(k) = 1$ implies validity of all strings $X_k^{k+l-1}, l = l_{\min_i}(k), ..., l_{\max_i}(k)$ started from position k . Subscript i in these functions has the same meaning as in $l_i(k)$.

To have the most complete set of valid strings with minimum redundancy, in which lengthy strings can be included as easily as short ones , and also to update the MVMLF efficiently , we force MVMLF to satisfy the following constraints :

- All prefixes of a valid string are valid.
- Each string with the occurrence of at least two times in the window is a valid string.
- Validity of a string is preserved as long as the string remains in the window.
- A string can be valid in just one position in the window.
- A string appearing in several positions in the window must be valid in the rightest position of its occurrence.

Assume that the subsequence X_i^{i+n-1} is in the window and MVMLF has been evaluated for all position at the left side of k. To evaluate MVMLF at position k, we first set $f_i(k) = 1$, $l_{\min_i}(k) = l_{\max_i}(k) = LMIN$. We then do the following steps sequentially for $k' = k-1, k-2, ..., 2, 1, 0$.

1- Specify l, the length of match between positions k and k' as :

$$l = \min\left\{\max_{l'}\left\{l' ; X_{i+k}^{i+k+l'-1} = X_{i+k'}^{i+k'+l'-1}\right\}, LMAX\right\}$$

2- $$if \begin{cases} LMIN \le l \\ l_{\max_i}(k) \le l \\ l_{\max_i}(k') \le l \end{cases}, Set \begin{cases} f_i(k') = 0 \\ l_{\max_i}(k) = l \\ l_{\max_i}(k') = l \end{cases} \quad \text{or}$$

$$if \begin{cases} f_i(k') = 1 \\ l_{\min_i}(k') \le l \le l_{\max_i}(k') \\ l_{\max_i}(k) \le l \end{cases}, Set \begin{cases} l_{\max_i}(k) = l \\ l_{\min_i}(k') = l+1 \end{cases}$$

The MVMLF defined in this way satisfies all five constraints mentioned above. We propose two data compression schemes based on using MVMLF. We prove that under the conditions :

$$\lim_{n\to\infty} \frac{\log LMAX(n)}{\log n} = 0 \ , \ LMAX(n) > \frac{\log n}{H+\varepsilon} \ , \ and$$

$$LMIN \le \frac{\log n + \log LMAX + 1}{\lceil \log \alpha \rceil} < LMIN + 1$$

the proposed schemes are asymptotically optimal.

REFERENCES

[1] J. Ziv and A. Lempel, "A universal algorithm for sequential data compression," IEEE Trans. Inform. Theory, Vol. IT-23, no. 3, pp.337-343, May 1977.

[2] A. Gavish and A. Lempel,"Match-length function for data compression," IEEE Trans. Inform. Theory, Vol. IT-42, no. 5,pp. 1375-1380, Sept 1996.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Asymptotic Properties on the Codeword Length Distribution of Optimal FV Codes for General Sources

Hiroki Koga
Institute of Eng. Mech. and Sys.
University of Tsukuba
1-1-1 Tennoudai, Tsukuba-shi
Ibaraki 305-8573, Japan

Hirosuke Yamamoto
Graduate School of Engineering
University of Tokyo
7-3-1 Hongo, Bunkyo-ku
Tokyo 113-8656, Japan

Naoto Yamaguchi
Multimedia Systems Research Laboratory
Matsushita Electric Industrial Co., Ltd.
4-5-15, Higashi-Shinagawa, Shinagawa-ku
Tokyo 140-8632 Japan

Abstract — **This paper treats the codeword length of a fixed-to-variable length code (FV code) as a random variable and analyzes its asymptotic properties. It is shown that for a given general source [2] the codeword length can be viewed as the self information as $n \to \infty$ if a certain kind of optimal lossless FV code is used.**

I. Introduction

Consider an FV code that encodes a discrete random variable $X^n \in \mathcal{X}^n$ into K-ary codewords with $K \geq 2$. We define the FV code as a pair of an encoder φ_n and a decode ψ_n, where φ_n is a surjective mapping from $\mathcal{X}^n$ to a code $\mathcal{C}_n \subset \{0,1,\ldots,K-1\}^*$ and ψ_n a mapping from $\mathcal{C}_n$ to $\mathcal{X}^n$. Usually, performance of FV codes is measured by the average codeword length $E[l(\varphi_n(X^n))]$ under the requirement that the decoding error probability $\varepsilon_n = \Pr\{\psi_n(\varphi_n(X^n)) \neq X^n\}$ is equal to zero, where $E[\cdot]$ denotes the expectation with respect to the probability distribution P_{X^n} of X^n.

In this paper we investigate asymptotic properties of a random variable $l(\varphi_n(X^n))$ as $n \to \infty$ for the cases that $\varepsilon_n = 0$ for all $n \geq 1$ and $\limsup_{n\to\infty} \varepsilon_n \leq \varepsilon$ for an arbitrary $\varepsilon \in [0,1)$. In both cases $l(\varphi_n(X^n))$ turns out to be deeply related to another random variable $\log_K \frac{1}{P_{X^n}(X^n)}$ provided that FV codes satisfying a certain kind of optimality are used.

II. Lossless Case

Suppose that $\mathbf{X} = \{X^n\}_{n=1}^{\infty}$ is an infinite sequence of random variables (or the general source [2]) with a countably infinite alphabet $\mathcal{X}$. In order to unveil a relationship between the two random variables, we consider the following class of FV codes for $\mathbf{X}$ originally defined in [5].

Definition 1 *An infinite sequence of FV codes $\{(\varphi_n,\psi_n)\}_{n=1}^{\infty}$ is called* asymptotically mean-optimal *if it satisfies all of*

(L1) $\sum_{x^n\in\mathcal{X}^n} K^{-l(\varphi_n(x^n))} \leq 1$ *for all* $n \geq 1$,

(L2) $\limsup_{n\to\infty} \left\{\frac{1}{n}E[l(\varphi_n(X^n))] - \frac{1}{n}H(X^n)\right\} \leq 0$,

(L3) $\varepsilon_n = 0$ *for all* $n \geq 1$.

It is easy to check the Shannon-Fano-Elias code (e.g., [1]) is asymptotically mean-optimal if it is applied to X^n, $n \geq 1$. We have the following theorem on asymptotically mean-optimal FV codes that is comparable with Nemetz and Simmons [4] treating discrete memoryless sources with a finite alphabet.

Theorem 1 *If $\{\frac{1}{n}\log_K \frac{1}{P_{X^n}(X^n)}\}_{n=1}^{\infty}$ is uniformly integrable, i.e., it satisfies*

$$\lim_{u\to\infty} \sup_{n\geq 1} \frac{1}{n} \sum_{x^n:\frac{1}{n}\log_K \frac{1}{P_{X^n}(x^n)} \geq u} P_{X^n}(x^n)\log_K \frac{1}{P_{X^n}(x^n)} = 0$$

[3], then for any $\delta > 0$ all sequences of asymptotically mean-optimal FV codes $\{(\varphi_n,\psi_n)\}_{n=1}^{\infty}$ satisfy

$$\lim_{n\to\infty} \Pr\{X^n \in \mathcal{W}_n(\delta)\} = 0,$$

where $\mathcal{W}_n(\delta)$ is defined as

$$\mathcal{W}_n(\delta) = \left\{x^n \in \mathcal{X}^n : \left|\frac{1}{n}\log_K \frac{1}{P_{X^n}(x^n)} - \frac{1}{n}l(\varphi_n(x^n))\right| \geq \delta\right\}.$$

III. ε-error Case

Next, we consider infinite sequences of prefix-free FV codes satisfying $\limsup_{n\to\infty} \varepsilon_n \leq \varepsilon$ for an arbitrarily fixed $\varepsilon \in [0,1)$. In this setting we characterize an asymptotic behavior of codeword length of FV codes belonging to the following class.

Definition 2 *An infinite sequence of FV codes $\{(\varphi_n,\psi_n)\}_{n=1}^{\infty}$ is called* asymptotically mean-ε-optimal *if it satisfies all of*

(E1) $\sum_{y^*\in\mathcal{C}_n} K^{-l(y^*)} \leq 1$ *for all* $n \geq 1$,

(E2) $\lim_{\gamma\downarrow 0}\limsup_{n\to\infty} \left\{\frac{1}{n}E[l(\varphi_n(X^n))] - \frac{1}{n}G_{\varepsilon+\gamma}(X^n)\right\} \leq 0$,

(E3) $\limsup_{n\to\infty} \varepsilon_n \leq \varepsilon$,

where $G_\varepsilon(X^n)$ is defined as

$$G_\varepsilon(X^n) = \inf_{A_n:\Pr\{X^n\in A_n\}\geq 1-\varepsilon} \sum_{x^n\in A_n} P_{X^n}(x^n)\log_2 \frac{\Pr\{X^n \in A_n\}}{P_{X^n}(x^n)}.$$

The mean-ε-optimal FV code can be easily constructed in the manner similar to the construction of the weak variable length code [3, Sect. 1.8]. We have the following theorem on the class of asymptotically mean-ε-optimal codes.

Theorem 2 *For any $\delta > 0$ all sequences of asymptotically mean-ε-optimal FV codes $\{(\varphi_n,\psi_n)\}_{n=1}^{\infty}$ satisfy*

$$\lim_{n\to\infty} \Pr\{X^n \in \mathcal{D}_n \cap \mathcal{W}_n(\delta)\} = 0,$$

where $\mathcal{D}_n$ is defined as $\mathcal{D}_n = \{x^n \in \mathcal{X}^n : \psi_n(\varphi_n(x^n)) = x^n\}$.

References

[1] T. Cover and J. Thomas, *Elements of Information Theory*, Wiley, 1989.

[2] T. S. Han and S. Verdú, "Approximation theory of output statistics," *IEEE Trans. on Inform. Theory*, vol. IT-39, pp. 752–772, 1993.

[3] T. S. Han, *Information-Spectrum Methods in Information Theory*, Baifuukan-Press, 1998 (in Japanese).

[4] T. Nemetz and J. Simmon, "Self-information and optimal codes," *Topics in Information Theory*, pp. 457–468, 1977.

[5] K. Visweswariah, S. R. Kulkarni and S. Verdú, "Source codes as random number generators," *IEEE Trans. on Inform. Theory*, vol. IT-44, pp. 462 - 471, 1998.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Almost Surely Complete Parsing and Variable-to-Variable Length Coding

Mikihiko Nishiara and Hiroyoshi Morita
Graduate School of Information Systems
Univ. of Electro-Communications
Chofu, Tokyo 182-8585, Japan
Email: mikihiko@math-sys.is.uec.ac.jp, morita@is.uec.ac.jp

Abstract — **We introduce the idea of proper and almost surely complete parsing. This parsing can uniquely segment the source output with probability one, and strengthens the coding converse theorem. Some kinds of non-proper parsing are involved in the proper and almost surely complete parsing.**

I. Introduction

So far, a variable-to-variable (VV) length encoder has been considered as a variable-to-fixed (VF) length encoder followed by a fixed-to-variable (FV) length encoder [1]. Let us call this type of VV length encoders as VF-FV length encoders. The VF length encoder has a parser as a preprocessor, which segments the source output into a concatenation of variable-length strings, each of which belongs to a dictionary. The dictionary is supposed to be *proper*, i.e., no string in the dictionary is a prefix of another string in the dictionary. Moreover, the dictionary is supposed to be *complete*, i.e., every infinite sequence has a prefix in the dictionary. Generally, a prefix and complete dictionary has exactly one prefix for every infinite sequence.

We consider an i.i.d. source with a countable alphabet $\mathcal{X}$ with distribution P. If the dictionary of the parser is proper and complete, then the lengths of its entries are uniformly bounded. However, it is not necessary to bound the lengths of the entries for a VV length encoder.

II. Almost Surely Completeness

Definition 1 A dictionary, which is a set of finite length sequences over $\mathcal{X}$, is said to be *almost surely complete* (a.s.c.) if the probability that the dictionary has a prefix of the sufficiently long source output is one.

For a proper and a.s.c. dictionary, the lengths of its entries are not generally uniformly bounded and the dictionary has exactly one prefix of a sufficiently long source output as its entry with probability one. The "weakly unique parsableness" for VF length coding defined in [2] is equivalent to this property. Note that being complete means being a.s.c. An example for a proper, a.s.c. and non-complete dictionary over $\{0,1\}$ is $\{0, 10, 110, 1110, \cdots\}$, which has no prefix of $111\cdots$.

With an a.s.c. dictionary, we reinterpret a VV length encoder. A VV length encoder consists of a parser and a prefix encoder φ. The parser have a proper and a.s.c. dictionary ψ. The prefix encoder φ emits a codeword $\varphi(x)$ for each string x in ψ. Let (ψ, φ) denote a VV length encoder. Note that the VV length encoder can no longer be decomposed into a VF length encoder and an FV length encoder. We now must abandon that every infinite sequence out of the source can be encoded. But they can be still encoded with probability one.

Theorem 1 (Coding Theorem) We define the coding rate of a VV length encoder (ψ, φ) as $\mathrm{E}|\varphi|/\mathrm{E}|\psi| = (\sum_{x\in\psi} P(x)|\varphi(x)|) \,/\, (\sum_{x\in\psi} P(x)|x|)$, where $|x|$ denotes the length of a string x. Let C denote the collection of VV length encoders with a proper and a.s.c. dictionary. We have

$$\inf_{(\psi,\varphi)\in C} \mathrm{E}|\varphi|/\mathrm{E}|\psi| = H(P),$$

where $H(P) = -\sum_{a\in\mathcal{X}} P(a)\log P(a)$ and the base of the logarithm is equal to the size of the code alphabet.

The theorem consists of the direct part and the converse part. The direct part can be replaced by that of the FV length coding because an FV length encoder is also a VV length encoder. The converse part can be demonstrated similarly to the VF-FV length coding theorem by means of

Lemma 1 For an i.i.d. source over a countable alphabet $\mathcal{X}$ with distribution P, if ψ is proper and a.s.c., then $-\sum_{x\in\psi} P(x)\log P(x) = \mathrm{E}|\psi| H(P)$.

The proof for a finite alphabet can be found in [3].

III. The Longest Matching

The properness and almost surely completeness together guarantee that the source output is uniquely segmented with probability one. However, the properness is not a necessary condition. We allow the dictionary not to be proper, and let the parser cut the source output at the tail of the longest match among the dictionary. Then, the necessary and sufficient condition for uniquely parsing is the following.

Definition 2 We say that a dictionary ψ is *longest matchable* if in ψ, there exists the longest prefix of a sufficiently long source output with probability one.

A longest matchable dictionary is a.s.c. but may be non-proper. A simple example of such a dictionary is $\{0, 00, 10, 110, 1110, \cdots\}$, which is obviously non-proper.

For a longest matchable dictionary, we will try to obtain an equivalent, proper and a.s.c. dictionary. Let (ψ_0, φ_0) be a VV length encoder with a longest matchable dictionary. For $n = 1, 2, \cdots$, we recursively define ψ_n as follows. Let M_{n-1} be the collection of entries of ψ_{n-1} each of that is a prefix of another entry in ψ_{n-1}. Define

$$\psi_n = (\psi_{n-1} \setminus M_{n-1}) \cup \{y \in M_{n-1}\psi_0 \mid \text{there is no prefix of } y \text{ in } \psi_{n-1} \setminus M_{n-1}\},$$

where $M_{n-1}\psi_0$ is the collection of concatenations of two strings from M_{n-1} and ψ_0, respectively. If ψ_0 is proper, then $\psi_n = \psi_0$ for all n. For $\{\psi_n\}$, we now let

$$\psi_\infty = \liminf_{n\to\infty} \psi_n.$$

It is shown that ψ_∞ is proper. But unfortunately, it may be empty.

Theorem 2 Let (ψ_0, φ_0) be a VV length encoder with longest matchable parsing. If ψ_∞ is a.s.c., then with some φ_∞, the VV length encoder $(\psi_\infty, \varphi_\infty)$ emits the same codewords as (ψ_0, φ_0) with probability one.

Corollary 1 If (ψ_0, φ_0) is a VV length encoder with longest matchable parsing and ψ_∞ is a.s.c., then (ψ_0, φ_0) obeys the VV length coding theorem with proper and a.s.c. parsing.

References

[1] J.Abrahams, "Code and parse tree for lossless source encoding," *Proc. of Sequences 97*, pp.145–171, Positano, Italy, 1997

[2] S.A.Savari, "Variable-to-fixed length codes and the conservation of entropy," *IEEE Trans. Inform. Theory*, val.45, pp.1612–1620, 1999

[3] L.Ekroot, T.M.Cover, "The entropy of randomly stopped sequence," *IEEE Trans. Inform. Theory*, vol.37, pp.1641–1644, 1991

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Signaling for the Gaussian Channel with Side Information at the Transmitter

Frans M.J. Willems
Eindhoven Univ. of Technology,
Electrical Engineering Department,
Eindhoven, The Netherlands.
e-mail: f.m.j.willems@tue.nl

Abstract — **We investigate the Gaussian side information channel in the Shannon [1] setup and propose a method that achieves correlation between the signal and the side information noise. The capacity still remains to be determined however.**

I. Introduction

Shannon [1] investigated the communication system in which the state s_k of the channel $P_{\rm ch}(y|x,s)$ during transmission $k = 1, 2, \cdots, K$ is selected according to the distribution $P_{\rm st}(s)$. Both the channel and the state selector are assumed to be memoryless. The encoder sends the message $m \in \{1, 2, \cdots, \exp(KR)\}$ to the decoder. When x_k is to be produced, the encoder may use its knowledge of the state s_k, which is made available to him just before transmission k is about to begin, and all previous states $s_1, s_2, \cdots, s_{k-1}$. Hence $X_k = F(M, S_1, S_2, \cdots, S_{k-1}, S_k)$ for some encoding function $F(\cdot)$. When the channel input alphabet $\mathcal{X}$ and state alphabet $\mathcal{S}$ are discrete, the capacity is known (see [1]). This is not the case for the Gaussian side information channel however. Here the channel output $Y = X + S + Z$, where S and Z are independent Gaussian random variables with mean 0 and variances Q and N respectively. The codewords $X_1^K = (X_1, X_2, \cdots, X_K)$ must satisfy the power constraint $\sum_{k=1,K} X_k^2 \leq KP$. The objective here is to find the capacity of this Gaussian channel.

An upper and lower bound for the capacity C in nats per transmission are

$$\frac{1}{2}\ln\left(\frac{P+Q+N}{Q+N}\right) \leq C \leq \frac{1}{2}\ln\left(\frac{P+N}{N}\right). \qquad (1)$$

In [3] noise cancelation and noise concentration was studied.

II. Correlating signal and noise

Here we transpose the Costa method [2] by trying to realize correlation on the symbol level. In transmission k we transmit a signal u_k from the set

$$\mathcal{B} \triangleq \{\cdots, -\frac{5B}{2}, -\frac{3B}{2}, -\frac{B}{2}, +\frac{B}{2}, +\frac{3B}{2}, +\frac{5B}{2}, \cdots\},$$

for some well chosen B. Assume that during transmission k the message $j \in \{1, 2, \cdots, J\}$ must be transmitted. This message corresponds to a subset $\mathcal{B}_j$ of $\mathcal{B}$. E.g. for $J = 2$ we could get the subsets

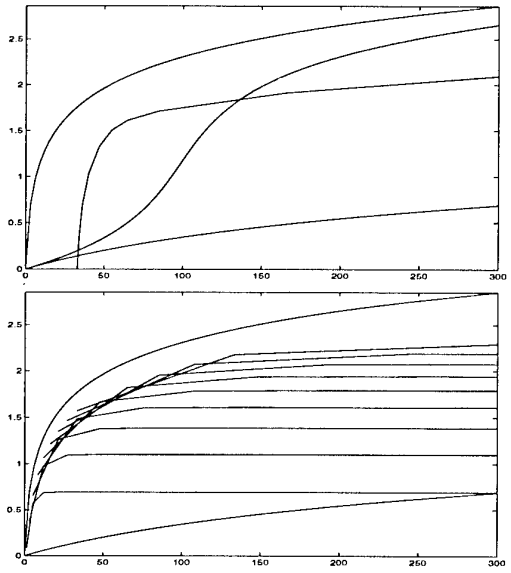
$$\mathcal{B}_1 = \{\cdots, -\frac{3B}{2}, +\frac{B}{2}, +\frac{5B}{2}, \cdots\},$$
$$\mathcal{B}_2 = \{\cdots, -\frac{5B}{2}, -\frac{B}{2}, +\frac{3B}{2}, \cdots\},$$

and for $j = 1$ we choose a signal $u_k \in \mathcal{B}_1$ and for $j = 2$ we choose a signal u_k from $\mathcal{B}_2$. What we mean by this is that the transmitter chooses the input x_k such that $u_k = x_k + s_k \in \mathcal{B}_j$ and x_k^2 is minimal, when message j is to be transmitted. The channel output $y_k = x_k + s_k + z_k = u_k + z_k$ is the signal u_k to which Gaussian noise with variance N is added. It will be clear that for $B^2 \gg N$ we obtain a rate R close to $\ln(J)$ bits per transmission. On the other hand the power P that is needed to concentrate the signal on $\mathcal{B}_j$ is roughly $(JB)^2/12$. Hence $J \approx \sqrt{12P/B^2}$. If we take $B^2 = 12N$ then $J \approx \sqrt{P/N}$ and we achieve a rate R close to $(1/2)\ln(P/N)$, which is independent of Q and more or less what we want for $P \approx J^2 N \gg N$ hence for J not too small.

Note that this method realizes that the transmitted symbol $u_k = x_k + s_k$ is correlated with the state s_k.

III. Numerical evaluation

For $Q = 100$, $N = 1$ for $0 \leq P \leq 300$ we have computed the lower and upper bound according to (1) and the rates achieved by the cancellation and concentration techniques from [3]. In the concentration case $A = 20$ was chosen. The curves are shown in the first figure.



Moreover for $J = 2, 3, \cdots, 10$ and $B = 2, 4, 6, \cdots$ we have determined the channel with input U taking values from the alphabet $\{1, 2, \cdots, J\}$ and output Y. The mutual information $I(U;Y)$ of this channel is computed assuming that U is uniformly distributed over $\{1, 2, \cdots, J\}$. Also the average concentration power is determined. This leads for each value of J to a curve representing the power-rate pairs for several values of B. These curves are in the second figure.

References

[1] C.E. Shannon, "Channels with side information at the transmitter," *IBM J. Res. Develop.*, vol. 2, pp. 289-293, Oct. 1958.

[2] M.H.M. Costa, "Writing on dirty paper," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 439-441, May 1983.

[3] F.M.J. Willems, "On Gaussian channels with side information at the transmitter." *Proc. 9th Symp. Inform. Theory in the Benelux*, Mierlo, The Netherlands, pp. 129-135, May 1988.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Capacities of Time-Varying Multiple-Access Channels with Side Information

Arnab Das
Bell Laboratories
Lucent Technologies
Holmdel, NJ 07733
e-mail: arnab@lucent.com

Prakash Narayan
Dept of Electrical & Computer Engg. and
Institute for Systems Research
University of Maryland
College Park, MD 20742
e-mail: prakash@eng.umd.edu

Abstract —

We determine the capacity regions for a class of *time-varying multiple-access channels* (TVMACs), when the underlying channel state evolves in time according to a probability law which is known to the transmitters and the receiver. Additionally, the transmitters and the receiver have access to varying degrees of channel state information (CSI) concerning the condition of the channel. Discrete-time channels with finite input, output and state alphabets are considered first. Next, in order to reduce transmitter complexity, we restrict the encoders at each time instant to depend only on a limited extent of CSI. As a special case, we consider a memoryless TVMAC, with the channel state process being a time-invariant, indecomposable, aperiodic Markov chain. We then study a *time-varying (multiple-access) fading channel* (TVFC) with additive Gaussian noise, when various amounts of CSI are provided to the transmitters while *perfect* CSI is available to the receiver, and the fades are assumed to be stationary and ergodic.

I. Preliminaries

Consider first a discrete-time two-sender TVMAC with (finite) input alphabets $\mathcal{X}_1, \mathcal{X}_2$, (finite) output alphabet $\mathcal{Y}$ and (finite) "state space" $\mathcal{S}$. The probability law of the channel is characterized by a sequence of (known) transition pmf's

$$\mathbf{W} = \{W(y^n|x_1^n, x_2^n, s^n) : x_1^n \in \mathcal{X}_1^n,\ x_2^n \in \mathcal{X}_2^n,\ s^n \in \mathcal{S}^n,\ y^n \in \mathcal{Y}^n\}_{n=1}^{\infty}, \quad \text{(I.1)}$$

and a (known) probability law P_S governing the $\mathcal{S}$-valued state process $\{S_t\}_{t=1}^{\infty}$ which allows the state at any time to depend on the previous states but not on the previous channel inputs or outputs.

Let $\mathcal{E}_1, \mathcal{E}_2$ and $\mathcal{D}$ be finite sets and $h_1 : \mathcal{S} \to \mathcal{E}_1$, $h_2 : \mathcal{S} \to \mathcal{E}_2$, and $g : \mathcal{S} \to \mathcal{D}$ be mappings which are used to describe the CSI available to the two senders and the decoder, respectively. Thus, at each time instant t, the encoder for sender-1 (resp. sender-2) is provided with the *instantaneous* CSI $e_{1,t} = h_1(s_t)$ (resp. $e_{2,t} = h_2(s_t)$) while the decoder is provided with CSI $d_t = g(s_t)$, all in a causal manner. The capacity region of the TVMAC in (I.1) for the average probability of error criterion will be denoted by $\mathbf{C}$.

In order to reduce encoder complexity, we shall often consider situations in which we restrict the encoder for sender-j, $j = 1, 2$, to depend only on the *limited* CSI $(e_{j,\max\{1,t-k+1\}}, \ldots, e_{j,t})$ at time t, for some fixed integer $k \geq 1$. The capacity region corresponding to this "encoder restriction of window-k" is denoted by $\mathbf{C}(k)$.

We shall also consider the *multiple-access time-varying fading channel* (TVFC) model, in which the received $\mathbb{R}$-valued signal is given by

$$Y_t = \sum_{j=1}^{2} \tilde{S}_{j,t} x_{j,t} + N_t, \quad t \geq 1, \quad \text{(I.2)}$$

where $\{x_{j,t}\}_{t=1}^{\infty}$ and $\{\tilde{S}_{j,t}\}_{t=1}^{\infty}$ are the $\mathbb{R}$-valued transmitted signal and $\mathbb{R}^+$-valued fade of sender-j, $j = 1, 2$, respectively, and $\{N_t\}_{t=1}^{\infty}$ is i.i.d. Gaussian noise with mean zero and variance σ_N^2. The fading processes $\{\tilde{S}_{j,t}\}_{t=1}^{\infty}$, $j = 1, 2$, are assumed to be jointly stationary and ergodic, though not necessarily independent of each other; they are independent of $\{N_t\}_{t=1}^{\infty}$. The state of the channel at time t, $t \geq 1$, is $S_t \triangleq (\tilde{S}_{1,t}, \tilde{S}_{2,t}) \in \mathcal{S} = \mathbb{R}^2$. The CSI available to sender-j is given by a mapping $h_j : (\mathbb{R}^+)^2 \to \mathcal{E}_j$, where $\mathcal{E}_j$ can be an arbitrary subset of $\mathbb{R}$ which is not necessarily finite. *The decoder is assumed to possess perfect CSI*, i.e., $d_t = s_t, t \geq 1$. Sender-j, $j = 1, 2$, is assumed to be subject to an input (average) power constraint $\mathcal{P}_j$.

II. Results

Our results include a determination of the following capacity regions with CSI at the encoders and decoder. Some of them constitute generalizations to the multiple-access situation of results for single-sender time-varying channels in [Caire-Shamai, IT Sept.1999].

- The capacity region $\mathbf{C}$ of the TVMAC in (I.1) (this follows as a straightforward consequence of the approach in [Han, IT Nov. 1998]), including in the special case when the CSI available to the encoders is contained in that available to the decoder.
- The capacity region $\mathbf{C}$ of the TVMAC in (I.1) when the channel is memoryless and when the state process $\{S_t\}_{t=1}^{\infty}$ is a time invariant, indecomposable, aperiodic Markov chain (TIAMC), under suitable sufficient conditions for the invariance of $\mathbf{C}$ with respect to the distribution of S_1.
- The capacity region $\mathbf{C}(k)$ under an encoder restriction of window-k, when the TVMAC and the state process are as in the previous situation; also, the capacity region $\mathbf{C}$ when the distribution of S_1 is the stationary distribution of the TIAMC.
- The capacity regions $\mathbf{C}(k)$ and $\mathbf{C}$, when the TVMAC in (I.1) is memoryless and the state process $\{S_t\}_{t=1}^{\infty}$ is stationary and ergodic.
- The capacity regions $\mathbf{C}(k)$ and $\mathbf{C}$ of the TVFC in (I.2), as also implications when the fades are Raleigh and varying degrees of CSI are provided to the transmitters.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Fourier and the White Gaussian Multiple-Access Channel with Feedback

Gerhard Kramer[1]
Bell Laboratories, Lucent Technologies
600 Mountain Ave, Murray Hill NJ 07974, U.S.A.
e-mail: gkr@research.bell-labs.com

Abstract — **Feedback strategies are presented for the K-user white Gaussian multiple-access channel. The strategies are based on the discrete Fourier transform of length K and achieve the sum-rate capacity for equal user powers if the signal-to-noise ratio is large enough.**

I. Introduction and Model

The capacity region of the 2-user white Gaussian multiple-access channel with feedback (MAC-FB) was determined in [1]. However, it seemed difficult to generalize this result to more than 2 users. We show that one can partially circumvent the difficulties by considering a complex noise model and by using the discrete Fourier transform.

The K user complex white Gaussian MAC-FB is a $K+1$ terminal channel with K inputs $X_1, X_2, \ldots, X_K$ and one output $Y = \left(\sum_{k=1}^{K} X_k\right) + Z$, where Z is a circularly symmetric complex Gaussian random variable with variance $\sigma^2 = \mathrm{E}[|Z|^2]$. Terminal k transmits a B_k bit message to the receiving terminal in N channel uses, so that its rate is $R_k = B_k/N$ bits per use, $k = 1, \ldots, K$. At time n the transmitting terminals use the past $n-1$ channel outputs Y^{n-1} to encode their messages. The power constraints on the transmissions are $\sum_{n=1}^{N} \mathrm{E}[|X_{kn}|^2]/N \leq P_k$ for some constants P_k, $k = 1, \ldots, K$.

II. Transmission and Reception

Terminal k transmits by mapping its message onto a point θ_k in the complex plane and by correcting the receiver's estimate of this point. More precisely,

$$X_k = \sqrt{P_k \Big/ \sigma^2_{k(n-1)}} \cdot \epsilon_{k(n-1)} \cdot m^*_{kn}, \tag{1}$$

where $\sigma^2_{k(n-1)} = \mathrm{E}[|\epsilon_{k(n-1)}|^2]$ is the variance of the receiver's error $\epsilon_{k(n-1)} = \hat{\theta}_{k(n-1)} - \theta_k$ after $n-1$ channel uses and m_{kn} is a *modulation coefficient*. We call this transmission technique *modulated estimate correction* (MEC) [2]. We will choose the m_{kn} to be entries from the length K discrete Fourier transform matrix, i.e., $m_{kn} = e^{j2\pi(k-1)(n-1)/K}$.

We let the receiving terminal estimate the θ_k by using a linear minimum-mean square error (LMMSE) estimator. The result is the K recursions

$$\sigma^2_{kn} = \sigma^2_{k(n-1)} \cdot V_{Y_n|X_{kn}} \Big/ V_{Y_n}, \tag{2}$$

where V_{Y_n} is the variance of Y_n and $V_{Y_n|X_{kn}}$ is the variance of Y_n given X_{kn}. Consider also the correlation coefficients

$$\rho_{k\ell n} = \mathrm{E}[\epsilon_{kn}\epsilon^*_{\ell n}] \Big/ \sqrt{\sigma^2_{kn}\sigma^2_{\ell n}} \tag{3}$$

[1]This work was performed while the author was with Endora Tech AG, Hirschgässlein 40, 4051 Basel, Switzerland.

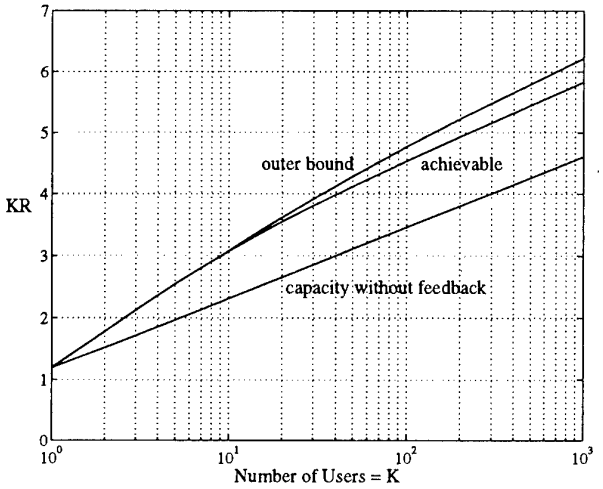


Fig. 1: Sum-rate achievable with $P = 10$ and $\sigma^2 = 1$. The rate units are nats/use/dimension.

and let $\bar{Q}_{\underline{\epsilon}_n}$ be the $K \times K$ matrix with $\rho_{k\ell n}$ in the (k,ℓ)th position. One finds that

$$\bar{Q}_{\underline{\epsilon}_n} = \odot \frac{\bar{Q}_{\underline{\epsilon}_{n-1}} V_{Y_n} - \underline{c}_n \underline{c}_n^H}{\sqrt{\underline{V}_{Y_n|X_n^K} \underline{V}^T_{Y_n|X_n^K}}}, \tag{4}$$

where $\underline{c}_n$ is the column vector of the

$$c_{kn} = \mathrm{E}[\epsilon_{k(n-1)} Y_n^*] \Big/ \sqrt{\sigma^2_{k(n-1)}}, \tag{5}$$

$\underline{V}_{Y_n|X_n^K}$ is the column vector of the $V_{Y_n|X_{kn}}$, the "$\odot$" in front of the fraction denotes *term-by-term division* (a "Hadamard quotient"), and the square-root in the denominator denotes taking *term-by-term* square roots. The recursion (4) yields good rates for a wide variety of power constraints and rates. Moreover, if $P_k = P$ for all k the analysis can be simplified to an eigenvalue recursion. Numerical results are depicted in Fig. 1 for $P = 10$ and $\sigma^2 = 1$, where the sum-rate capacity is achieved for $K \leq 8$. It can be shown that, in general, MEC combined with LMMSE estimation achieves the sum-rate capacity for equal user powers if the signal-to-noise ratio is beyond some finite number that depends on K only.

References

[1] L.H. Ozarow, "The capacity of the white Gaussian multiple access channel with feedback," *IEEE Trans. Inform. Theory*, vol. 30, no. 4, pp. 623–629, July 1984.

[2] G. Kramer, "Modulated estimate correction for the white Gaussian broadcast channel with feedback," *Proceedings of the 2000 Conf. on Inform. Sci. and Sys.*, Princeton University, NJ USA, March 15 – 17 2000, pp. TA4-17 – TA4-20.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Geometric Proof of Rate-Distortion Function of Gaussian Sources with Side Information at the Decoder

S. Sandeep Pradhan and Kannan Ramchandran [1]
Department of EECS, University of California, Berkeley, CA-94720,USA
pradhan5,kannanr@eecs.berkeley.edu

Abstract — **The achievability of the Wyner-Ziv theorem [1] for the Gaussian case is shown using only geometric arguments. The motivation for this is to inspire the construction of practical codes based on this [2].**

I. Introduction

Distributed source coding deals with the encoding of correlated sources that do not communicate with one another. The concept of distributed source coding has been considered for continuous sources with a fidelity criterion in [1] where X and Y are sources such that the decoder has (lossless) access to Y, and the encoder compresses X using the fact that the decoder knows Y. It was shown that when X and Y are jointly Gaussian with mean squared error as the fidelity criterion, it is possible to compress X as efficiently as the case when both the encoder and the decoder have access to Y i.e. $R_{x|y}(D) = R^*(D)$ [1]. In [2], a construction of generalized coset codes has been proposed based on the channel coding principles. Using geometrical arguments we establish the achievability of the following rate distortion bound with side information for X:

$$R = \frac{1}{2}\log\left(\frac{\sigma_n^2}{(1+\sigma_n^2)d^*}\right), \qquad (1)$$

where X is *i.i.d.* Gaussian with zero mean and unit variance, d^* is the reconstruction fidelity, and the side information is given by $Y = X + N$, where N is *i.i.d.* Gaussian with zero mean and with variance σ_n^2 and independent of X

II. Geometric Derivation of Wyner-Ziv bound

We encode the source X in blocks of length L. Randomly distribute 2^{LR_1} codewords independently and uniformly on the surface of an L-dimensional sphere $\mathcal{S}_L\left(\sqrt{1-\theta^2}\right)$ of radius $\sqrt{1-\theta^2}$ where R_1 is a real number which depends on θ ($\theta = \sqrt{\frac{d^*\sigma_n^2}{\sigma_n^2 - d^*}}$). Let $\mathcal{C}$ denotes this set of codewords. Randomly choose 2^{LR_2} codewords independently and uniformly from this set $\mathcal{C}$, and give an index to this subset called a coset. Keep repeating this until all the codewords are exhausted. Thus, there are $2^{L(R_1-R_2)} = 2^{LR}$ indices.

Encoding involves finding a codeword from the space of codewords satisfying a distance criterion (within distance θ) and sending the index of the coset containing the encoded codeword to the decoder. If none of the codewords satisfies the criterion, then an error is declared. We derive a lower bound on R_1. The basic idea behind the proof is the following: encoder chooses a codeword to represent X, and nature chooses the side information Y independent of the encoder using a "channel" $p(y|x)$ on X. Yet there exists a strong correlation between the quantized codeword and the side information, which needs to be exploited. This key result (also known as the Markov Lemma [1]) used in the geometric arguments is given by the following theorem.

Theorem: For any $\epsilon > 0$ (sufficiently close to 0), $\exists\ L_1(\epsilon)$ such that for any $L > L_1(\epsilon)$, $P\left[\left|\|\tilde{\mathbf{Y}}\|^2 - \theta^2 - \sigma_n^2\right| > \epsilon\right] < \epsilon$, where $\tilde{\mathbf{Y}} = \mathbf{Y} - \mathbf{W}$, $\mathbf{Y}, \mathbf{W}$ are side information and quantized codeword vectors respectively.

The first part of the decoder involves finding a "suitable" codeword in the given coset. If either more than one or none of the codewords satisfies the distance criterion, then an error is declared. We derive an upper bound on R_2. The second part of the decoder then gets the reconstruction vector as a function of the encoded codeword and the side information vector. It is shown geometrically that the probabilities of the error events can be made arbitrarily small for large L. The geometry for the ideal case of very large L is shown in Fig. 1.

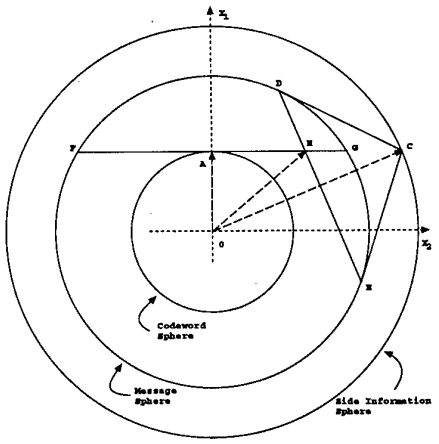


Figure 1: OA, OC and OH represent the codeword and observed side information and the reconstruction vectors respectively. A, H and C are collinear. OH gives the minimum distortion given that OA and OC are codeword and the side information respectively. FG and DE represent two spheres.

References

[1] A. D. Wyner, "The rate-distortion function for source coding with side information at the decoder-II: General sources," *Inform. Contr.*, vol. 38, pp. 60–80, 1978.

[2] S. S. Pradhan and K. Ramchandran, "Group-theoretic construction and analysis of generalized coset codes for symmetric/asymmetric distributed source coding," *Proc. Conf. on Info. Sci. and Sys. (CISS)*, Princeton, March 2000.

[1] This work was supported by in part by DARPA Grant F29601-99-1-0169 and NSF (CAREER) Grant MIP 97-03181.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

A Comparison of two schemes for generating DC-free RLL Sequences

Kees A. Schouhamer Immink
Institute for Experimental
Mathematics, Ellernstrasse 29,
45326 Essen, Germany.
immink@exp-math.uni-essen.de

Wang Yong Hong Wilson
Data Storage Institute, 5
Engineering Drive 1, Singapore
117608, dsiyhw@dsi.nus.edu.sg

Abstract — **We will discuss the generation of dc-free runlength-limited (DCRLL) sequences. We propose to employ standard RLL codes, where dc-control is effectuated by multiplexing the source data or the encoded data with dc-control bits. The dc-control bits offer the degree of freedom required to shape to spectrum. It will be shown that a new technique, called *parity preserving assignment,* will offer great benefits over other constructions.**

I. Introduction

The design of dc-free runlength-limited (DCRLL) codes can, at least in principle, be systematically accomplished by the many design techniques published [1]. Unfortunately, the design of a DCRLL code with a rate close to the Shannon capacity of the constrained channel, is severely hampered by the large number of states of the finite-state machine which models the channel constraints at hand. The large number of states of the underlying FSM, can, at least in principle, be handled by buying a larger computer, but the insight required is too easily lost. Essentially, there are two systematic design approaches that emerged in the literature.

The first method uses a standard method, such as the ACH algorithm to design an RLL code. In the final stage of the ACH algorithm we end up with a graph with the property that from any state of the graph there are at least 2^m (m is assumed to be the source word length) outgoing edges. These *surplus edges* are used as alternative codewords that can be used for dc-control. The rate 8/16, (2,10) EFMPlus code is an example of a DCRLL code used in practice (DVD) that was designed according to these guidelines [1].

In the second method, a given, state-of-the-art, RLL code, is used to generate RLL sequences. The sequences generated under the coding rules of said code are multiplexed with dc-control bits for minimizing the low-frequency components. The user data or alternatively the encoded data are partitioned into segments of ν bits. Between two consecutive ν-bit segments β dc-control bits are inserted, and the β dc-control bits, in turn, are chosen to minimize the low-frequency components.

II. Codes with parity preserving word assignment

In order to make it possible to efficiently control the dc-content in the source date level mode, we have made the assignment between source words and codewords in such a way that the *parity* of both source word and its assigned codeword are the same. The parity, P, of an n-bit word $(x_1, \ldots, x_n)$, $x_i \in \{0, 1\}$, (either source or codewords) is defined by

$$P = \sum_{i=1}^{n} x_i \bmod 2.$$

In other words, if the source word has an even (or odd) number of 'one's then its channel representation also has an even (or odd) number of 'one's. A code with a *parity preserving* assignment has the virtue that when it is used in conjunction with dc-control bits at data level that setting an even (or odd) number of 'one's at data level will result in an even (or odd) number of 'one's at code level. This leads, as we will demonstrate, to an efficient dc-control.

Table 1: Variable-length synchronous rate 2/3, $(1, \infty)$ code with parity preserving assignment.

Data		*Code*
00	$\leftarrow \rightarrow$	000
01	$\leftarrow \rightarrow$	010
10	$\leftarrow \rightarrow$	100
1100	$\leftarrow \rightarrow$	001010
1101	$\leftarrow \rightarrow$	001000
1110	$\leftarrow \rightarrow$	101010
1111	$\leftarrow \rightarrow$	101000

The variable length rate 2/3, $(1, \infty)$ code shown in Table 1, is an example of a code with the parity preserving property. It can easily be verified that indeed the assignment is parity preserving. In the presentation, we will show the difference in performance between various DCRLL codes.

References

[1] K.A.S. Immink, *Codes for Mass Data Storage Systems,* Shannon Foundation Publishers, Eindhoven, The Netherlands, 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Design of Binary Sequences with Optimal Frame Synchronization Property

Young Joon Song
Advanced Telecomm. Research Lab., LG Information & Communications, Ltd.,
LG R&D Complex, 533, Hogye-dong, Dongan-gu, Anyang-shi, Kyongki-do, 431-080, Korea

Abstract: Based on the ideal autocorrelation property of sequences with odd length n, a general method to generate binary sequences of length $N=2n$ with optimal frame synchronization property is studied. The sequence generation method may be useful in the field of communication systems.

I. Introduction

The importance of sequences with optimal frame synchronization property is increasing since by employing two thresholds at the output of correlator of such sequences, we can double-check frame synchronization and thus improve the frame synchronization performance [1]. If the autocorrelation function of a sequence has double maximum values equal in magnitude and opposite polarity at zero and middle shifts, and further if the function has the lowest out-of-phase values except for at middle shift, then such a sequence is said to have "optimal frame synchronization property". A sequence is said to have "ideal autocorrelation property" if the out-of-phase autocorrelation value of the sequence is all "-1" or "1". Based on sequences with ideal autocorrelation function, a general method to generate the optimal frame synchronization sequences of length $N=2n$ is proposed. Since all the binary maximal length sequences of period $n=2^r-1$ have the out-of-phase autocorrelation value "-1", we can easily construct the desired optimal frame synchronization sequences by using the proposed method.

II. Definitions and basic properties

Let $\boldsymbol{S}=(s_i)=(s_0,s_1,\cdots,s_{n-1})$ be an n-tuple binary sequence over GF(2)=$\{0,1\}$ and T be a cyclic shift left operator such that $T\boldsymbol{S}=(s_1,s_2,\cdots,s_0)$. The periodic autocorrelation function is defined by [2]

$$R_s(\tau)=\sum_{i=0}^{n-1}\chi(s_i)\cdot\chi(s_{(i+\tau)(\mathrm{mod}\,n)}) \qquad (1)$$

where $\chi(\cdot)$ is the unique isomorphism of the addition group $\{0,1\}$ onto the multiplication group $\{-1,1\}$. We call $R(0)$ the "in-phase autocorrelation value" and $R(\tau)$'s $(\tau\neq 0)$ the "out-of-phase autocorrelation values". The sequence $\boldsymbol{S}$ is said to have the "ideal autocorrelation property" if its periodic autocorrelation function has the lowest out-of-phase autocorrelation value of "1" or "-1".

III. Design of optimal frame synchronization sequences

Using the following important results, we can construct the optimal frame synchronization sequences.

Theorem 1: Let $\boldsymbol{S}=(s_i)$ be an n-tuple binary sequence over GF(2) with ideal autocorrelation function, where $n=2l+1$, $l=1,2,3,\cdots$. If a sequence $\boldsymbol{A}=(a_i)$ is constructed by the following relationships,

$$a_{2z(\mathrm{mod}\,N)}=s_{z(\mathrm{mod}\,n)} \qquad (2)$$

$$\chi(a_{(2z+1)(\mathrm{mod}\,N)})=-\chi(s_{(z+(n+1)/2)(\mathrm{mod}\,n)}) \qquad (3)$$

then the sequence $\boldsymbol{A}$ has the following optimal frame synchronization property.

$$R_a(\tau)=\begin{cases}N, & \tau\equiv 0(\mathrm{mod}\,N)\\ -N, & \tau\equiv n(\mathrm{mod}\,N)\\ 2, & \tau=\text{odd},\ \tau\neq n(\mathrm{mod}\,N)\\ -2, & \tau=\text{even},\ \tau\neq 0(\mathrm{mod}\,N)\end{cases}\quad\text{for positive odd } l \qquad (4)$$

$$R_a(\tau)=\begin{cases}N, & \tau\equiv 0(\mathrm{mod}\,N)\\ -N, & \tau\equiv n(\mathrm{mod}\,N)\\ -2, & \tau=\text{odd},\ \tau\neq n(\mathrm{mod}\,N)\\ 2, & \tau=\text{even},\ \tau\neq 0(\mathrm{mod}\,N)\end{cases}\quad\text{for positive even } l \qquad (5)$$

From theorem 1 we observe that the sequences with optimal autocorrelation property of even period can be generated by (2) and (3) based on binary sequences with ideal autocorrelation property.

Corollary 1: Let $\boldsymbol{S}$ be a maximal length sequence over GF(2) of period $n=2^r-1$, $r\geq 2$. Then the autocorrelation function of $\boldsymbol{A}$ with period $N=2n$, which is generated by (2) and (3) becomes (4).

Reference

[1] "Physical channels and mapping of transport channels onto physical channels (FDD)UTRA," *3GPP TSG RAN TS25.211.*

[2] R. Gold, "Optimal Binary Sequences for Spread Spectrum Multiplexing," *IEEE Trans. Inform. Theory*, vol. IT-13, pp.619-621, Oct. 1967.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Random Number Generation via Homophonic Coding

Andrei Fionov[1]
Siberian State University of Telecommunications and Information Sciences
Kirov St. 86, Novosibirsk 630102 Russia
e-mail: fionov@neic.nsk.su

Abstract — **We consider the problem of generating random numbers with a specified distribution by parsing a sequence of general coin tosses. We suggest a method based on homophonic coding that allows the number of tosses to approach arbitrarily close to the lower bound with exponentially less computational effort than other known methods.**

I. Introduction

The statement of the problem of random number generation is to produce a random number that obeys some prescribed target distribution when having as an input some known random process, e.g., repeated tosses of a coin. A general coin is assumed to take on values from $\{1, 2, \ldots, M\}$ with probabilities $p(1), p(2), \ldots, p(M)$. The additional natural setting to the problem is to minimize the (average) number of tosses required for generation of one random number.

Knuth and Yao [1] suggested a method for generating i.i.d. random numbers with specified probability distribution by making use of fair coin tosses. They constructed a parse tree which minimizes the average number of coin tosses and proved that $H+2$ is the lower bound for the average number of tosses, where H is the Shannon entropy of the target distribution. However, when a *sequence* of random numbers is to be generated, the size of the tree grows exponentially and the method is intractable. Han and Hoshi [2] suggested an interval algorithm which requires only linear growth of the memory size as the length of the sequence increases, and involves multiplication-type operations with linearly growing precision which results in roughly quadratic growth of computation time. They also used general coin tosses as an input.

To construct a class of less complex methods of random number generation we suggest an approach based on homophonic coding. We show that using the ACIS-method [3] requires only logarithmic growth of the memory size and roughly square-logarithmic growth of computation time when approaching the lower bound for the number of coin tosses.

II. The Essence of the Approach

In homophonic coding, a message $x_1x_2x_3\ldots$ with known probabilities of symbols is converted into a code sequence $c_1c_2c_3\ldots$, $c \in \{0, 1\}$, whose symbols are equiprobable and independent, i.e., indistinguishable from random bits. The decoder receives the sequence $c_1c_2c_3\ldots$ and also knows the source probability distribution. Having these data, it reconstructs the initial message $x_1x_2x_3\ldots$. Obviously, if instead of $c_1c_2c_3\ldots$ the decoder is given a sequence of fair coin tosses $r_1r_2r_3\ldots$ and a target distribution, it will produce a sequence of random numbers $y_1y_2y_3\ldots$ that obey this distribution.

Define the loss of generator to be the mean per random variable excess of the number of coin tosses over the random variable entropy. This loss is equal to the redundancy of a correspondent homophonic encoding that would produce such tosses. The ACIS-encoding [3] is to the date the fastest homophonic coding method that allows for arbitrarily small redundancy. Hence, the ACIS-decoding can provide arbitrarily small loss when used as a random number generator.

Let now a random variable X takes on values from $\{1, 2, \ldots, M\}$ with arbitrary (but known) probabilities. Let we are given a sequence of the random variable values $X^m = x_1x_2\ldots x_m$. It is required to generate a sequence of random numbers $Y^n = y_1y_2\ldots y_n$ that represent values of a random variable Y that obeys some target distribution over $\{1, 2, \ldots N\}$. Denote by $H(X)$ and $H(Y)$ the entropies of X and Y.

To solve this general problem we apply ACIS-encoding to X^m and transfer the code bits produced to ACIS-decoder that operates under the distribution for Y. But the encoder needs an extra source of random bits in order to make homophone selection. To obtain a solution in a standard framework, i.e., without any extra source of randomness, we replace the source of random bits with an auxiliary random bit generator and let a small fraction of the source numbers fork to the generator. Of course, this generator cannot be based on homophonic coding. But we could expect that even a relatively more complex generator would not increase the overall complexity since the number of random bits it must generate can be made arbitrarily small.

Theorem: Let the scheme based on ACIS encoding and decoding be used to generate a sequence of random numbers Y^n, $n \to \infty$, by parsing a sequence of general coin tosses X^m. Then the expected number of values of X required to generate one value of Y

$$\lim_{n\to\infty} \frac{E(m)}{n} = \frac{H(Y)}{H(X)} + \epsilon,$$

and the loss ϵ can be made arbitrarily small at the expense of the memory size S and computation time T growing as

$$S = O\left(\log \frac{1}{\epsilon}\right), \quad T = O\left(\log \frac{1}{\epsilon} \log\log \frac{1}{\epsilon} \log\log\log \frac{1}{\epsilon}\right).$$

References

[1] D. E. Knuth and A. C. Yao, "The complexity of nonuniform random number generation," in *Algorithms and Complexity: New Directions and Results*, J. F. Traub Ed., New York: Academic Press, 1976, pp. 357–248.

[2] T. S. Han and M. Hoshi, "Interval algorithm for random number generation," *IEEE Trans. Inform. Theory*, vol. 43, no. 2, pp. 599–611, 1997.

[3] B. Ryabko and A. Fionov, "Efficient homophonic coding," *IEEE Trans. Inform. Theory*, vol. 45, no. 6, pp. 2083–2091, 1999.

[1]This work was supported by RFBR Grant 99-01-00586.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

A new Class of Multiuser CDMA Receivers based on The Minimum Mean-Output-Energy Strategy

Stefano Buzzi *and* Marco Lops
Università degli Studi di Cassino
DAEIMI – Via G. Di Biasio, 43
I-03043 Cassino (FR), Italy
e-mail: (buzzi,lops)@unicas.it

Antonia M. Tulino
Un. di Napoli "Federico II"
DIET – Via Claudio, 21
I-80125 Napoli, Italy
e-mail:
tulino@diesun.die.unina.it

Abstract — **In this work we deal with the problem of linear multiuser detection for asynchronous DS/CDMA systems. We introduce a new Mean-Output-Energy cost function, whose constrained minimization leads to two new linear multiuser detectors, exploiting the information contained in the pseudoautocorrelation of the observables, and which generalize and outperform the classical decorrelating and minimum mean square error receivers.**

I. Introduction

The decorrelating detector [1] and the minimum mean square error (MMSE) receiver [2] are the two most popular linear multiuser detectors; indeed, both receivers have a complexity which is linear in the users number and achieve optimum performance in terms of near-far resistance. Both detectors, however, exploit only the information contained in the autocorrelation function of the observables. While this is the optimum strategy when dealing with proper complex random processes, it turns out to be suboptimal in situations where the disturbance is an improper complex random process[1]. Since, as shown in [3], the multiaccess interference (MAI) can be modeled as an improper complex noise, it is expected that designing receiving structures capable of exploiting the information contained in the pseudoautocorrelation function of the observables would permit achieving better performance. In this work, we deal with the problem of linear multiuser detection: a new cost function is introduced, whose constrained minimization leads to new versions of the decorrelating and the MMSE receivers exploiting the information contained in the observables pseudoautocorrelation function.

II. System Model and Detectors Design

We consider an asynchronous DS/CDMA network with K active users. Stacking in an NM-dimensional vector[2], the discrete-time samples of the received waveform in the p-th signaling interval $[pT_b, (p+1)T_b]$, and assuming that we are interested in decoding the bits from the user "0" and that $\tau_0 = 0$, we obtain the vector:

$$\boldsymbol{r}(p) = A_0 b_0(p)\boldsymbol{s}_0^0 + \boldsymbol{z}(p) + \boldsymbol{w}(p) \tag{1}$$

In the above equation, $\boldsymbol{z}(p)$ and $\boldsymbol{w}(p)$ contain the contribution from the MAI and from the additive thermal noise, respectively. Given the NM-dimensional observable vector $\boldsymbol{r}(p)$, any linear receiver takes a decision as to the bit $b_0(p)$ according to the rule:

$$\widehat{b}_0(p) = \mathrm{sgn}\left(\Re\left\{\boldsymbol{d}_0^H \boldsymbol{r}(p)\right\}\right) \tag{2}$$

where $\mathrm{sgn}(\cdot)$ denotes the signum function, $\Re\{\cdot\}$ denotes real part, while the vector $\boldsymbol{d}_0 \in \mathcal{C}^{NM}$ is to be designed according to some optimization criterion. Since, inspecting the decision rule (2), it is seen that the receiver performance is impaired by the disturbance term $\Re\left\{\boldsymbol{d}_0^H(\boldsymbol{z}(p)+\boldsymbol{w}(p))\right\}$, we propose here to choose the vector $\boldsymbol{d}_0$ as the solution to the following constrained minimization problem:

$$\mathrm{E}\left[\left(\Re\left\{\boldsymbol{d}_0^H \boldsymbol{h}(p)\right\}\right)^2\right] = \min \quad \text{s.t.} \quad \Re\left\{\boldsymbol{d}_0^H \boldsymbol{s}_0^0\right\} = 1 \tag{3}$$

The solution to the above problem can be shown to be written as:

$$\boldsymbol{d}_0 = \boldsymbol{H_{vv}}\boldsymbol{s}_0^0 - \boldsymbol{M}_{\boldsymbol{vv}}^{+}\boldsymbol{M}'_{\boldsymbol{vv}}\boldsymbol{H}_{\boldsymbol{vv}}^{*}\boldsymbol{s}_0^{0*} \tag{4}$$

with $\boldsymbol{H_{vv}} = 2\left(\boldsymbol{M_{vv}} - \boldsymbol{M}'_{\boldsymbol{vv}}\boldsymbol{M}_{\boldsymbol{vv}}^{*+}\boldsymbol{M}_{\boldsymbol{vv}}^{'*}\right)^{+}$. In the above equations, $(\cdot)^+$ denotes the Moore-Penrose generalized inverse, $\boldsymbol{M_{vv}} = E\left[\boldsymbol{v}(p)\boldsymbol{v}^H(p)\right]$ and $\boldsymbol{M}'_{\boldsymbol{vv}} = E\left[\boldsymbol{v}(p)\boldsymbol{v}^T(p)\right]$ represent the covariance and pseudocovariance matrix of the vector $\boldsymbol{v}(p)$, respectively[3], while, finally, $\boldsymbol{v}(p) = A_0 b_0(p)\boldsymbol{s}_0^0 + \boldsymbol{h}(p)$. It can be shown that, if we let $\boldsymbol{h}(p) = \boldsymbol{z}(p)$, solution (4) represents a generalization of the decorrelating detector, while, if we let $\boldsymbol{h}(p) = \boldsymbol{z}(p) + \boldsymbol{w}(p)$, solution (4) is a generalization of the MMSE linear multiuser detector. Only in the special case that the matrix $\boldsymbol{M}'_{\boldsymbol{vv}}$ is zero, does solution (4) reduce to the classical decorrelating and MMSE linear multiuser detectors.

As to the performance assessment, it can be shown that the newly proposed receivers outperform the classical linear multiuser receivers. Indeed, an analytical proof showing that the new receivers achieve a near-far resistance not smaller than that of the classical decorrelating receiver can be given, while computer simulations confirm the superiority of the new receivers in terms of error probability too.

[1] According to [3], a complex random process $n(t)$ is said to be proper if its pseudoautocorrelation function $R_n(t,u) = \mathrm{E}[n(t)n(u)]$ is zero $\forall t, u$, and it is said to be improper in the opposite case that $R_n(t,u)$ is non-zero.

[2] N is the processing gain, M is the number of samples per chip.

[3] $(\cdot)^H$ denotes conjugate transpose and $(\cdot)^T$ denotes conjugate.

References

[1] R. Lupas, S. Verdù, "Linear Multiuser Detectors for Synchronous Code-Division Multiple Access Channels", *IEEE Trans. on Information Theory*, Vol. 35, pp. 123-136, January 1989.

[2] U. Madhow, M. Honig, "MMSE Interference Suppression for Direct-Sequence Spread-Spectrum CDMA", *IEEE Trans. on Communications*, Vol. 42, pp. 3178-3188, December 1994.

[3] Y. Yoon, H. Leib, "Maximizing SNR in Improper Complex Noise and Applications to CDMA", *IEEE Communications Letters*, Vol. 1, pp. 5-8, January 1997.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

MMSE Multiuser Detection for Noncoherent Non-Orthogonal Multipulse Modulation

Michael L. McCloud and Louis L. Scharf
Department of Electrical and Computer Engineering
University of Colorado, Boulder, CO 80309-0425 USA
Email:*mccloud@ucsu.colorado.edu* *scharf@schof.colorado.edu*

Abstract — **In this summary, we present the minimum mean squared error multiuser detector for noncoherent detection of non-orthogonal multipulse modulation. The detector is analyzed in the large signal-to-noise ratio regime and it is shown that the MMSE detector approaches a new multiple access interference suppressing detector, termed the multipulse decorrelating (MD) detector. The asymptotic performance of the detectors is presented for the additive white Gaussian noise noncoherent channel.**

I. Introduction

We introduce the minimum mean squared error (MMSE) detector for non-orthogonal multipulse modulation (NMM) over the noncoherent multiple access channel. NMM is a generalization of orthogonal modulation in which the users may transmit correlated waveforms, allowing for bandwidth efficiency. The generalized maximum likelihood (GML) detector has been studied in [1]-[6] for detection on such channels and we compare the GML with the MMSE detector for large values of the signal-to-noise ratio (SNR). The MMSE will be seen to approach a new detector, termed the multipulse-decorrelating (MD) detector, at large SNRs. We show that the the MD (and hence the MMSE) detector is asymptotically superior to the GML detector for binary (M=2) signalling but that this performance advantage does not generalize to larger cardinality signal sets.

II. Discrete Time Model

We adopt the following discrete model for the output of the noncoherent multiple access channel after basis function matched filtering:

$$\mathbf{y} = \mathcal{H}\mathcal{D}\boldsymbol{b} + \mathbf{n}. \tag{1}$$

The matrix $\mathcal{H} = [\mathbf{H}(1), \mathbf{H}(2), \cdots, \mathbf{H}(K)]$ contains the signal vectors for each user with $\mathbf{H}(k) = [\mathbf{h}_1(k), \mathbf{h}_2(k), \cdots, \mathbf{h}_M(k)]$ and $\mathbf{h}_m(k)$ is the m^{th} signal corresponding to user k. The vector $\boldsymbol{b} = [\mathbf{b}^T(1), \mathbf{b}^T(2), \cdots, \mathbf{b}^T(K)]^T$ is an $MK \times 1$ vector with each $\mathbf{b}(k)$ a column of the $M \times M$ identity matrix which selects the signal transmitted by user k. The $MK \times MK$ matrix $\mathcal{D}$ contains the user energy and phase terms. The additive noise, $\mathbf{n}$, is modeled as zero-mean complex Gaussian with correlation matrix $E[\mathbf{n}\mathbf{n}^*] = \sigma^2\mathbf{I}$.

Assuming that the phase terms are independent zero mean random variables, the measurement $\mathbf{y}$ has first and second order statistics: $\mathbf{m} = E[\mathbf{y}] = \mathbf{0}$ and $\mathbf{R} = E[\mathbf{y}\mathbf{y}^*] = \mathcal{H}\mathbf{F}\mathcal{H}^* + \sigma^2\mathbf{I}$, where $\mathbf{F} = \text{diag}\{E_1\mathbf{I}, \cdots, E_K\mathbf{I}\}$ and E_k is the energy associated with the k^{th} user.

This work was supported by the National Science Foundation under Contract No. ECS 9979400 and by the Office of Naval Research under Contract No. N00014-00-1-0033. The results contained in this paper have been submitted to the *IEEE Transactions on Communications*.

III. The MMSE Detector

The (linear) minimum mean squared error estimate of the vector $\mathcal{D}\boldsymbol{b}$ is given by $\widehat{\mathcal{D}\boldsymbol{b}} = \mathbf{F}\mathcal{H}^*\mathbf{R}^{-1}\mathbf{y}$. We make decisions on user k by examining the k^{th} block, $\widehat{\mathbf{D}(k)\mathbf{b}(k)}$, of the estimate $\widehat{\mathcal{D}\boldsymbol{b}}$. This leads to the simple decision rule:

$$\begin{aligned}\hat{m}_{MMSE}(k) &= \arg\max_m \left|\left\{\widehat{\mathbf{D}(k)\mathbf{b}(k)}\right\}_m\right|^2 \\ &= \arg\max_m \left\{\left|\mathbf{h}_m^*(k)\mathbf{R}^{-1}\mathbf{y}\right|^2\right\},\end{aligned} \tag{2}$$

where $\mathbf{R} = E[\mathbf{y}\mathbf{y}^*]$.

At high values of the signal to noise ratio (SNR) we find that the MMSE detector approaches the asymptotic form:

$$\hat{m}_{MD}(k) = \arg\max_m \left|\left\{\left(\mathbf{H}(k)^*\mathbf{P}^{\perp}_{\mathbf{S}(k)}\mathbf{H}(k)\right)^+ \mathbf{H}(k)^*\mathbf{P}^{\perp}_{\mathbf{S}(k)}\mathbf{y}\right\}_m\right|^2,$$

where $\mathbf{A}^+$ is the pseudo-inverse of the matrix $\mathbf{A}$ and the interference matrix $\mathbf{S}(k)$ has the signals $\mathbf{H}(l)$ for $l \neq k$ as its columns. We call this detector the multipulse decorrelating (MD) detector in analogy to the linear decorrelating detector of [7].

Using standard union bounds and two signal lower bounds we find that as the SNR grows large, the error probability for the MD (and hence the MMSE) detector has the asymptotic form

$$P \sim \exp\left\{\min_{m\neq l} \frac{-E_k}{\sigma^2\left((\mathbf{G}^*\mathbf{G})^+_{m,m} + (\mathbf{G}^*\mathbf{G})^+_{l,l} + 2\left|(\mathbf{G}^*\mathbf{G})^+_{m,l}\right|\right)}\right\}, \tag{3}$$

where we have defined $\mathbf{G} = \mathbf{P}^{\perp}_{\mathbf{S}(k)}\mathbf{H}(k)$.

By comparing this expression with the probability of error for the generalized maximum likelihood (GML) detector of [1]-[5] we find that for $M = 2$ (binary signaling) the MD (MMSE) detector is superior to the GML rule asymptotically. This result does not generalize to larger cardinality signal sets. Neither detector is uniformly superior over constellation sizes $M > 2$.

References

[1] A. Russ, "Noncoherent detection for nonlinear binary modulation in Gaussian CDMA channels," M.S. thesis, Friedrich Alexander Universitaet, Erlangen-Nuremberg, Germany, Sep. 1996.

[2] M. McCloud, L. L. Scharf, and L. T. McWhorter, "Subspace coherence for detection in multiuser additive noise channels," in *Proc. SPAWC '97*, Paris, France, April 1997, pp. 225–228.

[3] M. Varanasi and A. Russ, "Noncoherent decorrelative multiuser detection for nonlinear nonorthogonal modulation," in *Proc. I.C.C.'97*, Montreal, Canada, June 1997.

[4] M. McCloud and L. L. Scharf, "Generalized likelihood detection on multiple access channels," in *Proc. Asilomar '97*, Monterey, CA, Nov. 1997.

[5] M. Varanasi and A. Russ, "Noncoherent decorrelative detection for nonorthogonal multipulse modulation over the multiuser Gaussian channel," *IEEE Trans. Commun.*, vol. 46, no. 12, pp. 1675–84, Dec. 1998.

[6] M. McCloud and L. L. Scharf, "Interference estimation with applications to blind multiple access communication over fading channels," *IEEE Trans. Inform. Theory*, vol. 46, no. 3, pp. 1–15, May 2000.

[7] R. Lupas and S. Verdu, "Linear multiuser detectors for synchronous code-division multiple-access channels," *IEEE Trans. Inform. Theory*, vol. 35, no. 1, pp. 123–136, Jan. 1989.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

A new Group Detection Strategy for DS/CDMA Systems

Stefano Buzzi *and* Marco Lops
Università degli Studi di Cassino
DAEIMI – Via G. Di Biasio, 43
I-03043 Cassino (FR), Italy
e-mail: (buzzi,lops)@unicas.it

Giuseppe Ricci
Università degli Studi di Lecce
Dip. di Ingegneria dell'Innovazione
Via Per Monteroni
I-73100 Lecce, Italy
e-mail: giuseppe.ricci@unile.it

Abstract — **In this paper we present a new group detection strategy for asynchronous DS/CDMA Systems. The new detector is a two-stage one: the first stage is a linear filter, aimed at suppressing the effect of the unwanted users signals, while the second stage is a non-linear block, implementing a maximum likelihood (ML) detection rule on the set of desired users signals. Simulation results confirm that the new structure, which encompasses Varanasi's group detector as a special case, achieves very satisfactory performance.**

I. Introduction

Given a Direct-Sequence Code-Division Multiple-Access (DS/CDMA) communication system with K active users, a group detector jointly demodulates the information bits stream from a certain subset, $\mathcal{G}$ say, of the K transmitting users. The concept of group detection was first introduced by Varanasi in [1], wherein, with reference to a synchronous CDMA system, new receiving structures were derived, based on the application of the generalized likelihood rule.

In the very recent past, group detection has become an attracting and intriguing research topic, in that it has been recognized that it can be successfully applied to wireless cellular communications so as to come up with multiuser receivers able to suppress both the intra-cell and the inter-cell interference [2] and with single-user receivers for multirate/multicode CDMA systems [3].

In this work we consider an asynchronous DS/CDMA system and present a new group detection structure; it is a two-stage receiver: the first stage is a linear filter, aimed at suppressing the multiaccess interference (MAI), and whose G-dimensional output (with G the cardinality of the set $\mathcal{G}$ of the desired users) is forwarded to the second stage, a non-linear device, which implements a maximum-likelihood detection strategy and takes the final decision on the G bits of interest.

II. System Model and Receiver Synthesis

We consider an asynchronous DS/CDMA System with K active users. Assume, without loss of generality, that the users to be decoded are indexed by $0,\ldots,G-1$, namely that $\mathcal{G}=\{0,\ldots,G-1\}$. It follows that the discrete-time version of the complex envelope of the received waveform in the bit-interval $[pT_b,(p+1)T_b]$, $\boldsymbol{r}(p)$ say, is an NM-dimensional[1] vector expressed as:

$$\boldsymbol{r}(p)=\sum_{k=0}^{G-1}A_k e^{j\phi_k}b_k(p)\boldsymbol{s}_k^0+\boldsymbol{z}(p)+\boldsymbol{w}(p) \qquad (1)$$

[1] N is the processing gain and M is the number of samples per chip.

wherein $\boldsymbol{z}(p)$ and $\boldsymbol{w}(p)$ represent the discrete-time versions of the MAI and of the thermal noise. We also suppose that the codes $\boldsymbol{s}_0^0,\ldots,\boldsymbol{s}_{G-1}^0$ are linearly independent. The detection structure that we consider is depicted in figure 1. The filter $\boldsymbol{D}$ is chosen as the solution to the following constrained minimization problem:

$$E\left[\left\|\boldsymbol{D}^H\boldsymbol{h}(p)\right\|^2\right]=\min \quad \text{subject to: } \boldsymbol{D}^H\boldsymbol{S}_G=\boldsymbol{K} \qquad (2)$$

wherein $\boldsymbol{S}_G$ is an $NM\times G$-dimensional matrix containing on its columns the signatures from the users to be decoded, and $\boldsymbol{K}$ is a $G\times G$ matrix, which we assume to have full-rank. If we let $\boldsymbol{h}(p)=\boldsymbol{r}(p)-\boldsymbol{w}(p)$, the filter $\boldsymbol{D}$ ends up coincident with a decorrelating group detector, and, if the signatures of all of the active users are linearly independent, it zero-forces the MAI. Under this circumstance, it can be also shown that, if we let $M=1$ and consider a synchronous CDMA system, the receiver structure in figure 1 reduces to the group detector presented in [1]. On the other hand, if we let $\boldsymbol{h}(p)=\boldsymbol{r}(p)$, the filter $\boldsymbol{D}$ reduces to a group MMSE detector. It is also seen that the choice of the constraint matrix $\boldsymbol{K}$ has no effect on the system structure, so that we can set $\boldsymbol{K}$ equal to the identity matrix.

As to the performance assessment, simulation results confirm that the new structure achieves very satisfactory performance. In keeping with the single-user receivers behavior, the MMSE group detector outperforms its decorrelating counterpart, especially for large number of users and/or for power-controlled systems.

Finally, it is worth pointing out that the new structures may be implemented in a blind adaptive fashion through a straightforward application of the Recursive-Least-Squares algorithm or of subspace tracking algorithms.

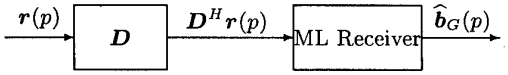


Figure 1: Block-scheme of the group detector.

References

[1] M.K. Varanasi, "Group Detection for Synchronous Gaussian Code-Division Multiple-Access Channels," *IEEE Trans. on Information Theory*, Vol. 41, pp. 1083-1096, July 1995.

[2] J. Yu, A. Host-Madsen, "Subspace Tracking for Group-Blind Multiuser Detectors," *IEEE Vehicular Technology Conference*, Houston, Texas, May 16-19, 1999.

[3] U. Mitra, "Comparison of Maximum Likelihood-based Detection for two Multi-rate Access Schemes for CDMA Signals," *IEEE Trans. on Communications*, Vol. 47, pp. 64-77, January 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Adaptive Linear-Quadratic Receivers for Time-Varying, Frequency-Selective Code-Division-Multiple-Access Channels

Richard J. Barton and Jian-Jun Ni
Department of Electrical and Computer Engineering
Iowa State University
3119 Coover Hall
Ames, IA 50011-3060
{barton,jjni}@iastate.edu

Abstract – In this paper we discuss a research effort focused on the design and analysis of robust, low-complexity, adaptive wireless receivers that exhibit good performance characteristics in the presence of multiple sources of complex structured interference as well as significant uncertainty regarding the exact structure of that interference. We consider problems primarily related to the code-division, multiple-access (CDMA) environment. In particular, we study adaptive one-shot linear-quadratic (LQ) receivers for time-varying, frequency-selective CDMA fading channels. We propose a novel Bayesian approach to this problem in which receivers are designed based on a probabilistic channel model that explicitly incorporates multiple sources of additive interference as well as a stochastic structure for the channel uncertainty. Under the assumption that the probabilistic structure of the channel model is known, we develop and analyze a design strategy for adaptive LQ receivers that are optimal with respect to the assumed channel model and robust with respect to uncertainty regarding the true instantaneous state of the channel. In addition, we develop and analyze an adaptive modulation scheme that works in conjunction with the proposed LQ receivers to either maximize throughput or minimize probability of error.

For the purposes of receiver design (but not performance analysis), we make the simplifying assumption that all additive interference on the channel is Gaussian. If we were to restrict attention to linear detectors incorporating antipodal signals, then it is easy to show that the proposed approach to receiver design would lead directly to an adaptive minimum-mean-squared-error (MMSE) linear detector analogous to the one developed in [1]. In this respect, the proposed approach can be regarded as a generalization of linear MMSE detection that is much less sensitive to errors in channel state estimates. Under the Gaussian assumption, the optimal detectors for a fixed signal structure and known estimates of the current channel state are necessarily linear-quadratic. We show that if the second-order structure of the channel is known, then the optimal detector for binary signals can be determined by maximizing a particular cost function. In addition, we show that the maximum value of the proposed LQ cost function for any pair of transmitted signals is equivalent to the Kullback-Leibler (KL) distance between the two corresponding Gaussian hypotheses. Hence, maximizing the cost function simultaneously with respect to both the signal and detector structure gives the optimal LQ detector for the signal pair that maximizes the KL distance between the corresponding Gaussian hypotheses subject to the known estimates of the channel state and the second-order channel structure. Furthermore, the structure of the cost function can be exploited to develop efficient adaptive algorithms for simultaneous signal selection and receiver design. Finally, this approach can be extended straightforwardly to M-ary signal constellations in order to adapt the modulation and detector structure to give minimum probability of error at a fixed data rate or maximum data rate at a fixed probability of error. This leads to adaptive modulation schemes that are analogous to those discussed in [2, 3] but much less sensitive to errors in channel state estimates.

As an indication of the potential of this approach, consider the results of a simulation experiment presented in Figure 1.

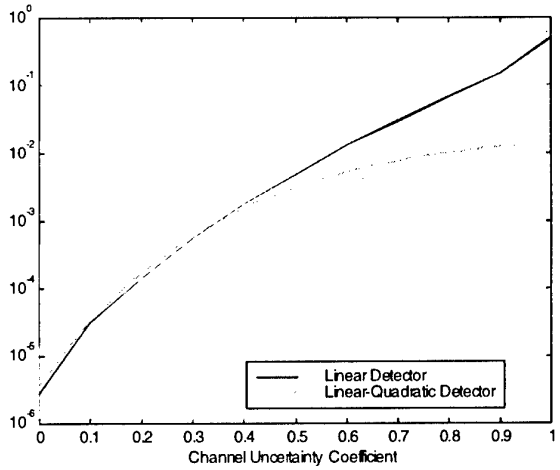


Figure 1. MMSE Linear Receiver versus LQ Receiver with Adaptive Binary Signaling at 8 dB SNR

References

[1] M. Honig, U. Madhow, and S. Verdu, "Blind Adaptive Multi-user Detection," *IEEE Transactions on Information Theory*, vol. 41, pp. 944-960, July, 1995.

[2] A. J. Goldsmith and S.-G. Chua, "Variable-Rate Variable-Power MQAM for Fading Channels," *IEEE Transactions on Communications*, vol. 45, no. 10, pp. 1218-1230, Oct., 1997.

[3] A. J. Goldsmith and S.-G. Chua, "Adaptive Coded Modulation For Fading Channels," *IEEE Transactions on Communications*, vol. 46, no. 5, pp. 595-602, 1998.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On Error-Free Filtering under Dependent Distortions [1]

M. S. Pinsker and V. V. Prelov
Institute for Information
Transmission Problems
of the Russian Acad. of Sci.,
19 Bol'shoi Karetnyi,
101447 Moscow, Russia
e-mail: pinsker@iitp.ru,
prelov@iitp.ru

Abstract — **The problem of error-free filtering for a discrete-time, stationary, singular, stochastic process $X = \{X_n\}$ from observations $Y = \{Y_n\}$ in the case of dependent distortions, i.e., where the pair (X, Y) forms a jointly stationary process is considered.**

Let (X, Y) be a two-dimentional, partially observable, discrete-time, stationary stochastic process where $X = \{X_n\}$ is the nonobservable and $Y = \{Y_n\}$ the observable component. We shall take an interest in finding rather general conditions under which error-free filtering of X_n from the observations $\{Y_j, j \le n\}$ is possible. In [1, 2], such conditions were pointed out for the case where $Y = X + Z$ and X and Z are independent stationary processes. In [3], such kind of conditions were found for the case of independent distortions, i.e., under the assumptions that, given a sequence $\{X_n\}$, the observations $\{Y_n\}$ are independent and

$$\mathbf{P}\{Y_n \in dy \mid X_j, j = 0 \pm 1, \ldots\} = \mathbf{P}\{Y_n \in dy \mid X_n\}$$

and, moreover, the conditional distribution $\mathbf{P}\{Y_n \in dy \mid X_n\}$ does not depend on n. Thus, in this case, the observations $\{Y_n\}$ can be considered as an output sequence of a stationary memoryless channel whose the input sequence is $\{X_n\}$.

Here, we consider a more general situation where, given a sequence $\{X_n\}$, the observations $\{Y_n\}$ can be dependent. The results obtained here are rather closed to some results of [4] though, in contrast to [4], we consider a *causal* filtering and, moreover, the methods of proof are absolutely different.

Let us now assume that the process X being estimated and the observable process Y form a two-dimentional jointly stationary stochastic process. Moreover, we shall assume that X is a singular process with a finite number of values in a set $\mathcal{X}$ and Y takes values in a measurable subset $\mathcal{Y}$ of the real line.

To state the main result, we introduce the notion of conditional regularity for a pair of processes $X = \{X_n\}$ and $Y = \{Y_n\}$. To do this, we need in some definitions. Denote by $\mathcal{X}^I$ the set of all infinite sequences $\mathbf{x} = (\ldots x_{-1}, x_0, x_1, \ldots)$, $x_i \in \mathcal{X}$, $i = 0, \pm 1, \ldots$. The set $\mathcal{Y}^I$ is defined similarly. Let $\mu^I_{\mathbf{x}}(\cdot)$, $\mathbf{x} \in \mathcal{X}^I$ be a probability measure on $\mathcal{Y}^I$ (with σ-algebra of measurable sets generated by all cylinder sets) which is a conditional distribution of $Y = \{Y_n\}$ given $X = \mathbf{x}$, $\mathbf{x} \in \mathcal{X}^I$, i.e., $\mu^I_{\mathbf{x}}(\cdot) = \mathbf{P}_{Y|X=\mathbf{x}}(\cdot)$.

Assume now that the measures $\mu^I_{\mathbf{x}}(\cdot)$, $\mathbf{x} \in \mathcal{X}^I$, have the following property: for all $B \in \mathcal{F}_Y(-\infty, \infty) = \bigcup_n \mathcal{F}_Y(-\infty, n]$ (where $\mathcal{F}_Y(-\infty, n] \equiv \sigma\{Y_j, j \le n\}$ is the σ-algebra generated by values of the process $Y = \{Y_j\}$ up to time instant n)

$$\sup_{A \in \mathcal{F}_Y(-\infty, n]} |\mu_{\mathbf{x}}(AB) - \mu_{\mathbf{x}}(A)\mu_{\mathbf{x}}(B)| \to 0 \quad \text{as} \quad n \to -\infty$$

uniformly in $\mathbf{x}$ for almost all $\mathbf{x} \in \mathcal{X}^I$ (with respect to the measure generated by the process X). In this case, we shall call that the process $Y = \{Y_n\}$ is *conditionally regular* with respect to $X = \{X_n\}$.

Note that in the case where X and Y are independent, the notions of conditional regularity and (usual) regularity coinside.

Let $\mu^n_{\mathbf{x}}(\cdot)$, $\mathbf{x} \in \mathcal{X}^I$, be a projection of $\mu^I_{\mathbf{x}}(\cdot)$ on the space of values of the random variable Y_n, i.e., $\mu^n_{\mathbf{x}}(\cdot) = \mathbf{P}_{Y_n|X=\mathbf{x}}(\cdot)$ is the conditional distribution of Y_n given $X = \mathbf{x}$. Finally, denote by $\nu^n_x(\cdot) = \mathbf{P}_{Y_n|X_n=x}(\cdot)$, $x \in \mathcal{X}$, a probability measure on $\mathcal{Y}$ which is a conditional distribution of Y_n given $X_n = x$. In the case of jointly stationary processes X and Y the measure $\nu^n_x(\cdot)$ does not depend on n and will be denoted by $\nu_x(\cdot)$.

The main result is given by the following

Theorem. *If Y is conditionally regular with respect to X,*

$$\mu^{n_0}_{\mathbf{x}}(\cdot) = \nu_{x_0}(\cdot)$$

for any $\mathbf{x} = (\ldots x_{-1}, x_0, x_1, \ldots)$, and

$$\nu_x(\cdot) \ne \nu_{x'}(\cdot) \quad \text{for} \quad x \ne x',$$

then for any integers m and n the equality

$$\mathbf{E}[X_n | Y^m_{-\infty}] = X_n \quad a.s.,$$

holds, i.e., the value of X_n, $n = 0, \pm 1, \ldots$, can be reconstructed without error from the observations $Y^m_{-\infty} = \{Y_j, j \le m\}$.

The proof of this theorem can be found in [5].

References

[1] H. Furstenberg, "Disjointness in ergodic theory, minimal sets, and a problem on Diophantine approximation," *Mat. Syst. Theory*, vol. 1, No. 1, pp. 1–49, 1967.

[2] M. S. Pinsker and V. V. Prelov, "On error-free filtering of some stationary processes," *Usp. Mat. Nauk*, vol. 52, No. 2, pp. 109–118, 1997.

[3] M. S. Pinsker and V. V. Prelov, "Error-free filtering of an entropy-singular signal under independent distortions," *Probl. Peredachi Inf.*, vol. 34, No. 3, pp. 3–6, 1998.

[4] H. Furstenberg, Y. Peres, and B. Weiss, "Perfect filtering and double disjointness," *Ann. Inst. Henri Poincare*, vol. 31, No. 3, pp. 453–465, 1995.

[5] M. S. Pinsker and V. V. Prelov, "Error-free filtering under dependent distortions," *submitted to Probl. Peredachi Inf.*

[1] This work was supported in part by the Russian Fundamental Research Foundation under Grant 99-01-00828.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Recovery Of Not Necessarily Band-Limited Signals From Noisy Observations

A. Krzyzak
Department of Computer Science,
Concordia University, Montreal,
P.Q., H3G 1M8, Canada

E. Rafajlowicz
Institute of Engineering
Cybernetics,
Wroclaw University of Technology,
Wroclaw, Poland

M. Pawlak
Department of Electrical and
Computer Engineering,
University of Manitoba, Winnipeg,
Manitoba, R3T 5V6, Canada

Abstract — **The purpose of this paper is to describe the extension of the Whittaker-Shannon sampling theorem to the case of signals observed in the presence of noise. We introduce a class of signal recovery methods being a smooth correction of the cardinal series. Both band-limited and non band-limited signals are considered. The weak and strong L_2 consistency of the algorithms are established and the rate of convergence is investigated.**

I. Introduction

The Whittaker-Shannon (WS) sampling-interpolation theorem is generally recognized as a milestone in information theory, communication systems, signal processing as well as Fourier analysis [1]. The result may be briefly stated as follows. Consider a class $BL(\Omega)$ of band-limited signals with bandwidth Ω and fintie energy. The WS theorem says that every $f \in BL(\Omega)$ can be reconstructed from its discrete values $f(j\tau)$, $j = 0, \pm 1, \pm 2, \ldots$ by

$$f(t) = \sum_{j=-\infty}^{\infty} f(j\tau)\mathrm{sinc}\left(\frac{\pi}{\tau}(t - j\tau)\right) \qquad (1)$$

provided that $\tau \leq \pi/\Omega$, where $\mathrm{sinc}(t) = \sin(t)/t$. Formula (1) is frequently referred as the cardinal series or the WS interpolation scheme. Many extensions of (1) have been given in the case when some assumptions in the sampling theorem are not satisfied. In particular, truncation, aliasing, location (jitter), amplitude errors of the WS cardinal expansion have been examined. Furthermore, generalizations to multiple dimensions, random signals, not necessarily bandlimited signals, missing data, wavelet subspaces and irregular sampling have been proposed [1], [4]. Relatively little attention, however, has been given to the problem of signal sampling in the presence of random noise. This issue has been mentioned a number of times in the signal processing literature, but no algorithms with established convergence properties for a signal reconstruction from noisy data were given. The rigorous theoretical threatment of this problem has been studied in [2] and [3]. In all these papers a particular class of reconstruction algorithms has been examined and only band limited signals have been taken into account. In this paper we study the previously introduced algorithms for both band-limited and also non band-limited signals. We observe that each particular technique can have good reconstruction accuracy and no technique dominates universally over a large class of signals. Hence our principal goal in this paper is to reconstruct a signal $f(t)$ from the following finite record of sampled and noisy data $y_j = f(j\tau) + \varepsilon_j, |j| \leq n$, where τ is a sampling rate.

We examine two types of estimators of $f(t)$ motivated by the cardinal expansion formula. The first one is a kernel type estimator with the *sinc* function being the reproducing kernel for $BL(\Omega)$. The second class is using an orthogonality property of the *sinc* function yielding an orthogonal series estimate. We also extend our theory to the case of not necessary band-limited signals. Hence we show that our estimates can adapt to a larger class of signals. This is carried out by approximating non-band-limited signal in $L_2(R)$ by a sequence of band-limited functions with the bandwidth increasing to infinity, i.e., $\Omega = \Omega_n \to \infty$ as $n \to \infty$. It is worth noting that allowing Ω to vary our construction can be viewed from the prespective of wavelet interpolation subspaces (multiresolution theory). Let us note, however, that our estimation algorithms do not interpolate data; the necessary property in the presence of noise.

II. Estimators and Results

The first estimator of $f(t)$ is based on the fact $K(t) = \sin(\Omega' t)/\pi t$ is a reproducing kernel for $BL(\Omega)$ provided that $\Omega \leq \Omega'$. Hence we obtain the following kernel estimate $\hat{f}_n(t) = \tau \sum_{|j| \leq n} y_j \frac{\sin(\Omega'(t - j\tau))}{\pi(t - j\tau)}$. Note that $\hat{f}_n \in BL(\Omega')$, hence $\hat{f}_n$ lives in the same space as f. Such a property is not shared by ordinary kernel estimators. To construct the second estimator we observe that (1) can be written in the following equivalent form $f(t) = \sum_{j=-\infty}^{\infty} f(j\tau)\, s_j(t)$, where it is known that $\{s_j(t) = \mathrm{sinc}(\pi(t - j\tau)/\tau), j = 0, \pm 1, \ldots\}$ defines as orthogonal and complete system of functions for $BL(\Omega)$, provided that $\tau \leq \pi/\Omega$.

The above interpretation of the cardinal expansion suggests the following orthogonal type estimate of $f(t)$: $\tilde{f}_n(t) = \sum_{|k| \leq N} \tilde{y}_k\, s_k(t)$, where $\tilde{y}_k = \sum_{|i| \leq M} w_i\, y_{k-i}$ is the weighted moving average of $\{y_k\}$ in the neighborhood of $f(k\tau)$. The global mean integrated sequared error (MISE) converges rates for the aforementioned estimators are established. In particular it is shown that for $f \in BL(\Omega)$ we have $MISE(\hat{f}_n) = O(n^{-r/(r+1)})$ and $MISE(\tilde{f}_n) = O(n^{-2(2r+1)/(5r+7)})$, where the index $r \geq 1$ defines the decay of band-limited signals at $\pm\infty$. The rate of convergence for $\tilde{f}_n$ is valid for all positive weight sequences $\{w_i\}$.

References

[1] R. Higgins. *Sampling Theory in Fourier and Signal Analysis.* Calrendon Press, Oxford, 1996.

[2] A. Krzyzak, E. Rafajlowicz and M. Pawlak. Moving average algorithms for band-limited signal recovery. *IEEE Trans. Signal Processing*, **45**, 2967–2976, 1997.

[3] M. Pawlak and U. Stadtmüller. Recovering band-limited signals under noise. *IEEE Trans. Information Theory*, **42**, 1425–1438, 1996.

[4] M. Unser and I. Daubechies. On the approximation power of convolution-based least squares versus interpolation. *IEEE Trans. Signal Processing*, **45**, 1697–1711, 1997.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Linear Almost-Periodically Time-Variant Filtering of Generalized Almost-Cyclostationary Signals

Luciano Izzo Antonio Napolitano
Dipartimento di Ingegneria Elettronica e delle Telecomunicazioni
Università di Napoli Federico II
via Claudio 21, I-80125 Napoli, Italy
e-mail: izzoluc@unina.it antnapol@unina.it

Abstract — **In this paper, the linear almost-periodically time-variant (LAPTV) filtering of generalized almost-cyclostationary (GACS) signals is considered in the fraction-of-time probability framework. It is shown that in general GACS signals, when processed by LAPTV filters, deliver output signals with zero power.**

I. Introduction

Very recently, a class wider than that of the almost-cyclostationary (ACS) signals has been introduced and characterized [2]. Signals belonging to this class are called generalized almost-cyclostationary (GACS) and exhibit multivariate statistical functions that are almost-periodic functions of time whose Fourier series expansions have coefficients and frequencies that can depend on the lag shifts of the signals. Moreover, the union over all the lag shifts of the lag-dependent frequency sets is not necessarily countable. The GACS signals have been characterized in [2] in both time and frequency domains in terms of generalized cyclic statistics.

In this paper, the linear almost-periodically time-variant (LAPTV) filtering of GACS signals is considered in the fraction-of-time (FOT) probability framework [1] in which statistical parameters are defined through infinite-time averages of a single time-series rather than ensemble averages of a stochastic process.

II. LAPTV filtering of GACS signals

Let us consider the impulse-response funcion of a LAPTV system

$$h(t,u) = \sum_{\sigma\in\Omega} h_\sigma(t-u)\, e^{j2\pi\sigma u}\,, \qquad (1)$$

where Ω is the set of the frequency shifts introduced by the system. It can be shown that the Nth-order temporal moment function (TMF) of the output $y(t)$, that is, the almost-periodic component contained in the Nth-order lag product of $y(t)$, is given by

$$\mathcal{R}_{\boldsymbol{y}}(\mathbf{1}t+\boldsymbol{\tau}) = \sum_{\boldsymbol{\sigma}\in\Omega^N} e^{j2\pi\boldsymbol{\sigma}^{\mathsf{T}}(\mathbf{1}t+\boldsymbol{\tau})}\, \mathcal{D}_{\boldsymbol{x},\boldsymbol{\sigma}}(\mathbf{1}t+\boldsymbol{\tau})\,, \qquad (2)$$

where

$$\mathcal{D}_{\boldsymbol{x},\boldsymbol{\sigma}}(\mathbf{1}t+\boldsymbol{\tau}) \triangleq \int_{\mathbb{R}^N} \prod_{n=1}^{N} H_{\sigma_n}(\lambda_n+\sigma_n)\, \mathcal{S}_{\boldsymbol{x}}(\boldsymbol{\lambda}) e^{j2\pi\boldsymbol{\lambda}^{\mathsf{T}}(\mathbf{1}t+\boldsymbol{\tau})}\, \mathrm{d}\boldsymbol{\lambda}. \qquad (3)$$

In (2) and (3), $\mathbf{1} \triangleq [1,\cdots,1]^{\mathsf{T}}$, $H_\sigma(f)$ is the Fourier transform of $h_\sigma(t)$, and $\mathcal{S}_{\boldsymbol{x}}(\boldsymbol{\lambda})$ is the Nth-order spectral moment function of the input signal $x(t)$, that is, the N-fold Fourier transform of the Nth-order TMF.

It can be shown that if $h_\sigma(t) \in L^2(\mathbb{R})$ and $x(t)$ is a GACS signal not containing any ACS component, then $\mathcal{D}_{\boldsymbol{x},\boldsymbol{\sigma}}(\mathbf{1}t+\boldsymbol{\tau})$ is infinitesimal as $\|\boldsymbol{\tau}\| \to \infty$ and then, as $|t| \to \infty$. Therefore, $\mathcal{D}_{\boldsymbol{x},\boldsymbol{\sigma}}(\mathbf{1}t+\boldsymbol{\tau})$, as function of t, is a function with zero power so that the product $\mathcal{D}_{\boldsymbol{x},\boldsymbol{\sigma}_1}(\mathbf{1}t+\boldsymbol{\tau}_1)\mathcal{D}_{\boldsymbol{x},\boldsymbol{\sigma}_2}(\mathbf{1}t+\boldsymbol{\tau}_2)$ does not contain any additive sinewave component. Thus, the TMF (2) of any order N is zero in the temporal mean-square sense, that is, the output signal has zero power. Moreover, it results that the output TMF can be not identically zero only if the input time-series contains ACS components (in which case the output time-series is ACS), unless some function $h_{\sigma_n}(\cdot)$ contains impulsive terms, as in the case of systems introducing constant time delays or frequency shifts.

Some limitations in the applicability of (higher-order) cyclostationarity-based signal processing algorithms arise, when the increasing of the collect time makes the GACS model more appropriate than the ACS one, since possible time variations of timing parameters of the signals must be taken into account. In fact, in such a case, (generalized) cyclic statistic estimates of the output signal are asymptotically zero when the collect time approaches infinity. Therefore, there exists an upper limit to the maximum usable collect time and, consequently, there exists a limit to the minimum acceptable signal-to-noise ratio for cyclostationarity-based algorithms which are, in principle, under mild assumptions, intrinsically immune to the effects of noise and interference, provided that the collect time approaches infinity.

The identically zero (generalized) cyclic statistics of the LAPTV filtered GACS signals are consequence of the properties of the single observed time-series (e.g., the possible time variation of a timing parameter, such as the carrier frequency or the baud rate). In contrast to this, statistic functions of a stochastic process can be identically zero as a consequence of the presence, in the stochastic process model, of a random parameter whose effect is to make the statistical expectations equal to zero. In such a case, however, in general the stochastic process is not ergodic. Therefore, the FOT probability framework is very actractive due to the equivalence between theoretical statistical functions and their asymptotic estimates.

References

[1] W.A. Gardner, "An introduction to cyclostationary signals," in *Cyclostationarity in Communications and Signal Processing*, W.A. Gardner, Ed., pp. 1-90, IEEE Press, New York, 1994.

[2] L. Izzo and A. Napolitano, "The higher-order theory of generalized almost-cyclostationary time-series," *IEEE Trans. Signal Processing*, vol. 46, pp. 2975-2989, November 1998.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Sphere Decoding of Space-Time Codes

Oussama Damen
Ecole Nationale Supérieure
des Télécommunications de Paris
46 rue Barrault, 75634 Paris
e-mail: mdamen@com.enst.fr

Ammar Chkeif
Ecole Nationale Supérieure
des Télécommunications de Paris
46 rue Barrault, 75634 Paris
e-mail: chkeif@tsi.enst.fr

Jean-Claude Belfiore
Ecole Nationale Supérieure
des Télécommunications de Paris
46 rue Barrault, 75634 Paris
e-mail: belfiore@com.enst.fr

Abstract — **We explore in this paper the lattice sphere packing representation of a multi-antenna system and the algebraic space-time (ST) codes. We apply the sphere decoding (SD) algorithm to the resulted lattice code. For the uncoded system, SD yields, with small increase in complexity, a huge improvement over the well-known V-BLAST detection algorithm. SD of algebraic ST codes exploits the full diversity of the coded multi-antenna system, and makes the proposed scheme very appealing to take advantage of the richness of the multi-antenna environment. The fact that the SD does not depend on the constellation size, gives rise to systems with very high spectral efficiency, maximum likelihood (ML) performance, and low decoding complexity.**

I. Introduction

Recently, the field of multi-antenna processing and space-time (ST) coding has attracted large interest in the communication community due to the huge capacity of the multi-antenna environment [1]. Because of the maximum likelihood (ML) detection high complexity sub-optimal detection like the V-BLAST have been proposed for the uncoded system [2].

In this paper, we prove that one can reach the ML performance of the uncoded system with low complexity by applying the sphere decoder [3] on the lattice sphere packing representation of a multi-antenna system. Moreover, it is shown that one can achieve the full diversity of the multi-antenna system by using full spatial diversity rotated constellations without adding redundancy [4], and still reach the ML performance with reasonable complexity.

II. Simulation Results

In simulations we use the constellation q-QAM, with $q = 4$, 16. The average energy per bit is fixed to $\bar{E}_b = 1$. We consider a multi-antenna system with M transmitters and $N = M$ receivers. The algebraic coding is done over l periods by using rotated constellations of dimension Ml. The channel transfer matrix is modeled by independent complex Gaussian random variables of variance 0.5 per real dimension. The curves are plotted as a function of SNR (the signal-to-noise ratio per bit), and the variance σ^2 of the complex AWGN per real dimension is adjusted by the formula $\sigma^2 = \frac{M\bar{E}_s}{2\log_2(q)}10^{-SNR/10}$, where $\bar{E}_s$ is the average symbol energy of the q-QAM when $\bar{E}_b = 1$ and equals $\frac{2(q-1)}{3}$. In figures 1 and 2 we applied the SD on both uncoded data streams and algebraic ST codes over l periods with $M = N$ transmit/receive antennas [4]. Comparisons are done with the V-BLAST detection algorithm [2]. It is shown that at the expense of a moderate increase in complexity, a huge improvement in performance is achieved.

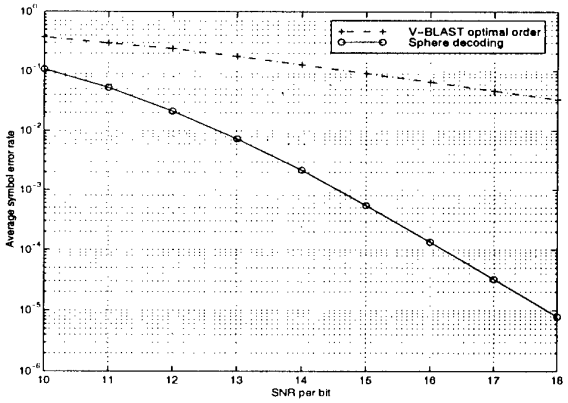


Fig. 1: SD of V-BLAST architecture, $M = N = 8$, average symbol error rate of the 16-QAM modulation, 32 bits/s/Hz.

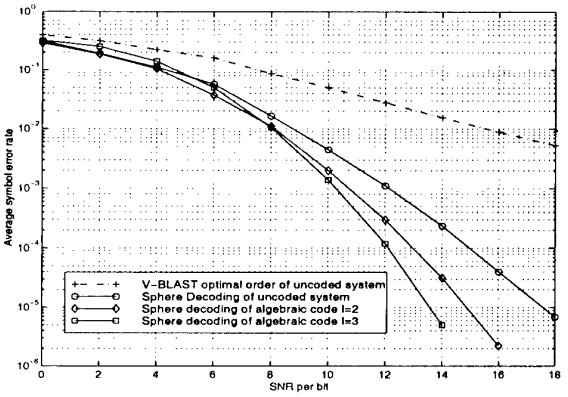


Fig. 2: SD of algebraic ST codes, $M = N = 4$, average symbol error rate of the 4-QAM modulation, 8 bits/s/Hz, $l = 1, 2, 3$.

References

[1] V. Tarokh, N. Seshadri and A. Calderbank, "Space-time codes for high data rate wireless communications: performance criterion and code construction," *IEEE Trans. on Inf. Theory* , vol. 44, pp. 744–765, Mar. 1998.

[2] G. Golden, C. Foschini, R. Valenzuela and P. Wolniasky, "Detection algorithm and initial laboratory results using V-BLAST space-time communication architecture," *Elec. Lett.* , vol. 35, Jan 1999.

[3] E. Viterbo and J. Boutros, "A universal lattice code decoder for fading channel," *IEEE Trans. on Inf. Theory* , vol. 45, pp. 1639–1642, July 1999.

[4] M. O. Damen, Joint Coding/Decoding in a Multiple Access System, Application to Mobile Communications. PhD thesis, ENST de Paris, "http://www.enst.fr/~mdamen", Oct. 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Space-Time Cut-off Rate for the Flat Rayleigh Fading Channel

Alfred O. Hero[1]
Dept. EECS
University of Michigan
1301 Beal Avenue
Ann Arbor, MI 48109-2122 USA
hero@eecs.umich.edu

Thomas L. Marzetta
Mathematical Sciences Research Center
Bell Laboratories
Lucent Technologies
600 Mountain Avenue
Murray Hill, NJ 07974 USA
tlm@research.bell-labs.com

Abstract — **The computational cut-off rate is studied for the complex Rayleigh flat fading spatio-temporal channel under a peak power constraint. Any optimal finite constellation of signals must admit an equalizer distribution which equalizes the conditional decoding error probabilities. For small constellations the set of equiprobable mutually-orthogonal unitary matrices attains cut-off rate. For low SNR these matrices are rank one and a single transmit antenna is as good as multiple antennas.**

I. Introduction

There are M transmitter antennas and N receiver antennas and the MN channel fading coefficients are i.i.d. constant complex Gaussian over the coherent fade interval of length T time periods [2]. While the SNR η is known the fading coefficients are unknown to both transmitter and receiver. In a frequency hop system each coherent fade interval corresponds to a different frequency band. A baseband transmitted signal S_i is a $T \times M$ matrix having complex valued entries. When the S_i's are drawn from a constellation of K possible signals the signalling rate is K/T symbols/sec/hz. The computational cut-off rate specifies the maximum practical rate that can be supported by the channel and is often simpler to calculate than channel capacity. For more details on the following results see [1].

II. Cutoff Rate Representations

For any K-dimensional constellation $\{S_1, \ldots, S_K\}$ define the $K \times K$ *dissimilarity matrix* $E_K = \left(\left(e^{-ND(S_i\|S_j)}\right)\right)_{i,j=1}^{K}$ where

$$D(S_i\|S_j) \stackrel{\text{def}}{=} \frac{1}{2}\log \frac{\left|I_T+\frac{\eta}{2}(S_iS_i^H+S_jS_j^H)\right|^2}{\left|I_T+\eta S_iS_i^H\right|\left|I_T+\eta S_jS_j^H\right|}.$$

is a pairwise distance function between signal matrices in the constellation.

Proposition 1 *[1] Let $\tilde{R}_o(K)$ denote the peak power constrained cut-off rate restricted to K-dimensional constellations. Then*

$$\tilde{R}_o(K) = \log\left\{\max_{0<k\le K}\max_{\{S_i\}_{i=1}^k \in \tilde{\mathcal{S}}_{\text{peak}}^k} \underline{1}_k^T E_k^{-1}\underline{1}_k\right\}.$$

where $\tilde{\mathcal{S}}_{\text{peak}}^K$ is the set of K-dimensional peak constrained constellations for which there exists an "equalizer probability vector" $\underline{P}_K$ satisfying $E_K\underline{P}_K = c\underline{1}_k$ for some $c > 0$.

III. Optimality of Unitary Orthogonal Matrices

For given η, T and M define the integer M_o

$$M_o = \text{argmax}_{m\in\{1,\ldots,M\}}\left\{m\log\frac{(1+\eta TM/(2m))^2}{1+\eta TM/m}\right\}. \quad (1)$$

and

$$D_{\max} \stackrel{\text{def}}{=} \max_{S_1,S_2\in\mathcal{S}_{\text{peak}}^K} D(S_1\|S_2) = M_o\log\frac{(1+\eta TM/(2M_o))^2}{1+\eta TM/M_o}.$$

$D_{\max}$ is the maximum value of the minimum distance achievable by any constellation of dimension $K \le T/M_o$.

Proposition 2 *[1] Let $2M \le T$ and let M_o be as defined in (1). Suppose that $M_o \le \min\{M, T/K\}$. Then*

$$\tilde{R}_o(K) = \log\left(\frac{K}{1+(K-1)e^{-ND_{\max}}}\right)$$

and $D_{\max}$ is given by (2). Furthermore, the optimal constellation attaining $\tilde{R}_o(K)$ is the set of K equiprobable rank M_o mutually orthogonal unitary matrices: $S_i^HS_i = I_{M_o}$ and $S_i^HS_j = 0$, $i \ne j$.

The rank M_o of the matrices in the optimal constellation increases from 1 to M as the SNR parameter ηTM increases from 0 to ∞. If SNR is sufficiently large, e.g. for $M = 6$ and $T \ge 12$ if $\eta TM \ge 17$, then $M_o = M$ and the optimal signal matrices utilize all M transmit antennas. On the other hand for small SNR, e.g. $\eta TM < 4$, then $M_o = 1$ and the optimal signal matrices apply all available transmit power to a single antenna element over each coherent fade interval.

References

[1] A. O. Hero and T. L. Marzetta, "On computational cut-off rate for space time coding," Technical memo, Bell Laboratories, Lucent Technologies, Murray Hill, NJ, 2000.

[2] T. L. Marzetta and B. M. Hochwald, "Capacity of a mobile multiple-antenna communication link in Rayleigh fading," *IEEE Trans. on Inform. Theory*, vol. IT-45, pp. 139–158, Jan. 1999.

[1]This research was performed, in part, while the first author was visiting the Mathematical Sciences Research Center, Bell Laboratories, Lucent Technologies

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Sphere Packing in the Grassmann Manifold: A Geometric Approach to the Noncoherent Multi-Antenna Channel

Lizhong Zheng, David N.C. Tse[1]
Department of EECS
University of California
Berkeley, CA94720 USA
email:{lzheng,dtse}@eecs.berkeley.edu

Abstract — **In this paper, we study the capacity of multi-antenna channel where the fading coefficients are unknown to either transmitter or receiver. The high SNR channel capacity is computed, and a geometric interpretation of sphere packing in Grassmann manifold is given.**

I. Introduction

Recent research has shown that by using multiple antennas at both the transmitter and the receiver, the spatial diversity provides much larger spectral efficiency than the conventional channels. In contrast of the single antenna AWGN channel, where 1 bps/Hz capacity gain can be achieved with every $3dB$ increase in SNR, in a channel with N transmit and N receive antennas, it is shown that the corresponding capacity is gain is N bps/Hz. [1]

The result above is derived under the key assumption that the instantaneous fading coefficients are known or precisely estimated at the receiver end. In practical applications, especial mobile systems, the fading coefficients can change quite rapidly and the precise estimation of the channel parameters becomes difficult. In this paper, we will study the channel capacity with no assumption on the prior knowledge of the fading coefficients to understand the fundamental limit of *noncoherent* multi-antenna communications.

II. System Model

We will use the same model given in [2]. Assume the system has N transmit and N receive antennas. The propagation coefficients between all antenna pairs form a $N \times N$ random matrix $\mathbf{H}$ with iid $CN(0,1)$ entries. $\mathbf{H}$ is unknown to the transmitter and receiver. To approximate the continuously varying coefficients, we assume that $\mathbf{H}$ remains constant for T symbol periods, and change to new independent realizations afterwards. The time period that $\mathbf{H}$ remains constant will be referred as *coherence interval*, and T referred as *coherence time*. The channel in each coherence interval can thus be written as

$$\mathbf{Y} = \mathbf{HX} + \mathbf{W}$$

where $\mathbf{X}, \mathbf{Y} \in \mathcal{C}^{N\times T}$ are the transmitted and received signals, respectively. $\mathbf{W} \in \mathcal{C}^{N\times T}$ is the additive white Gaussian noise. The SNR at each receive antenna is denoted as ρ.

The goal of this paper is to compute the capacity of this channel at high SNR, $\rho \to \infty$. In [2], it is shown that increasing the number of antennas N beyond T provides no capacity gain. Therefore in this paper, we will only consider the case where $N \leq T$.

[1]This research is supported by a National Science Foundation Early Faculty CAREER Award and by DARPA grant F30602-97-2-0346.

III. Channel Capacity

To approach this problem, we need to introduce the following new coordinate system. A $N \times T$ matrix R with $N \leq T$, can be represented as the N dimensional subspace Ω_R spanned by the row vectors, together with a $N \times N$ matrix C_R which specifies the N row vectors of R with respect to a prescribed basis in Ω_R. The transformation

$$R \to (C_R, \Omega_R)$$

is a change of coordinate system: $\mathcal{C}^{N\times T} \to \mathcal{C}^{N\times N} \times G(T,N)$. Here $G(T,N)$ is the Grassmann manifold defined as the set of all N dimensional subspaces of $\mathcal{C}^T$.

The motivation of using this new coordinate system is that the transmitted subspace is not corrupted by the fading coefficients, $\Omega_{\mathbf{HX}} = \Omega_{\mathbf{X}}$. Therefore,the new coordinates decompose $\mathcal{C}^{N\times T}$ into the directions that affected by both fading and additive noise and those directions affected by noise alone. In this new coordinate system, the relevant differential entropies can be computed, and the optimization problem can be solved more easily.

Theorem 1 *For system with N transmit and receive antennas, if the coherence time $T \geq 2N$, the high SNR channel capacity (bps/Hz) is given by*

$$\begin{aligned} C(\rho) &= \frac{1}{T}\log_2|G(T,N)| + (1-\frac{N}{T})E[\log_2\det(\mathbf{HH}^\dagger)] \\ &\quad + N(1-\frac{N}{T})\log_2\frac{T\rho}{N\pi e} + o(1) \end{aligned}$$

where $|G(T,N)|$ is the volume of Grassmann manifold $G(T,N)$, and $E[\log\det\mathbf{HH}^\dagger] = \sum_{i=1}^{N} E\log\chi^2_{2i}$ for χ^2_{2i} chi-square distributed with dimension $2i$.

This capacity is asymptotically achieved by the constant equal norm input $P(\mathbf{A} = \sqrt{T}I_N) = 1$. Under this input, one can show that all the mutual information is carried by the random subspace $\Omega_{\mathbf{X}}$, which lies in the Grassmann manifold $G(T,N)$ with dimension $N(T-N)$. Therefore, the number of degrees of freedom available to communicate non-coherently is $N(T-N)$ per T symbol time. The capacity gains $N(1-N/T)$ bps/Hz for each $3dB$ SNR increase.

The capacity result above can also be interpreted as sphere packing in Grassmann manifold.

References

[1] G. J. Foschini, "Layered space-time architecture for wireless communication in a fading environment when using multi-element antennas," *Bell Labs Technical Journal.* , vol. 1, no. 2, pp. 41-59, 1996;

[2] T.Marzetta and B. Hochwald, "Capacity of mobile multiple-antenna communication link in a Rayleigh flat-fading environment," *IEEE Trans. on Info. Theory,* vol. 45, no. 1, pp.139-57, 1999

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Multiple-Antenna Signal Constellations for Fading Channels

Dakshi Agrawal
Coordinated Science Laboratory
University of Illinois–Urbana-Champaign
Urbana, IL 61801, USA
email: dakshi@csl.uiuc.edu

Thomas J. Richardson
Bell Labs
Lucent Technologies
Murray Hill, NJ 07974, USA
email: tjr@lucent.com

Rüdiger Urbanke
Communication Lab
Ecole Polytechnique Federale de Lausanne
Lausanne, Switzerland CH-1015
e-mail: ruediger.urbanke@epfl.ch

Abstract — **In this paper, we design multiple-antenna signal constellations for a Rayleigh flat-fading channel unknown to the receiver. It is shown that good signal constellations correspond to packings with large minimum distances in complex Grassmannian space. We describe a numerical optimization procedure for finding such packings. The corresponding signal constellations improve significantly upon previously best-known signal constellations.**

I. Introduction

This paper concerns with the design of unitary space-time constellations [2] for an M transmit-antenna communication system operating in a Rayleigh flat-fading environment. Assume that the fading coefficients among different pairs of transmit and receive antennas are statistically independent and are unknown to the receiver. The fading coefficients remain constant for a *coherence interval* of T symbol periods, and then change simultaneously to independent realizations. A unitary space-time constellation of cardinality L is a collection of L complex orthonormal matrices of size $T \times M$, where the i-th column of each matrix contains symbols transmitted over a coherence interval through the i-th transmit antenna.

We show that for a small number of transmit antennas, the pairwise probability of error between two distinct signal points, Φ_1 and Φ_2, of a unitary space-time constellation is related to the correlation $\langle \Phi_1^* \Phi_2, \Phi_1^* \Phi_2 \rangle$, where $\langle A, B \rangle = \sum_{j,k} A_{jk} B_{jk}^*$. Thus, the maximum correlation between two distinct signal points can be used as a *figure of merit* and the problem of finding good unitary space-time constellations can be stated as follows:

Unitary space-time constellation design problem: Given natural numbers T, M, and L, with $M < T$, find a collection $S = \{\Phi_1, \Phi_2, \ldots, \Phi_L\}$ of $T \times M$ complex orthonormal matrices such that the maximum correlation, given by

$$\sigma^*(S) := \max_{1 \leqslant i < j \leqslant L} \langle \Phi_i^* \Phi_j, \Phi_i^* \Phi_j \rangle \qquad (1)$$

is minimized. ⋄

II. Complex Grassmannian Space

The complex Grassmannian space $\mathcal{G}(T, M, \mathbb{C})$ is the set of all M-dimensional subspaces of $\mathbb{C}^T$. Let Φ_1, Φ_2 be two $T \times M$ complex orthonormal matrices whose column spaces are $P_1, P_2 \in \mathcal{G}(T, M, \mathbb{C})$ respectively. The squared distance between P_1 and P_2 can be defined as

$$d^2(P_1, P_2) = T - \langle \Phi_i^* \Phi_j, \Phi_i^* \Phi_j \rangle'$$

We refer to a finite subset of the complex Grassmannian space $\mathcal{G}(T, M, \mathbb{C})$ as a *packing* in $\mathcal{G}(T, M, \mathbb{C})$ The squared minimum distance $d^2(S)$ of a packing S is given by

$$d^2(S) = \min_{\substack{P_i, P_j \in S \\ P_i \neq P_j}} d^2(P_i, P_j) \qquad (2)$$

From (1) and (2), it follows that the problem of designing good unitary space-time constellations is the same as the problem of finding packings in complex Grassmannian space that have large minimum distances.

III. Optimization Technique

Since the complex Grassmannian space $\mathcal{G}(T, M, \mathbb{C})$ is a differentiable manifold, parameters involved in the optimization problem given by (1) lie in a differential manifold. Thus, one can consider the direct minimization of $\sigma^*(S)$ using gradient search algorithms. Unfortunately, $\sigma^*(S)$ has many local minima that are far away from the global minima. Moreover, $\sigma^*(S)$ is not very smooth—in fact, it is not even differentiable everywhere.

In order to circumvent these difficulties, we introduce a family of *potential functions* $f_\alpha(S)$ with the following properties: For all α the functional f_α is smooth; for small values of α the functional f_α has few local minima; the functionals f_α mimic σ^*, as $\alpha \to \infty$.

The search procedure starts with a relatively small value of α, say α_0, and a randomly generated unitary space-time constellation S. It uses numerical optimization techniques to find a set S_{α_0} such that the value of f_{α_0} is (nearly) locally minimized. Next, we slightly increase α to α_1 and starting from the set S_{α_0}, find a new set S_{α_1} that (nearly) locally minimizes f_{α_1}. We continue in this manner, each time increasing the value of α slightly and tracking the minimizer of f_α. For very large values of α, f_α would be essentially equivalent to σ^* and minimizing f_α will also essentially minimize σ^*.

IV. Results

Using the numerical technique described above, we generate unitary space-time constellations of cardinality 2^T for $M = 1, 2, 3$ and $T = 5, 6, \ldots, 10$ [1]. In all cases, these constellations improved upon previously best known constellations [3]. The unitary space-time constellations generated here can be used as a benchmark to assess the optimality of other signal constellations designed subjected to constraints such as the ability to 'easily encode and decode'.

References

[1] D. Agrawal, T. Richardson, and R. Urbanke, "Multiple-antenna signal constellations for fading channels," submitted to *IEEE Trans. Info. Theory.*

[2] B. M. Hochwald and T. L. Marzetta, "Unitary space-time modulation for multiple-antenna communications in Rayleigh Flat Fading," *IEEE Tran. Info. Theory*, vol. 46, pp. 543–564, March 2000.

[3] B. Hochwald, T. Marzetta, T. Richardson, W. Sweldens, and R. Urbanke, "Systematic design of unitary space-time constellations," submitted to *IEEE Trans. Info. Theory.*

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Extending the Evaluation of Serial Concatenated Turbo Code Performance to Longer Block Lengths

Andrew J. Viterbi and Audrey M. Viterbi
Viterbi Group, LLC
viterbi@pacbell.net

SUMMARY

As new classes of iteratively decodable very long block-length codes are discovered, they appear to have the potential of achieving extremely low error probabilities close to the Shannon limit. While the degree to which the suboptimal iterative decoding process degrades this performance is not yet well determined, progress has occurred in establishing the optimal maximum likelihood performance.

Following the approaches of [1] and [2], we obtain that for arbitrarily long block lengths on a Gaussian channel, vanishingly low error probabilities can be achieved by maximum likelihood decoding provided

$r(d)<K(Es/No,d)$ for $0<d<1$

where r(d) is the code "rate-weight function", which is the normalized logarithm of the ensemble average number of codewords of normalized distance d, and K(Es/No,d) is a function only of the channel parameters. We have evaluated K( ) for the SNR range of interest. For certain serial-concatenated and accumulated-convolutional codes [3], r(d) has been approximated, from which the closeness of the code's performance to the Shannon limit can be estimated.

REFERENCES:

1. A.M. Viterbi and A.J. Viterbi, "Improved Union Bound on Linear Codes for the Input-Binary AWGN Channel, with Applications to Turbo Codes", IEEE International Symposium on Information Theory, Cambridge MA, August, 1998

2. S. Aji, H. Jin, R.J. McEliece and D.J.C. MacKay, "BSC Thresholds for Code Ensembles based on "Typical Pairs" Decoding", Unpublished Memorandum

3. A.M. Viterbi and A.J. Viterbi, "New Results on Serial Concatenated and Accumulated-convlutional. Turbo Code Performance", Annals of Telecommunications, Vol. 54, pp.173-182, March-April,1999

0-7803-5857-0/00/$10.00 ©2000 IEEE.

An Interactive Concatenated Turbo Coding System[1]

Ye Liu
Datapath System Inc.

Heng Tang and Shu Lin
University of California, Davis

Marc Fossorier
University of Hawaii, USA

I. Introduction

Although turbo codes with iterative decoding have been shown to achieve bit-error rates (BER's) close to the Shannon limit, they suffer from three disadvantages: a large decoding delay, an error floor at low BER's, and a relatively poor frame error performance (FER). This paper presents an *interactive concatenated turbo coding system* in which a Reed-Solomon outer code is concatenated with a binary turbo inner code. In the proposed system, the outer code decoder and the inner turbo code decoder *interact* to achieve both good bit error and frame error performances. Also presented in the paper are an effective criterion for stopping the iterative decoding process and a new reliability-based decoding algorithm called *Chase-GMD algorithm* for nonbinary codes.

II. The Chase-GMD Decoding Algorithm

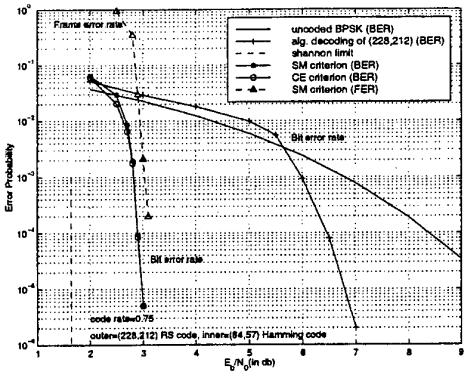
The Chase-GMD decoding algorithm is a reliability-based decoding algorithm which combines Chase-2 and GMD algorithms. Consider an (n_o, k_o, d) RS code over GF(q) with $q = 2^m$. Let $\mathbf{y}$ be the received sequence and $\mathbf{z}$ be the hard-decision received sequence. Without loss of generality, we assume that the hard-decision received symbols in $\mathbf{z}$ are ordered in the order of increasing reliability. We also assume that an error-and-erasure algebraic decoder is used to generate candidate codewords. For $0 \leq P \leq \lfloor d/2 \rfloor$, let E denote the set of test error patterns with errors (nonzero components) confined to the P least reliable positions. Let $A_i(q')$ denote the set of $q' \leq q$ most probable symbols in GF(q) at the i-th symbol position, $0 \leq i < P$. The error at the i-th position of E is chosen from $A_i(q')$. Let CGA(P, q') denote the Chase-GMD algorithm with parameter P and q'. This CGA(P, q') processes all the vectors $\mathbf{w} = \mathbf{z} + \mathbf{e}$ with $\mathbf{e}$ in E. Let $I(P) = \{i : \ 0 \leq i \leq d - 2P - 1$ and $d - i$ is odd$\}$. For each $\mathbf{w}$ and each integer $i \in I(P)$, erase i symbols of $\mathbf{w}$ starting from symbol position $P+1$ to symbol position $P+i$. This results in a vector $\mathbf{w}^*$ with i erasures. Perform error-and-erasure decoding on $\mathbf{w}^*$. If decoding is successful, the decoded codeword is a candidate codeword. After performing $q'^P(\lfloor (d+1)/2 \rfloor - P)$ decodings, we obtain a set of candidate codewords. Among these candidate codewords, the one with the best metric is the decoded codeword. The performance of CGA(P, q') improves as P increases.

III. A Concatenated Turbo Coding System

To construct a concatenated turbo coding system, a turbo code with two block component codes is chosen as the inner code, and an (n_o, k_o, d) RS code over GF(2^m) is chosen as the outer code. At the decoder, the received sequence is first turbo decoded in parallel mode[1], i.e., two component code decoders operate simultaneously. At the each phase of a decoding iteration, two decoders produce two decoded information sequences, each segmented into λ vectors with n_o symbols over GF(2^m). Then, compare each pair of corresponding vectors from the two turbo decoders, and check how many symbol positions where two corresponding symbols do not match. If the number of mismatched symbol positions for each pair of corresponding n_o-vectors is less than or equal to the error correcting capability of the outer RS code, $\lfloor (d-1)/2 \rfloor$, we stop the inner turbo decoding iteration and let the outer code decoder with algebraic decoding to take over and complete the decoding process. This new stopping criterion for inner turbo decoding is called *symbol matching (SM) criterion.* It saves more decoding iterations and requires much less computational complexity than the cross-entropy (CE) criterion in [2]. If the outer code decoding is not successful (decoding failure), the outer code decoder instructs the inner turbo decoder to continue its decoding iterations from the phase where it was stopped until the symbol errors at the input of the outer decoder is reduced within the error correction capability of the outer code. The interactive process continues until either the outer decoding is successful or a preset maximum number of decoding iterations for the inner turbo decoder is reached. In the latter case, the outer code decoder computes the reliability values of its input symbols based on the soft output information (log-likehood ratios of the decoded bits) of inner turbo code decoder and carries out the reliability-based CGA(p, q') decoding.

IV. Simulation Results

Consider a concatenated turbo coding system in which the (228, 212) shortened RS code over GF(2^8) is used as the outer code and the (64,57) distance-4 extended Hamming code is used as the two component codes for constructing the inner turbo code. The rate of this system is R=0.75. The bit-error and frame-error performances of this system for AWGN channel are shown below. We see the waterfall performance without error floor. It is 1.3 dB away from Shannon limit.



References

[1] D. Divsalar *et. al.*, "Turbo Codes for PCS Applications," *Proc. of ICC'95.*

[2] J. Hagenauer *et. al.*, "Iterative Decoding of Binary Block and Convolutional Codes," *IEEE Trans. on IT*, March 1996.

[1]This research was supported by NSF under Grants NCR 94-15374, CCR 97-32959, CCR 98-14054 and NASA under Grants NAG 5-931 and NAG 5-8414.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Simultaneous zero-tailing of parallel concatenated codes

Marten van Dijk, Sebastian Egner, Ravi Motwani, Arie Koppelaar
Philips Research Laboratories
Prof. Holstlaan 4, 5656 AA Eindhoven, The Netherlands
Email : marten.van.dijk,sebastian.egner,ravi.motwani,aric.koppelaar@philips.com

Abstract — **In a parallel concatenated convolutional code (pccc) an information word is encoded by a first convolutional encoder and an interleaved version of the information word is encoded by a second convolutional encoder. We discuss the situation in which we require that both convolutional encoders end in the all zero state. To do so, we have to split the information word in two parts. One part containing information bits, and a second part containing bits, called tail-bits, computed such that both encoders end in the all zero state, which we call simultaneous zero-tailing. Depending on the structure of the interleaver, different number of tail-bits are needed. By using a constructive method we characterize all interleavers for a prescribed number of tail-bits. We explain methods of encoding. In addition simulations have been carried out to investigate the performance of simultaneous zero-tailing. This shows that simultaneous zero-tailing is similar in performance compared with previously known zero-tailing methods and that it is better than zero-tailing just one of the encoders.**

I. Mathematical Characterization

We know that the joint end state $[S_1, S_2]$ of the two encoders is a linear function of the information word I. This linear function depends on the interleaver π used. Moreover, the dimension of the space of end states is between k (fully simultaneous zero-tailing) and $2k$ (fully independent zero-tailing), where k is the memory of both encoders. We have derived a characterization of interleavers with which simultaneous zero-tailing is possible. Our method, being more general, gives a larger class of interleavers than discussed in literature of simultaneous zero-tailing interleavers so far [1, 2].

Using the mathematical characterization we have developed in this work, it is possible to design an interleaver such that the dimension of the space of end states is a given number $k + s$ for any $s \in \{0..k\}$. This characterization can be used in several ways. Given an interleaving permutation one can compute the number of zero-tailing bits that are necessary for simultaneous zero-tailing. Conversely, the characterization allows counting and construction of interleavers with a prescribed number of tail-bits. This construction can be augmented to look for interleavers with large spread [3].

II. Simulation Results

We performed experiments in order to answer the following questions.

1. How does zero-tailing both encoders compare to only one encoder being zero-tailed?
2. How does the simultaneous zero-tailing compare in performance to the zero-tailing strategy proposed for the UMTS standard (both encoders of the pccc are zero-tailed separately)?

Observe that the number of additional bits sent through the channel (tail-bits and their corresponding parity bits) amounts to $4k$ for independent zero-tailing of both encoders (such as in UMTS), whereas our proposal requires between $3k$ and $6k$ bits depending on the interleaver used. We use a pccc with 8-state constituent encoders and an interleaver of size 150 and spread 4 for the simulations. The four schemes compared are **(1)** both encoders are truncated, **(2)** one encoder is zero-tailed and the other is truncated, **(3)** both encoders are zero-tailed using the zero-tailing strategy proposed for the UMTS standard and **(4)** both encoders are zero-tailed using a simultaneous zero-tailing interleaver leading to $3k$ additional bits.

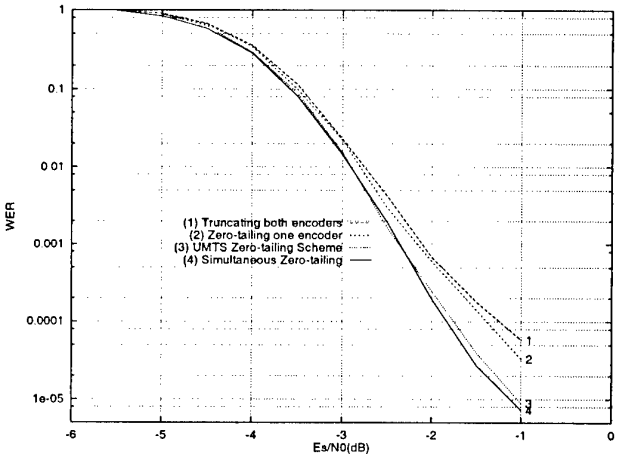


Figure 1: WER for the four schemes discussed for pccc with 8-state constituent codes and interleaver size 150, spread 4.

We have plotted the WER corresponding to the above four experiments for different Signal to Noise Ratios (Figure 1). Simulations show that our method of zero-tailing is comparable in performance to previously known zero-tailing techniques and better than termination strategies in which only one encoder is zero-tailed.

References

[1] M. Breitling, S. Peeters and J. Huber *The Class of Double Terminating Turbo Code Interleavers.* Electronic Letters, Vol. 35, No. 5, March 1999.

[2] ETSI SMG2 UMTS L1 Expert Group *Algebraic interleavers for turbo codes.* CANON CRF, SMG2 UMTS-L1 571/98, Meeting # 8, 9-12 November 1998.

[3] C. Heegard, & S.B. Wicker, *Turbo Coding.* Boston : Kluwer Academic Publishers, 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Performance of Turbo Codes with a Single-Error Correcting BCH Outer Code

Hyun Cheol Kim, Pil Joong Lee

Dept. of Electronics and Electrical Engineering, POSTECH
Pohang, 790-784, Republic of Korea
Email: hckim@oberon.postech.ac.kr, pjl@postech.ac.kr

Abstract — **In this paper, we present a simple method using a single-error correcting BCH outer code in order to improve the performance of turbo codes. It is shown that this method reduces the errors dramatically at moderate-to-high E_b/N_o.**

I. Introduction

Narayanan and Stüber proposed a selective serial concatenation of turbo codes using a double-error correcting BCH outer code to protect the non-zero bit positions in the weight 2 inputs generating many low-weight codewords [1]. In this paper, we present a new method, using a single-error correcting BCH outer code, to protect most of the non-zero bit positions corresponding to low-weight codewords. We show that this method has a simpler decoder, better performance and a smaller loss of code rate compared to the scheme of [1].

II. Turbo Codes with a Single-error BCH Outer Code

The low-weight inputs generating low-weight codewords for a (7, 5) component code and a 512 random interleaver are listed in Table 1. The errors of one frame occur simultaneously in the non-zero bit positions associated with low-weight codewords [2]. So, if we select each one non-zero bit position from each information words associated with low-weight codewords, the number of the error occurring in the selected bit positions is mostly one at moderate-to-high E_b/N_o. For example, 15 bit positions are identified in each group in Table 1 (e.g. 134, 165, 179, 474, 9, 16, 94, 112, 171, 214, 224, 243, 88, 130), and then 11 information bits are encoded by a (15, 11) single-error correcting BCH code. The 15 bits from the BCH code are interposed in the above 15 bit positions. Finally, the encoder encodes the overall information frame using the turbo encoder and transmits the codeword through channel. If the bit errors are not corrected by the iterative decoding of turbo codes, most of them are errors of the non-zero bit positions in Table 1 at moderate-to-high E_b/N_o. So, one of the errors can be found using a single-error correcting BCH decoder. From the error bit position found by the BCH decoder, we can find the other error bit positions by Table 1.

Table 1: Non-zero bit positions generating the codewords of weight less than 10.

Distance (d)	Bit positions in information frame		
6	(134, 137)	(165, 168)	(179, 182)
	(474, 477)	(491, 494)	
8	(9, 18)	(16, 19)	(94, 103)
	(112, 115)	(171, 174)	(214, 217)
	(224, 233)	(243, 252)	
9	(88, 95, 96)	(130, 131, 132)	
	(368, 376, 378)	(453, 460, 464)	
	(476, 478, 483)		

III. Simulation and Discussion

The rate 1/2 turbo code for the simulations consists of two $(7, 5)_8$ RSC codes linked by a length 512 random interleaver. The MAP was used for iterative decoding of turbo codes. BPSK modulation and AWGN channel were also assumed. For the outer code, a (31, 21) double-error correcting BCH code and a (63, 57) single-error correcting BCH code were used. The proposed scheme (1-BCH turbo) was simulated using fewer parity bits than the scheme of [1] (2-BCH turbo). Fig. 1 shows that the turbo code using a BCH outer code is superior to the original turbo code (turbo) at moderate-to-high E_b/N_o. The proposed scheme shows a performance improvement of 0.75 dB compared to the original turbo code and 0.15 dB compared to the scheme of [1] at BER 10^{-6}. The FER performance improvement is 1.00dB compared to the original turbo code and 0.20dB compared to the scheme of [1] at FER 10^{-4}.

The proposed scheme has only a slight reduction of code rate due to protection of many non-zero bit positions by small parity bits. Moreover, the proposed scheme has an advantage of protecting the non-zero bit positions in information frames of weight greater than 2. Due to these two characteristics, the proposed scheme is superior to the scheme of [1] in performance. Since single-error correcting BCH codes have very simple decoding structure, the complexity of decoder and decoding time are reduced.

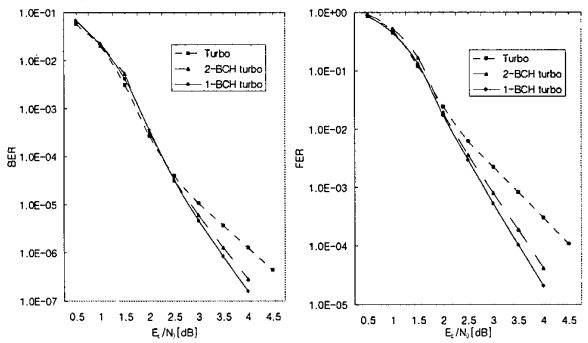


Fig. 1: The performance of the original turbo code and the turbo code with the BCH outer codes after 7 iterations.

References

[1] K. R. Narayanan, G. L. Stuber, "Selective serial concatenation of turbo codes," *IEEE Communication Letters*, pp.136-140, Sept. 1997.

[2] L. Perez, J. Seghers, D. J. Costello Jr., "A distance spectrum interpretation of turbo codes," *IEEE Trans. Inform. Theory*, vol. 42, no. 6, pp. 1698-1709, November 1996.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Asymptotic Average Redundancy of Huffman (and Shannon-Fano) Block Codes

Wojciech Szpankowski[1]
Department of Computer Science
Purdue University
W. Lafayette, IN 47907
U.S.A.
spa@cs.purdue.edu

Recall that Huffman code is an iterative algorithm built over the associated Huffman tree, in which the two nodes with lowest weights are combined into a new node with a weight that is the sum of the weights of its two children. Such a construction is not unique but fortunately with a simple modification to the Huffman algorithm, it is possible to construct a unique Huffman code so that the longest code words are as short as possible (cf. [6]). Hereafter, we deal with such modified Huffman codes and present a precise asymptotic results on the average redundancy of such codes for memoryless sources.

Given a probabilistic source model, we let $P(x_1^n)$ be the probability of the message $x_1^n \in \mathcal{A}^n$. For a code C_n, we denote by $L(C_n, x_1^n)$ the code length for x_1^n. The *average redundancy* $\bar{R}_n(C_n, P)$ is defined as

$$\bar{R}_n(C_n) = \mathbf{E}_{X_1^n}[R_n(C_n, P; X_1^n)] = \mathbf{E}[L(C_n, X_1^n)] - H_n(P)$$

where $H_n(P)$ is the entropy, and $\mathbf{E}$ denotes the expectation.

To the best of our knowledge, no asymptotic results have been reported in literature on the average redundancy of Huffman codes. However, many elegant, insightful and useful lower and upper bounds on $\bar{R}_n^H$ are known. Gallager [4] proved that $\bar{R}_n^H \le p_1 + \lg(2(\log e)/e) \approx p_1 + 0.086$ where p_1 is the probability of the most likely symbol. This bound was further improved by Capocelli and de Santis [2], Stubley [6] and others (cf. [1]).

Let p denote the probability of generating a 0 and $q = 1 - p$ denote the probability of emitting a 1. Throughout, we assume that $p < \frac{1}{2}$. Certainly, this does not restrict the generality of the analysis.

We start with the average redundancy of the Shannon-Fano code of a block x_1^n of length n. It assigns code length $\lceil -\log_2 p^k(1-p)^{n-k} \rceil$ to the block x_1^n where k is the number of "1" in x_1^n. Thus, its average redundancy is

$$\bar{R}_n^{SF} = 1 - \sum_{k=0}^{n} \binom{n}{k} p^k q^{n-k} \langle \alpha k + \beta n \rangle$$

where $\langle x \rangle = x - \lfloor x \rfloor$ being the fractional part of x, $\alpha = \log_2(1-p)/p$ and $\beta = \log_2(1-p)/p$.

Theorem 1 *Consider the Shannon-Fano block code of length n binomially(n,p) distributed over a binary alphabet. Then, for $p < \frac{1}{2}$ as $n \to \infty$*

$$\bar{R}_n^{SF} = \begin{cases} \frac{1}{2} + o(1) & \alpha \quad \text{irrational} \\ \frac{1}{2} - \frac{1}{M}\left(\langle Mn\beta \rangle - \frac{1}{2}\right) + O(\rho^n) & \alpha = \frac{N}{M} \end{cases}$$

where $\rho < 1$ and $\gcd(N, M) = 1$.

Now, we are in position to summarize our results for the Huffman code. Stubley [6] was led to the following asymptotic formula for the Huffman's average redundancy for the block x_1^n generated by a memoryless source

$$\bar{R}_n^H \sim 1 + \bar{R}_n^{SF} - -2\sum_{k=0}^{n} \binom{n}{k} p^k q^{n-k} 2^{-(\alpha k + \beta n)}$$

where $\rho < 1$.

Theorem 2 *Consider the Huffman block code of length n binomially(n,p) distributed over a binary alphabet. Then, for $p < \frac{1}{2}$ as $n \to \infty$*

$$\bar{R}_n^H \sim \begin{cases} \frac{3}{2} - \frac{1}{\log 2} + o(1) \approx 0.057304, & \alpha \quad \text{irrational} \\ \frac{3}{2} - \frac{1}{M}\left(\langle \beta M n \rangle - \frac{1}{2}\right) - \frac{1}{M(1-2^{-1/M})} 2^{-(n\beta M)/M}, & \alpha = \frac{N}{M} \end{cases}$$

where N, M are integers such that $\gcd(N, M) = 1$.

Observe that if we set in the rational case $x = \langle Mn\beta \rangle$, then

$$\max_{0 \le x < 1} \bar{R}_n^H = 1 - \frac{1 + \log\log 2}{\log 2} = \lg(2(\lg e)/e) = 0.08607\ldots,$$

which is the Gallager upper bound (since the most likely probability $p_1 = O(1/\sqrt{n})$ in this case). We formulate it as a corollary.

Corollary 1 *The maximum value of the average Huffman redundancy is*

$$\max\{\bar{R}_n^H\} = 1 - \frac{1 + \log\log 2}{\log 2} = \lg(2(\lg e)/e) = 0.08607\ldots,$$

as $n \to \infty$.

[1] This work was supported in part by NSF Grants NCR-9415491 and C-CR-9804760.

References

[1] J. Abrahams, "Code and Parse Trees for Lossless Source Encoding, *Proc. of Compression and Complexity of SEQUENCE'97*, Positano, IEEE Press, 145-171, 1998.

[2] R. Capocelli and A. de Santis, Tight Upper bounds on the Redundancy of Huffman Codes, *IEEE Trans. Information Theory*, 35, 1084-1091, 1989.

[3] M. Drmota and R. Tichy, *Sequences, Discrepancies, and Applications*, Springer Verlag, Berlin Heidelberg 1997

[4] R. Gallager, Variations on the Theme by Huffman, *IEEE Trans. Information Theory*, 24, 668-674, 1978.

[5] D. Huffman, A Method for the Construction of Minimum Redundancy Codes, *Proc. IRE*, 40, 1089-1101, 1952.

[6] P. Stubley, On the Redundancy of Optimum Fixed-to-Variable Length Codes, *Proc. Data Compression Conference*, 90-97, Snowbird 1994.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Byte-oriented Decoding of Canonical Huffman Codes

Yakov Nekritch
Department of Computer Science,
University of Bonn
yasha@cs.uni-bonn.de

I. Introduction

Huffman codes or minimum-redundancy prefix codes is one of the most widespread compression techniques nowadays.

Canonical codes are a subclass of Huffman codes, described by Conell[1] and Schwartz and Kallick[4]. The canonical codes have a *numerical sequence property*, i.e. codewords with the same length are binary representations of consecutive integers. Once the length of the current codeword is known, it can be decoded by several arithmetic operations in the following way. Supposed we have read the prefix b of the current codeword and all codewords with prefix b have length l. Indexes of the codewords with prefix b are consecutive integers and the codewords themselves are binary representations of consecutive integers.Let l_b be the length of the prefix b, $first_l$ be the index of the first codeword with length l and b_n be a value of the next $l - l_b$ bits. Then the index of the current codeword can be computed as $b_n + first_l$. This idea is used in the algorithm, described in [3]. Single bits are read from the input stream, until the codeword length l can be determined, then we read another $l - l_b$ bits and compute codeword index with the above formula. A special data structure, called an *sk-tree* is used to check, whether a codeword length can be determined from the read bits.

II. Decoding with sequential look-up tables

In this work we describe a table look-up decoding method. It leads to fast decoding without causing too high memory requirements. Besides that, combined with a special data structure, it enables memory-efficient decoding without bit-oriented processing of the input stream.

Let l_{min} and l_{max} denote minimal and maximal codeword lengths respectively, $l_{b_{min}}$ and $l_{b_{max}}$ will denote minimal and maximal codeword lengths for codewords with prefix b.

Instead of reading a fixed number of bits, we use the already read codeword prefix to determine a possible codeword length. We do not traverse a Huffman tree bit-by-bit, but read at each stage as many bits as possible. Thus, we begin with reading l_{min} bits.If the codeword length of the current codeword equals l_{min}, than the corresponding symbol is output. If the symbol length can be identified from bits already read, next l_b bits are read, otherwise, next $l_{b_{min}} - l_{min}$ bits are read. The process is repeated until a symbol is output. This process can be implemented with a series of tables. Every table record consists of two fields. One field is used to indicate, whether a codeword has been read or the next table has to be used. The second field contains either a symbol, corresponding to a codeword or a pointer to the next table. We look up the value of the first l_{min} bits in the first table. If the bits read so far constitute a codeword we output the corresponding symbol, otherwise we read the next bit sequence.

The number of records in all tables does not exceed the number of nodes in the Huffman tree, therefore $2n - 1$ is an upper bound for the number of table records. Let S be the set of codeword prefixes b, such that length of b equals to the length of some codeword in the Huffman code. Let $length(b)$ be the length of b. Then the total number of records can be computed as $\sum_{b \in S} 2^{l_{b_{min}} - length(b)} + 2^{l_{min}} + n$

```
Procedure Read_Next_Symbol( )
begin
while (table[bitval].type <> DIRECT_DECODE)
  next_length:=table[bitval].length;
  table:=table[bitval].next_table;
  bitval:=get_next_bits( next_length );
output table[bitval].value;
end
```

The described algorithm uses essentially less space than classical Huffman tree approach and allows for faster decompression. Our algorithm is also faster then $sk-tree$ decoding, for we always read groups of bits and not individual bits.

Further we suggest a special finite-automaton-based data structure, which allows reading of up to i bits from the input stream without using bit-oriented operations. This finite automaton has states corresponding to all binary sequences b with length between 1 and 8. The input alphabet consists of integers between 1 and i, the output alphabet consists of pairs (v, j), where j is an integer between 1 and i. States of the automata correspond to the "rest" of current byte, that is not yet processed. Input l indicates the number of bits to be read, v is the value of read bits, j is the number of bits that should be read at the next step. Supposed the FSM is in a state s, corresponding to the bit sequence of length k and input integer is l. If $l > k$ the automaton outputs pair $(v, l - k)$, where v is the value of b shifted $l - k$ bits left. If $l \leq k$, the automaton outputs pair $v, l - k$, where v is the value of b shifted $k - l$ bits right. Thus in the output pair (v, j) the first component v is the value of "as many as possible" read bits from the current byte and j indicates the number of bits which should be read from the next bytes.

The algorithm and data structure described in this work allow fast decoding of Huffman codes, that can be efficiently implemented without using bit operations.

References

[1] Connell J.B., "A Huffman-Shannon-Fano Code", Proc. of IEEE 61,7(July),1973, 1046-1047.

[2] D.A.Huffman, "A method for construction of minimum redundancy codes", Proc IRE 40(1951),1098-1101.

[3] Shmuel T.Klein, "Space- and time- efficient decoding with canonical Huffman trees", 8th Annual Symp. on Combinatorial Pattern Matching,Aarhus,Denmark, LNCS 1264, 65-75.

[4] Schwartz E.S. Kallick B., "Generating a canonical prefix encoding", Communications of the ACM 7(1964), 166-169.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

A New Upper Bound on the Data Expansion of Huffman Codes

Jia-Pei Shen and John Gill
Information System Laboratory, Department of Electrical Engineering
Stanford University, California, USA
e-mail: jiapei@stanfordalumni.org, gill@isl.stanford.edu

Abstract — **We prove that the maximum data expansion of Huffman coding is at most 0.83485 bits per symbol, improving on the previous best known bound of 1.256 bits per symbol. Our bound is very close to the 0.8 bits per symbol conjectured by Cheng et al.**

I. Problem Definition

The data expansion problem for Huffman codes was first proposed by Cheng et al. [1] and has been investigated in [1]-[5]. Let N be the size of the source alphabet and assume a binary alphabet for the codewords. Denote the probability and the Huffman codeword length of the i-th source symbol by p_i and l_i, respectively. The data expansion of the code is defined as follows.

$$\delta = \sum_{\{i \mid l_i > \lceil \log_2 N \rceil\}} p_i \, (l_i - \lceil \log_2 N \rceil) \qquad (1)$$

Data expansion is a measure of the temporary increase of the file size in the worst case if the Huffman codewords replace the fixed-length codewords sequentially and "in place" [1]. It is also a measure of the penalty for using long codewords for less likely codewords if we ignore the benefit we get from using short codewords for more likely symbols.

The goal of this paper is to find a universal upper bound on the data expansion, for any number of codewords and any probability distributions. The conjectured and the best known bounds are 0.8 [1] and 1.256 [5] bits per symbol respectively.

II. Canonical Ordered Huffman Code Trees and Sufficient Sets

A *canonical ordered Huffman code tree* is an ordered Huffman code tree [6] in which the probability of every intermediate node is no less than the probability of every terminal node at the same level.

Define S as the space of all possible combinations of Huffman code tree structures and probability distributions. A subset S' of S is called a *sufficient set* if for any data expansion δ achieved by some element of S, there exists an element of S' with data expansion at least as large as δ.

III. Data Expansion Upper Bound

Theorem 1 *The set of Huffman code trees with the following properties is a sufficient set for the maximum data expansion problem of Huffman codes.*

1. *The Huffman code tree is canonical ordered.*
2. *There is at most one codeword at each level up to level* $\log_2 N$, *and the probability of each such codeword is equal to the maximal node probability at the next level.*
3. *The only codewords at levels greater than* $\log_2 N$ *are at the largest level and the second largest level.*
4. *Either all codewords at the largest and second largest levels have the same probability (case A) or codewords at the second largest level have twice the probability of the codewords at the largest level (case B).*

It is sufficient to consider only N a power of 2, say $N = 2^m$. Consider any Huffman code from the sufficient set of Theorem 1. Let N' be the number of intermediate nodes at level m. Let K, $K \leq m$, be the number of codewords of length at most m. Denote the largest level as L. Define $\beta = (N-K)/N'$. It can be shown that

$$L = m + \gamma + \left\lfloor \log_2 \frac{N-K}{N'} \right\rfloor, \qquad (2)$$

where γ is 0 if the number of codewords at level $L-1$ is 0 and 1 otherwise. It can then be shown that the data expansion is

$$\delta = \begin{cases} (\lfloor \log_2 \beta \rfloor + 2(1 - \frac{1}{\beta} \cdot 2^{\lfloor \log_2 \beta \rfloor})) \, P_A, & \text{case A} \\ (\lfloor \log_2 \beta \rfloor - 1 + \frac{\beta}{2^{\lfloor \log_2 \beta \rfloor}}) \, P_B, & \text{case B} \end{cases} \qquad (3)$$

where P_A and P_B represent the total probability that contributes to the data expansion in each case. We prove that

$$P_A \leq P_B \qquad (4)$$

$$P_B = \frac{2N'(\theta_1 - \theta_2)}{2^{m-l}(\theta_1^l - \theta_2^l) + (2^{m-l} + N')(\theta_1^{l+1} - \theta_2^{l+1})} \qquad (5)$$

$$\leq \frac{2(\theta_1 - \theta_2)}{2^{-l}\beta(\theta_1^l - \theta_2^l + \theta_1^{l+1} - \theta_2^{l+1}) + (\theta_1^{l+1} - \theta_2^{l+1})} \qquad (6)$$

where $\theta_1 = (1+\sqrt{5})/2$, $\theta_2 = (1-\sqrt{5})/2$, and l is defined as $\min\{j \mid n_j = 0\} - 1$, where n_j is the number of codewords at level j. It can be shown that

$$l = \left\lfloor \log_2 \frac{N}{N'} \right\rfloor . \qquad (7)$$

Using (3), (4), (6), (7), and the fact that the maximum data expansion is monotonically increasing with m, we show that the maximum data expansion for case A and B is at most 0.83485 and 0.8 bits per symbol respectively.

Theorem 2 *The maximum data expansion of Huffman codes is at most 0.83485 bits per symbol.*

References

[1] J-F. Cheng, S. Dolinar, M. Effros, R. McEliece, "Data Expansion with Huffman codes", *Proc. of ISIT 95, Whistler, BC, Canada*, pp. 325, 1995.

[2] H. D. L. Hollmann, "A simple proof of finite data expansion per symbol with Huffman codes," Philips Res. Labs., ms. 18.724, Oct. 1995.

[3] R. D. Prisco and A. D. Santis, "A new bound for the Data Expansion of Huffman codes," *IEEE Trans. Inform. Theory*, vol. 43, no. 6, pp. 2028-2032, Nov. 1997.

[4] R. D. Prisco and A. D. Santis, "On the redundancy and data expansion of Huffman codes", *Proc. of ISIT 98, Cambridge, MA, USA*, pp. 272, 1998.

[5] R. D. Prisco and A. D. Santis, "On the data expansion of the Huffman compression algorithm", *Computer Journal*, vol. 41, no. 3, pp. 137-144, 1998.

[6] R. G. Gallager, "Variations on a Theme by Huffman," *IEEE Trans. Inform. Theory*, vol. 24, no. 6, pp. 668-674, Nov. 1978.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

The complexity of minimum redundancy coding

Tjalling Tjalkens[1]
Eindhoven Univ. Tech.
P.O.Box 513
5600 MB Eindhoven
The Netherlands
e-mail: t.j.tjalkens@ele.tue.nl

Abstract — **An efficient implementation of a Huffman code is based on the Shannon-Fano construction. An important question is: how complex is such an implementation. In the past authors have considered this question assuming an ordered source symbol alphabet. For of the compression of blocks of binary symbols this ordering must be performed explicitly and it turns out to be the complexity bottleneck.**

I. The Huffman-Shannon-Fano code

We consider a binary, memoryless source $\{X_i\}_{i=1}^{\infty}$ with $\Pr\{X_i = 1\} = p \leq \frac{1}{2}$. The *Huffman-Shannon-Fano (HSF) codes* [1] that we shall consider are described as follows.

First assign to each block x^n a unique index $i(x^n) \in \{0, 1, \ldots, 2^n - 1\}$ such that for all pairs of blocks $x^n, y^n \in \{0,1\}^n$ holds $i(x^n) < i(y^n) \Rightarrow P(x^n) \geq P(y^n)$. Let $\underline{w} = w_0, w_1, \ldots, w_{2^n-1}$ be a vector of code word lengths such that: - $\underline{w}$ satisfies Kraft's inequality with equality; - $\mathbb{E}\{W\} = \sum_{x^n \in \{0,1\}^n} P(x^n) w_{i(x^n)}$ is minimal; - For all $i, j \in \{0, 1, \ldots, 2^n - 1\}$ $i < j \Rightarrow w_i \leq w_j$. So, $\underline{w}$ is a non-decreasing sequence given the index ordering $i(x^n)$.

Now it is time to introduce the Huffman-Shannon-Fano encoding procedure briefly. Given the code word lengths $\underline{w}$ we determine the number of codewords $v(i)$ of a given length i. We shall use the notation w_- for the shortest, and w_+ for the longest code word length.

From Nemetz and Simon [3] we know that for all x^n holds

$$|w_{i(x^n)} + \log_2 P(x^n)| = \mathcal{O}(n), \tag{1}$$

and with the fact that $\Pr\{0^n\} = -n\log_2(1-p)$ and $\Pr\{1^n\} = -n\log_2 p$ we obtain that

$$w_+ = -n\log_2 p + \mathcal{O}(n), \tag{2}$$
$$w_- = -n\log_2(1-p) + \mathcal{O}(n). \tag{3}$$

Now we can compute the 'base' values by: $\forall_{w \in \{w_-, \ldots, w_+\}}$: $\mathsf{base}(w) \triangleq \sum_{j=w_-}^{w-1} v(j) 2^{w-j} - v(j)$.

The encoding procedure is now as follows. Given a source sequence x^n do: - Determine the index $i = i(x^n)$; - Determine the code word length $w = w_i$; Produce the code word for x^n from the binary representation of $\mathsf{base}(w) + i$ in w bits.

II. Complexity considerations

Storage complexity: We shall consider only the storage requirements for the encoding (and decoding) of a block X^n. So, we do not take into account the cost of the preprocessing (designing the code).

Time complexity: We require that the total time complexity is $\mathcal{O}(n)$. Again we only consider the encoding and decoding cost and not the preprocessing cost.

Usually, but not always, we can interchange storage and time complexity by adding more units to perform more operations in parallel thus increasing the storage complexity while decreasing the time complexity and vice versa.

III. Conclusions

The storage complexity of the HSF code is bounded by the cost of indexing the source sequence. This is a fact that is ignored in the Computer-Science literature where one is concerned with an efficient determination of the codeword lengths. However that is a one time only problem, while for the encoding and decoding one needs the indexing once per codeword.

Summarizing the complexity:

- The cost of the code word generation. When we store the base array the time complexity is $\mathcal{O}(1)$ and the storage cost is $\mathcal{O}(n^2)$ bits. We also showed that it is possible to *compute* the base values when we need them in $\mathcal{O}(n)$ time. The storage cost then is $\mathcal{O}(n)$ because we must save the resulting codeword.
- The cost of the code word length array. We described an algorithm that produces the required code word length from the source sequence index in $\mathcal{O}(\log n)$ time and $\mathcal{O}(n^2)$ storage space.
- The index computation is still an open question. Using enumerative techniques similar to [2] we have two options, either we use a table of binomial coefficients, *Pascal's triangle*, or we *compute* the required coefficients. Pascal's triangle requires $\mathcal{O}(n^3)$ bits of storage and the computation of the index then costs $\mathcal{O}(n)$ time. Computing the coefficients requires $\mathcal{O}(n)$ divisions that must be performed sequentially thus resulting in a time complexity of $\mathcal{O}(n^2)$, which is unacceptable.

References

[1] J.B. Connell, "A Huffman-Shannon-Fano Code," *Proc. IEEE*, vol 61, pp. 1046–1047, 1973.

[2] T. Cover, "Enumerative source coding," *IEEE Trans. Inform. Theory*, vol IT-19, pp. 73–76, Jan. 1973.

[3] T. Nemetz and J. Simon, "Self-information and optimal codes," in *Topics in IT*, pp. 457–468, 1977.

[1]This work was performed during a visit at the Information Technology Department of Lunds Tekniska Högskola, Sweden.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Some Results on the Classification of N Objects in M Classes with at Least c Objects in Each Class

Bruno Cernuschi-Frías[1]
Facultad de Ingeniería
Universidad de Buenos Aires and
CONICET
Casilla 8, Sucursal 12(B)
1412 Buenos Aires, ARGENTINA
e-mail: bcf@ieee.org

Abstract — **An approach towards an information theoretic based analysis and design of cache memories is presented. Computer systems usually have a slow *main* memory and a faster *cache* memory, usually much smaller than the main memory because of its cost. A somewhat similar situation is present also in Internet servers. A *miss* happens whenever an item is not found in the cache memory. If so, the item is fetched from the main memory and placed in the cache. A hit is obtained whenever the item is found in the cache. Usually the cost of a miss is several times that of a hit. The goal is to find strategies for the many to one mapping of addresses of the main memory to the cache memory, as well as the replacement strategies. Usual replacement strategies are Least Recently Used, *LRU*, Random Replacement, *RR*, etc. The main goal is to obtain strategies that will optimize the running time of the program under execution. Since almost all programs use branch instructions and loops, some of the information theoretic approaches previously introduced consider the prediction of the result of a branch based on its past behavior. Here a different approach is considered. In particular the opposite case is analyzed, i. e. a linear loop that is executed indefinitely. In particular a combined Random Replacement and Least Recently Used strategy is analyzed. It is shown that this model is equivalent to the one of classifying N objects in M classes with at least c objects in each class, and that this problem gives a generalization of the Ehrenfests' urn model used in Statistical Thermodynamics in connection with the Boltzmann H-theorem. In that sense, a combinatorial generalization of the Stirling Numbers of the Second Kind is presented as the number of partitions of a set with n elements in m subsets with at least c elements each. Combinatorial properties and a recursive relation are obtained. The generating function is obtained as the m-th power of a truncated exponential series expansion at c. Asymptotic results are given for n going to infinity, with m fixed, and with n/m constant, from which, in particular, the Stirling Formula is obtained. The connection with some large deviation theory results are discussed, as well as the relation with the minimum variance unbiased estimator of Truncated at c Poisson Distributions. The solution of the linear loop model is given in terms of a Markov chain which generalizes the Ehrenfests' urn model. Finally, it is discussed how the results obtained so far suggest an information measure for the behavior of arbitrary programs and a Bayesian approach to cache memory optimization.**

[1]This work was partially supported by the *Universidad de Buenos Aires*, grant No. TI-09, and the *Consejo Nacional de Investigaciones Científicas y Técnicas*, grant No. PIP-4030, CONICET, Argentina.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

The Mastermind game and the rigidity of the Hamming space

G. Kabatianski [1] , V.Lebedev
IPPI, Russian Academy of Sciences
Bolshoy Karetniy 19, Moscow,
101447, Russia
kaba@iitp.ru

J. Thorpe [1]
College of Engineering,
University of California at
Riverside
CA 92521, USA.

Abstract — **A new approach to investigating the Mastermind game and related problems, among them uniquely decodable codes for noiseless adder channel, based on ideas and methods of coding theory is proposed. This approach leads to improved bounds in various problems associated with the rigidity of Hamming spaces.**

I. INTRODUCTION

We call a set B a *base* of a metric space L if every point of L is uniquely determined by its distances to the points of B. The minimal possible number of points of a base is called the rigidity of the metric space and denoted by $r(L)$. Let $H_{n,q}$ be the n-dimensional q-ary Hamming space and $r_{n,q}$ be its rigidity. This notion was introduced in 1963 by P. Erdős and A. Renyi [1] for solving the following weighing problem: what is the minimal number $W(n)$ of weighings on an accurate scale to determine all counterfeit coins in a set of n coins. It is easy to see that the minimal number $W_d(n)$ of weighings for deterministic strategies differs from $r_{n,2}$ by not more than on one. Note that this problem is equivalent to the problem of uniquely decodable codes for noiseless n-user adder channel [2].

Many mathematicians have worked on the game of Mastermind. For instance, in 1977 D. Knuth proved [3] that 4 questions suffice to determine a hidden "code" - i.e., a word x of length n in an alphabet of q elements for $n = 4, q = 6$. Denote by $m(n,q)$ the minimal number of queries to determine *any* "hidden" word x, and by $m_d(n,q)$ the minimal number of queries for the case of deterministic strategies. Obviously, $q-1$ queries is enough to find the composition of the word x. Therefore, $r_{n,q}-(q-1) \le m_d(n,q) \le r_{n,q}$, and the asymptotic behavior of the both values $m_d(n,q)$ and $r_{n,q}$ is the same at least for the case of $n >> q$.

II. THE RIGIDITY OF THE HAMMING SPACE: THE CASE q IS FIXED

Obviously, $r_{n,q} \ge \frac{n}{\log_q(n+1)}$, because the number of possible distances is not more than $n+1$. Straightforward generalization of [1] gives twice better bound:

$$r_{n,q} \ge 2\frac{n}{\log_q n}(1+o(1)). \qquad (1)$$

By considering a random base of $H_{n,q}$ V.Chvatal [4] proved that $r_{n,q} \le C(q)\frac{n}{\log_q n}(1+o(1))$, where $C(q) = 2(2+\log_q 2)$. More precise calculations show that

$$r_{n,q} \le c(q)\frac{n}{\log_q n}(1+o(1)), \qquad (2)$$

where $c(q) = 2\log_q(1+(q-1)q) < 4 < C(q)$.

It was proved in [5],[6] that $r_{n,2} = 2\frac{n}{\log_2 n}(1+o(1))$. We prove that

Theorem 1: *For* $q = 3,\ 4$

$$r_{n,q} = 2\frac{n}{\log_q n}(1+o(1))$$

III. THE RIGIDITY OF THE HAMMING SPACE, MASTERMIND AND "BULL AND COWS" GAMES: THE CASE $n = q$

Let us consider the case $n = q$. Further, consider among all n-letter words the set S_n of words without repetitions of symbols, i.e., permutations. This space corresponds to another famous (and much older, see [3]) game, "Bulls and Cows". As in the last section, random choice of a base and entropy techniques proves the following result.

Theorem 2:

$$O(n\log_2 n) \le r(H_{n,n}), r(S_n) \le 4n\log_2 n(1+o(1)).$$

IV. CONCLUSION

We show how information theory techniques can be useful for investigating several long standing problems. However, the centeral question, *"what is the rigidity of q-ary Hamming space?"* remains open for $q > 4$. We conjecture that, as in the binary case, random choice does not give the final answer to the problems considered. We have considered the case of deterministic strategies of the games. Much less is known about adaptive strategies, which corresponds, in particular, to noiseless adder channel with feedback. Another interesting direction is the relationship of these problems with superimposed codes on the n-dimensional cube (i.e., l_∞^n-space), see [7].

[1]This work was supported by the NSF grant NCR-9703844

REFERENCES

[1] P. Erdős and A. Renyi, On two problems of information theory, *Publ. Hung. Acd. Sci,* vol. 8,pp. 241–254, 1963.

[2] S-C. Chang and E.J. Weldon, Coding for T-user multiple-access channels, *IEEE Trans.-IT,* vol. 25, no. 6, pp. 684–691, 1979.

[3] D.E Knuth, The computer as mastermind, *J. of Recreational Mathematics,* vol. 9, pp. 1–6, 1976-77.

[4] V. Chvatal ,Mastermind, *Combinatorica* vol. 3, pp. 325–329, 1983.

[5] B. Lindsrom, On a combinatorial detection problem, *Publ. Hung. Acd. Sci,* vol. 9,pp. 195–207, 1964.

[6] D.G. Cantor, Determining a set from the cardinalities of its intersections with other sets, *Canad.J. Math.,* vol. 16, pp. 94–97, 1964.

[7] Z. Furedi and M. Ruszinko, An improved upper bound of the rate of Euclidean superimposed codes, *IEEE Trans.-IT,* vol. 45, no.2, pp. 779-802, 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Strategy for Data Transmission over Binary Channels with Noiseless Feedback and Upper Bound on the Number of Questions in Searching with Lies

Vladimir B. Balakirsky
Electr. Eng. Dept., TUE
P.O. 513, 5600 MB Eindhoven
The Netherlands

Abstract — **A transmission strategy that allows the sender to deliver any of M messages to the receiver over a binary channel when at most e errors can occur is presented. The total number of bits required by the strategy differs from the known lower bound by $3e$. This statement simultaneously gives a new upper bound on the number of questions in the process of searching with lies known as the "Ulam's game".**

I. Introduction and formulation of the result

Let $[M] = \{1, \ldots, M\}$ denote the set of messages. One of them should be transmitted over a binary channel where at most e errors $0 \to 1$ and $1 \to 0$ can occur. For all $\tau = 1, 2, \ldots$, the sender noiselessly observes the received bit y_τ and sends the next bit $x_{\tau+1}$ based on the message $m \in [M]$ and the bits $x_1, \ldots, x_\tau, y_1, \ldots, y_\tau$ which were transmitted and received at the previous time instants. Any transmission strategy is the algorithm for computing the bits $x_1, \ldots, x_n$ by the sender and for decoding the message m by the receiver, where n is the total number of transmitted bits. The equivalent problem can be formulated as searching for an integer $m \in [M]$ by asking questions when at most e lies are allowed in the answers : the question $\mathcal{Q}$ is a subset of the set $[M]$; the answer is either 0 or 1, and the answers 0 if $m \in \mathcal{Q}$ and 1 if $m \notin \mathcal{Q}$ are considered as lies.

Theorem : *There exist searching strategies such that any of M integers can be discovered with $n^* = n + 3e$ questions when at most e lies are allowed in the answers, where n is the minimal integer satisfying the inequality $MV_e^{(n)} \le 2^n$ and $V_e^{(n)} = \sum_{i=0}^{e} \binom{n}{i}$.*

II. Basic ideas of the proof

Suppose that $\mathcal{M}_0, \ldots, \mathcal{M}_e$ are pairwise disjoint subsets of the set $[M]$ constructed by the questioner in such a way that if $m \in \mathcal{M}_j$, then j lies are allowed in all further answers, $j = 0, \ldots, e$. Then the vector $\mathbf{c} = (|\mathcal{M}_0|, \ldots, |\mathcal{M}_e|)$ can be interpreted as the state of the search. Let $\mathcal{D}(c)$ denote the set consisting of integers δ such that $|\delta| \le c$ and $\delta \equiv c \pmod 2$. For all $\boldsymbol{\delta} = (\delta_0 \in \mathcal{D}(c_0), \ldots, \delta_e \in \mathcal{D}(c_e))$, let $\mathbf{a}(\mathbf{c}|\boldsymbol{\delta}) = (a_0, \ldots, a_e)$, $\mathbf{b}(\mathbf{c}|\boldsymbol{\delta}) = (b_0, \ldots, b_e)$, where $a_j = (c_j + c_{j+1} + \delta_j - \delta_{j+1})/2$, $b_j = (c_j + c_{j+1} - \delta_j + \delta_{j+1})/2$ and $j = 0, \ldots, e$ (we assume that $c_{e+1} = \delta_{e+1} = 0$). Let the vector $\boldsymbol{\delta}$ specify the question $\bigcup_{j=0}^{e} \mathcal{Q}_j$, where $\mathcal{Q}_j$ is the subset consisting of $(c_j + \delta_j)/2$ smallest elements of the subset $\mathcal{M}_j$ for all $j = 0, \ldots, e$. We will call this procedure "partitioning of the subsets $\mathcal{M}_0, \ldots, \mathcal{M}_e$ in accordance with the vector $\boldsymbol{\delta}$". Let $\mathcal{Q}_{e+1} = \mathcal{M}_{e+1} = \emptyset$ and $\overline{\mathcal{Q}}_j = \mathcal{M}_j \backslash \mathcal{Q}_j$ for all $j = 0, \ldots, e+1$. If the answer is 1, the new vector of sets has components $\mathcal{M}'_j = \mathcal{Q}_j \bigcap \overline{\mathcal{Q}}_{j+1}$ and $\mathbf{a}(\mathbf{c}|\boldsymbol{\delta})$ is the new state of the search. If the answer is 0, the new vector of sets has components $\mathcal{M}''_j = \overline{\mathcal{Q}}_j \bigcap \mathcal{Q}_{j+1}$ and $\mathbf{b}(\mathbf{c}|\boldsymbol{\delta})$ is the new state of the search.

A key point of our considerations is the introduction of a special class of rooted regular binary trees whose nodes "contain" possible states of the search. This construction relates binary trees to coverings of the Hamming spaces by sets having the cardinalities coincident with the sizes of the Hamming balls and leads to the following statement, which is essentially used in the searching strategy. *Let $\mathcal{M}_0, \ldots, \mathcal{M}_e$ be current pairwise disjoint subsets constructed by the questioner and let t be the minimal integer satisfying the inequality $\sum_{j=0}^{e} |\mathcal{M}_j| \cdot V_j^{(t)} \le 2^t$. Then the searching problem under consideration cannot be solved using less than t questions, and a solution with t questions exists only if this problem can be solved using t questions when some set $\hat{\mathcal{M}}_0$ assigned in such a way that $|\hat{\mathcal{M}}_0| = 2^t - \sum_{j=0}^{e} |\mathcal{M}_j| \cdot V_j^{(t)}$; $\hat{\mathcal{M}}_0 \supseteq \mathcal{M}_0$; $\hat{\mathcal{M}}_0 \bigcap \mathcal{M}_1 = \ldots = \hat{\mathcal{M}}_0 \bigcap \mathcal{M}_e = \emptyset$ is substituted for $\mathcal{M}_0$.*

To prove the theorem we present a specific algorithm for assigning the vector $\boldsymbol{\delta}$ for any vector $\mathbf{c}$ that can be obtained by the questioner and denote this vector by $\boldsymbol{\delta}^*(\mathbf{c})$. Let η denote the index of the last positive component of the vector $\mathbf{c}$. If $c_\eta = 1$, then $\delta_1^* := -c_1, \ldots, \delta_{\eta-1}^* := -c_{\eta-1}$; $\delta_\eta^* := 1$; $\delta_{\eta+1}^* := \ldots := \delta_e^* := 0$. If $c_\eta > 1$, then

$$\delta_j^* := \arg \min_{\delta \in \mathcal{D}(c_j)} \left| \binom{t-1}{j} \delta + \sum_{i=j+1}^{e} \binom{t-1}{i} \delta_i^* \right|$$

for $j = e, \ldots, 1$. In both cases, $\delta_0^* := -\sum_{j=1}^{e} \binom{t-1}{j} \delta_j^*$.

The searching strategy is given below, where the vector of length $e+1$ containing 1 in the j-th position and 0's in all other positions is denoted by $\mathbf{1}_j$, $j = 0, \ldots, e$.

1. $c_0 := 2^n - MV_e^{(n)}$; $\mathcal{M}_0 := \ldots := \mathcal{M}_{e-1} := \emptyset$; $\mathcal{M}_e := [M]$.
2. $\mathbf{c} := (c_0, |\mathcal{M}_1|, \ldots, |\mathcal{M}_e|)$. If $\mathbf{c} \in \{\mathbf{1}_0, \ldots, \mathbf{1}_e\}$, then go to 5.
3. Construct the vector $\boldsymbol{\delta}^*(\mathbf{c}) = (\delta_0^*, \ldots, \delta_e^*)$ using the algorithm described above with the value of t determined by the equation $\sum_{j=0}^{e} c_j V_j^{(t)} = 2^t$. If $|\delta_0^*| > c_0$, then $c_0 := c_0 + \sum_{j=0}^{e} c_j \binom{t}{j}$ and go to 2.
4. Partition the subsets $\mathcal{M}_0, \ldots, \mathcal{M}_e$ in accordance with the vector $\boldsymbol{\delta}^*(\mathbf{c})$. If the answer is 1, then $c_0 := (c_0 + c_1 + \delta_0^* - \delta_1^*)/2$ and $\mathcal{M}_j := \mathcal{M}'_j$, $j = 0, \ldots, e$. If the answer is 0, then $c_0 := (c_0 + c_1 - \delta_0^* + \delta_1^*)/2$ and $\mathcal{M}_j := \mathcal{M}''_j$, $j = 0, \ldots, e$. Go to 2.
5. End : the singleton $\mathcal{M}_j$, where j is such that $c_j = 1$, contains the defined integer.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Perfect, Minimally Adaptive, Error-Correcting Searching Strategies

Ferdinando Cicalese[1]
Dip. Informatica ed Applicazioni
University of Salerno
84081 Baronissi (SA), Italy
e-mail: cicalese@dia.unisa.it

Daniele Mundici
Dip. Scienze Informazione
University of Milan
20135 Milan, Italy
e-mail: mundici@unimi.it

Ugo Vaccaro
Dip. di Informatica ed Applicazioni
University of Salerno
84081 Baronissi (SA), Italy
e-mail: uv@dia.unisa.it

Abstract — **Let $q_e(m)$ be the smallest integer q satisfying Berlekamp's bound $\sum_{i=0}^{e}\binom{q}{i} \leq 2^{q-m}$ [1]. We prove that for any fixed $e \geq 1$ and all sufficiently large m there is a binary searching strategy to guess a number $x \in \{0,\ldots,2^m-1\}$ in spite of up to e lies in the answers, which uses exactly $q_e(m)$ questions and adaptiveness only once. The strategy goes through a first batch of m non-adaptive questions asking for the bits of the binary expansion of x and then, only depending on the answers to these questions, a second batch of $q_e(m)-m$ non-adaptive questions.**

I. Introduction

We consider the following scenario: Two players, called Questioner (**Q**) and Responder (**R**) , first agree on fixing an integer m and a search space $S = \{0,\ldots,2^m-1\}$. Then **R** thinks of a number $x_* \in S$ and **Q** must find out x_* by asking questions to which **R** can only answer yes or no. It is agreed that **R** the Responder is allowed to lie at most e times. We are interested in the problem of determining the minimum number of questions **Q** has to ask in order to infallibly guess the number x_*. This problem was posed by Ulam [7] and Rényi [4], and has been intensively ivestigated in the last decades (see [2] for a survey).

In the fully adaptive case, i.e., when the ith question is asked knowing the answer to the $(i-1)$th question, a remarkable result of Spencer [5] shows that $q_e(m)$ questions are *necessary* and *sufficient*, up to finitely many exceptional m's. At the other, *totally non-adaptive* extreme, when all the questions are asked at the outset, before knowing *any* answer, a series of negative results culminating in the paper by Tietäväinen [6] shows that searching strategies with exactly $q_e(m)$ questions—or equivalently, perfect binary e-errors correcting codes with 2^m codewords of length $q_e(m)$—are sporadic exceptions for $e \leq 3$, and do not exist for $e > 3$, except in trivial cases.

Our main result, stated in the abstract, says that for each e, and for all sufficiently large m, searching strategies do exist having the least possible degree of adaptiveness (just *once*) and using exactly $q_e(m)$ questions. Since **Q** can adapt his strategy only once, our paper yields e-fault tolerant search strategies with *minimum* adaptiveness and the least possible number of tests.

II. The Two-Round Strategy

By a *yes-no question* we simply mean an arbitrary subset T of S. If the answer to the question T is "yes", numbers in T are said to *satisfy* the answer, while numbers in $S \setminus T$ *falsify* it. At any time **Q**'s *state* of knowledge is represented by an $(e+1)$-tuple $\sigma = (A_0, A_1, \ldots, A_e)$ of pairwise disjoint subsets of S, where A_i is the set of numbers falsifying exactly i answers, $i = 0,1,2,\ldots,e$. The *type* of σ is the $(e+1)$-tuple $(|A_0|, |A_1|, \ldots, |A_e|)$. Moreover, σ is a *final* state iff $|A_0 \cup A_1 \cup \cdots \cup A_e| \leq 1$. For any state $\sigma = (A_0,\ldots,A_e)$ and question $T \subseteq S$, the two states σ^{yes} and σ^{no} respectively resulting from a positive or a negative answer, are given by $\sigma^{yes} = (A_0^{yes},\ldots,A_e^{yes})$ and $\sigma^{no} = (A_0^{no},\ldots,A_e^{no})$ where, setting $A_{-1} = \emptyset$, we define $A_i^{yes} = (A_i \cap T) \cup (A_{i-1} \setminus T)$ and $A_i^{no} = (A_i \setminus T) \cup (A_{i-1} \cap T)$ for each $i = 0,1,\ldots,e$.

The first batch of questions is easily described as follows: *For each $i = 1,2,\ldots,m$, let $D_i \subseteq S$ denote the question "Is the ith binary digit of x_* equal to 1?" Thus a number $y \in S$ belongs to D_i iff the ith bit y_i of its binary expansion $\vec{y} = y_1 \cdots y_m$ is equal to 1.*

Upon identifying $1 = yes$ and $0 = no$, let $b_i \in \{0,1\}$ be the answer to question D_i. Let $\vec{b} = b_1 \cdots b_m$. Beginning with the initial state $\sigma = (S, \emptyset, \ldots, \emptyset)$, the resulting state as an effect of the answers $b_1 \cdots b_m$, is $\sigma^{\vec{b}} = (A_0, A_1, \ldots, A_e)$, where $A_i = \{y \in S \mid d_H(\vec{y},\vec{b}) = i\}$, for all $i = 0,1,\ldots,e$. Here $d_H(\cdot,\cdot)$ denotes the Hamming distance. Thus $\sigma^{\vec{b}}$ has type $(1, m, \binom{m}{2}, \ldots, \binom{m}{e})$.

The second batch of questions. We can prove that for all sufficiently large m there exists a second batch of $n = q_e(m) - m$ non-adaptive questions allowing **Q** to infallibly guess the secret number. Here follows the key lemma.

Lemma II.1 *For any fixed e and all sufficiently large m let $n = q_e(m) - m$. Then there exists a family of codes $\Gamma = \{\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_{e-1}\}$ together with integers $d_i \geq 2(e-i)+1$ $(i = 0,1,\ldots,e-1)$ such that* (i) *Each $\mathcal{C}_i$ is an $(n, \binom{m}{i}, d_i)$ code [3];* (ii) *$\Delta(\mathcal{C}_i, \mathcal{C}_j) \geq 2e - (i+j) + 1$, (whenever $0 \leq i < j \leq e-1$), where $\Delta(\mathcal{C}_1, \mathcal{C}_2) = \min\{d_H(\vec{x},\vec{y}) \mid \vec{x} \in \mathcal{C}_1, \vec{y} \in \mathcal{C}_2\}$.*

Let f be any mapping associating elements in A_i to codewords of $\mathcal{C}_i$ $(i = 0,\ldots,e-1)$ and elements of A_e to n-bit vectors of $\{0,1\}^n \setminus \Gamma$. Let $f(x)_j$ be the jth bit of $f(x)$. Let the set $T_j \subseteq S$ be defined by $T_j = \{z \in S \mid f(z)_j = 1\}$, $(j = 1,\ldots,n)$. This makes the second batch of questions. Intuitively, T_j asks "is the jth bit of $f(x_*)$ equal to 1?"

References

[1] E. R. Berlekamp, *Block coding for the binary symmetric channel with noiseless, delayless feedback*, In: Error-correcting Codes, H.B. Mann (Editor), Wiley, New York (1968), 61-88.

[2] R. Hill, *Searching with lies*, In: Surveys in Combinatorics, Rowlinson, P. (Editor), Cambridge Univ. Press (1995), 41–70.

[3] F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

[4] A. Rényi, *Napló az információelméletről*, Gondolat, Budapest, 1976.

[5] J. Spencer, *Ulam's searching game with a fixed number of lies*, Theoretical Comp. Sci., **95** (1992), 307-321.

[6] A. Tietäväinen, *On the nonexistence of perfect codes over finite fields*, SIAM J. Appl. Math., **24**, (1973), 88-96.

[7] S.M. Ulam, *Adventures of a Mathematician*, Scribner's, New York, 1976.

[1]This work was supported by Enea-Grant.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Lower Bound on the Total Squared Correlation of the Bandwidth Constrained, Time-Limited Signal Sets

Ha H. Nguyen and E. Shwedyk[1]
Department of Electrical & Computer Engineering, University of Manitoba
Winnipeg, Manitoba, Canada R3T 5V6
e-mail: nguyen@ee.umanitoba.ca, shwedyk@.ee.umanitoba.ca

I. Introduction

Welch's bound for a set of K equal-energy sequences of length N ($K > N$) is defined as the lower bound on the sum of the squared correlations between all pairs of these sequences [1, 2]. The sets of sequences that achieve the Welch bound are desirable in many signal design problems for multiple access communications [2]. Here a similar bound for the set of K equal-energy, time-limited signals is derived when no specific format of signal waveforms is assumed and when the bandwidth of the signal set is taken into account. Signal sets that achieve the lower bound are also obtained.

Let $\mathbf{s}(t) = [s_1(t), \ldots, s_K(t)]^{\mathrm{T}}$, $0 \le t \le T$, be a vector of K unit-energy signals. The total squared correlation (TSC) of the signal set is $\mathrm{TSC} = \sum_{i=1}^{K}\sum_{j=1}^{K}\left(\int_0^T s_i(t)s_j(t)\mathrm{d}t\right)^2$. The *average* root-mean-square (RMS) bandwidth $b(\mathbf{s}(t))$ of the signal set satisfies $b^2(\mathbf{s}(t)) = \frac{1}{K}\sum_{k=1}^{K}\int_{-\infty}^{\infty} f^2|S_k(f)|^2\mathrm{d}f$ and the signal set is said to have an *average* fractional out-of-band energy (FOBE) bandwidth W at level η if $\epsilon(\mathbf{s}(t)) = \frac{1}{K}\sum_{k=1}^{K}\int_{|f|>W}|S_k(f)|^2\mathrm{d}f \le \eta$, where $0 < \eta < 1$.

II. Results

The same approach as in [3] has been used to obtain the following results.

Proposition 1 *Given T, W and K. If $1 \le (2WT)^2 < (K+1)(2K+1)/6$, then the minimum total squared correlation (MTSC) of the set of K unit-energy signals of duration T and average RMS bandwidth less than or equal to W is*

$$\mathrm{MTSC} = \frac{K^2}{N}\left(1 + \frac{5[(N+1)(2N+1) - 6(2WT)^2]^2}{(N-1)(N+1)(2N+1)(8N+11)}\right)$$

where N is the largest integer less than or equal to K such that $(2WT)^2 \ge [(N+1)(2N-1)(2N+1)]/[5(4N+1)]$. The MTSC is achieved by the signal set

$$\mathbf{s}(t) = \sqrt{\frac{2}{T}}\mathbf{V}\mathbf{\Lambda}^{1/2}\left[\sin\left(\frac{\pi t}{T}\right), \sin\left(\frac{2\pi t}{T}\right), \ldots, \sin\left(\frac{K\pi t}{T}\right)\right]^{\mathrm{T}}$$

where $\mathbf{\Lambda} = \mathrm{diag}(\lambda_1, \ldots, \lambda_K)$

$$\lambda_k = \frac{K}{N}\left(1 + 5[(N+1)(2N+1) - 6(2WT)^2]\cdot \cdot \frac{(N+1)(2N+1) - 6k^2}{(N-1)(N+1)(2N+1)(8N+11)}\right)$$

for $k = 1, \ldots, N$; $\lambda_k = 0$ for $k = N+1, \ldots, K$ and $\mathbf{V}$ is any $K \times K$ orthogonal matrix such that $\mathbf{V}\mathbf{\Lambda}\mathbf{V}^{\mathrm{T}}$ is a unit-diagonal matrix.

If $(2WT)^2 \ge (K+1)(2K+1)/6$ then MTSC $= K$ *and the set of K orthonormal signals achieves the MTSC.*

If $(2WT)^2 < 1$ then no signal set of duration T and RMS bandwidth less than or equal to W exists.

Proposition 2 *Given T, W, K and $0 < \eta < 1$. Let $\{\hat{\psi}_0(t), \hat{\psi}_1(t), \ldots, \hat{\psi}_{K-1}(t)\}$ and $\{\chi_0, \chi_1, \ldots, \chi_{K-1}\}$ be the first K time-truncated, normalized and shifted prolate spheroidal wave functions and their eigenvalues, corresponding to $c = \pi WT$ [4]. If $\frac{1}{K}\sum_{k=0}^{K-1}\chi_k < 1 - \eta \le \chi_0$, then the MTSC of the set of K signals of duration T and average FOBE bandwidth at level η less than or equal to W is*

$$\mathrm{MTSC} = \frac{K^2}{N}\left[1 + \frac{(v(N) - \eta)^2}{u(N) - v^2(N)}\right]$$

where

$$u(N) = \frac{1}{N}\sum_{k=0}^{N-1}(1-\chi_k)^2, \quad v(N) = \frac{1}{N}\sum_{k=0}^{N-1}(1-\chi_k)$$

and N is the largest integer less than or equal to K such that

$$(1 - \chi_{N-1})(v(N) - \eta) \le u(N) - \eta v(N).$$

The MTSC is achieved by the signal set

$$\mathbf{s}(t) = \mathbf{V}\mathbf{\Lambda}^{1/2}\left[\hat{\psi}_0(t), \hat{\psi}_1(t), \ldots, \hat{\psi}_{K-1}(t)\right]^{\mathrm{T}}$$

where $\mathbf{\Lambda} = \mathrm{diag}(\lambda_1, \ldots, \lambda_K)$

$$\lambda_k = \frac{K}{N}\frac{(\eta v(N) - u(N)) + (v(N) - \eta)(1 - \chi_{k-1})}{v^2(N) - u(N)}$$

for $k = 1, \ldots, N$; $\lambda_k = 0$ for $k = N+1, \ldots, K$ and $\mathbf{V}$ is any $K \times K$ orthogonal matrix such that $\mathbf{V}\mathbf{\Lambda}\mathbf{V}^{\mathrm{T}}$ is a unit-diagonal matrix.

If $\frac{1}{K}\sum_{k=0}^{K-1}\chi_k \ge 1 - \eta$ then MTSC $= K$ *and the set of K orthonormal signals achieves the MTSC.*

If $1 - \eta > \chi_0$ then no signal set of duration T and FOBE bandwidth at level η less than or equal to W exists.

[1]This work is supported by the University of Manitoba Graduate Fellowship (UMGF) and by an NSERC Operating Grant.

References

[1] L. R. Welch, "Lower bound on the maximum cross correlation of signals," *IEEE Trans. Inform. Theory*, vol. IT-20, pp. 397-399, May 1974.

[2] J. L. Massey and T. Mittelholzer, "Welch's bound and sequence sets for code-division multiple access systems," *Sequences II, Methods in Communication, Security and Computer Sciences*, R. Capocelli, A. De Santis and U. Vaccaro, Eds. New York: Springer-Verlag, 1993.

[3] D. Parsavand and M. K. Varanasi, "RMS bandwidth constrained signature waveforms that maximize the total capacity of PAM-synhcronous CDMA channels," *IEEE Trans. Commun.*, vol. 44, pp. 65-74, Jan. 1996.

[4] D. Slepian and H. O. Pollak, "Prolate spheroidal wave functions, Fourier analysis and uncertainty–I," *Bell System Tech. J.*, vol. 40, pp. 43-63, Jan. 1961.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Design of Spread Spectrum Sequences Using Ergodic Theory[1]

Chi-Chung Chen
Electrical Engineering Department
UCLA, USA
e-mail: ccchen@ee.ucla.edu

Ezio Biglieri
Dipartimento di Elettronica
Politecnico di Torino, Italy
e-mail: biglieri@polito.it

Kung Yao
Electrical Engineering Department
UCLA, USA
e-mail: yao@ee.ucla.edu

Abstract — **This paper derives general results on the partial auto-correlation function of the optimal spreading sequences to minimize the average error probability under the Standard Gaussian Approximation (SGA) and also provides a real-valued spreading sequence implementation which is at the same time optimal and practical.**

I. Introduction

System performance of asynchronous CDMA communications with single-user matched filter reception critically depends on the auto-correlation and cross-correlation of the spreading sequences. This paper derives general results on the partial auto-correlation function of the optimal spreading sequences to minimize the average error probability under the SGA condition without the assumption of "random processes" on the spreading sequences [1]. Based on the ergodic theory of dynamical systems we can design a family of optimal chaotic spreading sequences and evaluate their performance analytically if the invariant measure of the dynamical system is known. We describe a simple method to implement spreading sequences with optimum auto-correlation properties by using Chebyshev polynomials, which are exact (and hence ergodic) transformations, and admit a closed-form invariant measure.

II. Derivation of Optimal Sequences

An asynchronous CDMA system with K users and spreading factor N is considered. By using a single-user matched-filter detector, the MAI power for the i-th user from all other users can be computed [2] as $\sigma_i^2 = \frac{1}{6N}\sum_{k\neq i}^{K}\sum_{l=1-N}^{N-1}[2C_{k,i}^2(l) + C_{k,i}(l)C_{k,i}(l+1)]$, where $C_{k,i}(l)$ is the partial cross-correlation between the k-th and i-th sequence. Using the identities $\sum_{l=1-N}^{N-1} C_{x,y}(l)C_{x,y}(l+n) = \sum_{l=1-N}^{N-1} C_x(l)C_y(l+n)$ and $C_k(l) = C_k(-l)$ given in [2], the MAI power can be simplified to $\sigma_i^2 = \frac{1}{6N}\sum_{k\neq i}^{K}[2C_k(0)C_i(0) + 4\sum_{l=1}^{N-1} C_k(l)C_i(l) + \sum_{l=0}^{N-1} C_k(l)C_i(l+1) + C_k(l+1)C_i(l)]$. With the normalization $C_i(0) = 1$, the solution that minimizes MAI power is given by $C_k(l) = (-1)^l(r^{l-N} - r^{N-l})/(r^{-N} - r^N)$ where $r = 2-\sqrt{3}$, and the corresponding minimum MAI power is $\sigma_{opt}^2 = \sqrt{3}(K-1)(r^{-2N} - r^{2N})/6N(r^{-2N} + r^{2N} - 2)$. Note that when $l \ll N$, $C_k(l) \approx (-r)^l$ which decays exponentially with alternative sign. Moreover, the minimum MAI power is given by $\sigma_{opt}^2 = \sqrt{3}(K-1)/6N$ as N is large, which increases by 15% the number of users achieved with white sequences, i.e., $(K-1)/3N$.

III. Sequences Design Using Ergodic Theory

For spreading sequences generated by ergodic deterministic dynamical systems, the performance can be computed analytically by using the Birkhoff individual ergodic theory. The n-th ($n \geq 2$) degree Chebyshev polynomials defined by $T_n(x) \equiv \cos(n \arccos(x))$ with invariant measure $\rho(x)dx = dx/\pi\sqrt{1-x^2}$ is considered. The auto-correlation functions for these Chebyshev sequences can be computed using ergodic theory and is given by $< C_x(l) >= \frac{N}{2}\delta(l)$. Therefore, the system performance of an asynchronous CDMA system using Chebyshev sequences is identical to the random white sequences with the MAI power $\sigma^2 = (K-1)/3N$.

Since the auto-correlation function of a Chebyshev sequence is a Kronecker delta function, we can design the optimal spreading sequences by passing these Chebyshev sequences through a low-pass filter with a single pole at $(-r)$. Then each non-overlapped section of the output sequences is assigned to a different user. The system performance comparison using various spreading sequences are shown in Figure 1. These simulation results show that the optimal sequences are better than random white sequences by about 15% in terms of allowable number of users, which is consistent with the analytical expression.

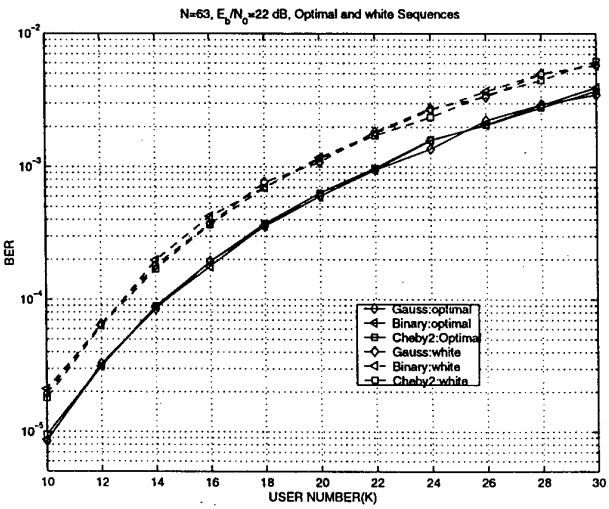


Figure 1: Asynchronous CDMA performance comparison using various optimal and white sequences.

References

[1] G. Mazzini, R. Rovatti, and G. Setti, "Interference Minimization by Auto-Correlation Shaping in Asynchronous DS-CDMA Systems: Chaos-Based Spreading is Nearly Optimal," *IEE Electr. Lett.* vol. 35. pp. 1054-5, June 1999.

[2] M. B. Pursley and D. V. Sarwate, "Performance Evaluation for Phased-Coded Spread-Spectrum Multiple-Access Communication-Part I and II," *IEEE Trans.* **COM-25**, 1977.

[1]This work is partially supported by MURI-ARO grant DAA G55-98-0269 and NASA/Dryden grant NCC2-374.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Two-Dimensional Sequence Estimation

Richard E. Blahut
University of Illinois

Loren E. Laybourn
University of Washington

Abstract — **An algorithm is described for demodulating full-surface two-dimensional data, such as two-dimensional on-off keying, in the presence of two-dimensional intersymbol interference, a topic that is becoming important in the field of optical recording.**

I. Introduction

Page-oriented storage systems are full-surface recording systems that use two-dimensional waveforms to record the user data. In contrast to those older recording methods that define one-dimensional tracks on a two-dimensional surface, the recording waveforms in a full-surface recording system are truly two-dimensional. Data is densely packed in both the horizontal and the vertical directions and, in a high-density recording system, intersymbol interference will be present in both the horizontal and the vertical directions because of the need to pack data closely in comparison with the resolution of the read transducer, whether that transducer be a magnetic read head or an optical lens system. In a high density waveform, the demodulator must be able to recover the stored user data in the presence of two-dimensional intersymbol interference, as well as additive noise and storage media defects. A two-dimensional waveform can be used to obtain a desired storage density only if each pattern is uniquely recognizable by a computationally tractable algorithm so that the correct user data can be recovered by the demodulator even in the presence of the storage impairments mentioned above.

A two-dimensional sequence estimation algorithm may be regarded as a generalization of the Viterbi algorithm to a two-dimensional trellis, which is a trellis standing on $\mathbf{Z}^2$ with branches at each trellis site connecting every node at that site to one of the nodes at each of the four nearest neighboring sites. The algorithm finds, at minimum-euclidean distance from a given data array of numbers, a set of nodes comprised of one node at each site such that nodes at neighboring sites are connected by branches. When used to demodulate a two-dimensional senseword with two-dimensional intersymbol interference in white gaussian noise, the performance is nearly the performance of a two-dimensional maximum-likelihood demodulator provided that E_b/N_0 is above some critical value.

II. The Laybourn Algorithm

Two-dimensional intersymbol interference is a straightforward generalization of one-dimensional intersymbol interference to two dimensions. Algorithms for processing intersymbol interference and recovering data, however, do not generalize so easily. We are interested in algorithms for minimum euclidean-distance demodulation, which for white gaussian noise is equivalent to maximum-likelihood demodulation.

The generalization of a trellis to a two-dimensional structure is straightforward in principle, but it is not entirely straightforward to formalize this generalization or to portray the trellis structure in a useful form. Consider the two-dimensional integer lattice $\mathbf{Z}^2$. The sites of the trellis are the lattice points of $\mathbf{Z}^2$. Standing on each point of the lattice $\mathbf{Z}^2$ is an identical column of nodes. Each node represents a state. At each trellis site branches every node at that site is connected to one or more nodes at each of the four neighboring sites.

The Viterbi algorithm, which is a systematic method of finding a preferred path in a one-dimensional trellis, does not generalize directly to two dimensions. More generally, the dynamic programming principal does not directly apply to the problem of searching a two-dimensional trellis.

The notions of *past* and *future*, which are natural in one dimension, do not have immediate counterparts in two dimensions. Instead, more advanced notions such as *neighbor*, *region*, *inside*, and *outside* must be introduced. Although such notions themselves are not very difficult, they are more difficult than the one-dimensional notions of past and future. In particular, all of the familiar techniques surrounding the Viterbi algorithm become much more difficult when generalized to this two-dimensional setting. For one thing, the boundary of a neighborhood is variable in size, which is quite different from the one-dimensional case. To construct a systolic two-dimensional trellis-search algorithm, some approximations are inevitable.

In this paper, we shall describe and evaluate a recursive formulation of a demodulator for two-dimensional sensewords with intersymbol interference. Because the first author for some time has been referring to the algorithm as the *Laybourn algorithm*, we shall continue to use this terminology, though with some breach of modesty for the second author.

However, if the signal-to-noise ratio (as measured by E_b/N_0) is above a critical value, which we may call the critical temperature, then there seems to be a kind of phase transition in the nature of the two-dimensional problem. The structure of the problem freezes and, with high probability, only local decisions are needed to find the proximate codeword. Conversely, the structure of the problem thaws at low E_b/N_0, and an algorithm that uses only local decisions will fail.

References

[1] R. E. Blahut, L. E. Laybourn, and J. T. Russell, "Alignment Method and Apparatus for Retrieving Information From a Two-Dimensional Data Array." U.S. Patent Application, Filed May 7, 1997.

[2] K. Chugg, "Performance of Optical Digital Page Detection in a Two-Dimensional ISI/AWGN Channel," *Proceedings of the 1996 30th Asilomar Conference on Signals Systems and Computers*, (Sponsored by IEEE), pp. 958–962, pp. 1058–6393 CCSCE2.

[3] G. D. Forney, "The Viterbi Algorithm," *Proceedings of the IEEE*, vol. 61, no. 3, pp. 268-278, 1973.

[4] J. Heanue, M. Bashaw, and L. Hesselink, "Decision Feedback Viterbi Detection in Page Oriented Optical Memory," *Journal of the Optical Society of America A*, vol. 12, pp. 2432, 1995.

[5] B. M. King and M. A. Neifeld, "Parallel Detection Algorithms for Page-Oriented Optical Memories," *Applied Optics*, vol. 37, pp. 6275–6298, 1998.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Efficient Coding for High-Order Spectral-Null Sequences*

Yan Xin and Ivan J. Fair

Department of Electrical and Computer Engineering
University of Alberta, Edmonton, Alberta, T6G 2G7, Canada

TR*Labs*, #800 Park Plaza, 10611-98 Avenue
Edmonton, Alberta, T5K 2P7, Canada

E-mail: xiny@ee.ualberta.ca, fair@ee.ualberta.ca

Abstract — **We show that block coded sequences are cycloergodic, and based on this property, we introduce a new non-probabilistic formula to calculate the average power spectral density of these sequences. We present a new sufficient condition to construct codes with an arbitrarily high-order spectral-null at zero frequency. Given this condition, we outline two new coding schemes and use them to generate new classes of efficient high-order spectral-null sequences.**

I. Introduaction

First-order spectral-null codes have received considerable attention in the literature. Recently, high-order spectral-null sequences have also attracted interest [1]. In high-order spectral-null codes, the power spectrum of the encoded sequence and its higher-order derivatives are zero at zero frequency to achieve a wide spectral notch at low-frequency. We denote sequences with an Mth-order spectral null at zero frequency to be dc^M-codes, individual words to be dc^M-words, and denote these sequences and words to be from sets $\Phi(N,M)$ and $\varphi(N,M)$ respectively, where N is the codeword length. Let the source word length be I. Such block codes are called I/N codes.

Construction of high-order spectral-null sequences is usually based on concatenation of block codewords with the same order spectral-null [1]. We denote $\Phi(N,M\,|\,[\varphi(N,M)])$ to be a subset of $\Phi(N,M)$ for this coding scheme (Mth-order zero-disparity). In this approach, as the order of spectral-null increases, the code rate becomes very low and makes coding impractical. One proposed approach [2] to increase the cardinality of useable codewords of those codes is to employ codewords with fixed moments. We introduce a new class of efficient dc^M-codes composed of block dc^{M-1}-words. We denote this subset of dc^M-codes as $\Phi(N,M\,|\,[\varphi(N,M-1)])$. Comparison of cardinality of these schemes is shown in Fig. 1.

II. Block Encoded Sequences With High-Order Spectral-Null

Assuming that the input source sequence of a line encoder is composed of independent identically distributed (i.i.d.) symbols, the state sequence is a stationary Markov chain. We show that if the Markov chain has finite number of states and is irreducible and aperiodic (i.e. ergodic), the output codeword sequence is both wide-sense stationary and wide-sense ergodic, and the output symbol sequence $X(n)=\{x_n\}$ is both wide-sense cyclostationary and wide-sense cycloergodic with the period of the word length. We show that the statistical mean and autocorrelation of a cycloergodic cyclostationary stochastic process evaluated by averaging over ensemble statistics are identical to the asymptotic time average and time average autocorrelation of one sample function of the process.

The limiting time-average autocorrelation and limiting power spectrum are a Fourier transform pair [3, p. 74]. Therefore, the average power spectrum $H_X(\omega)$ equals the limiting time-averaged (smoothed) periodogram given in [3, p. 81]:

$$H_X(\omega)=\lim_{L\to\infty}\lim_{K\to\infty}\frac{1}{2K+1}\sum_{k=-K}^{K}\frac{1}{2L+1}\left|\sum_{n=k-L}^{k+L}x_n e^{-j\omega n}\right|^2. \quad (1)$$

By taking derivatives of (1), we conclude that if the first M-1 moments of every codeword are zero and the M-1th moment of the sequence is bounded, then the sequence concatenated by these codewords has an Mth-order spectral-null at zero frequency.

III. Constructions of DC^M-Codes

We present explicit constructions to implement spectral-null codes of order M using (A) codewords from the set of $\Phi(N,M\,|\,[\varphi(N,M-1)])$ and (B) codewords from $\Phi(N,M\,|\,[\varphi(N,M-1),\varphi(N,M)])$. We propose two methods of doing so: with coding tables and through guided scrambling (GS) [4]. Define two codewords to be a codeword pair if they have the same zero moments and if they have the same absolute values and opposite sign for nonzero moments. In approach (A), a source word is mapped to a set of codewords where there exists at least one pair of codewords from $\varphi(N,M-1)$. Encode the source words to satisfy the requirement for a bounded M-1th moment of the coded sequence. In approach (B), the only difference from (A) is that a source word is assigned to a unique codeword from $\varphi(N,M)$ or at least one pair of codewords from $\varphi(N,M-1)$. This improves code efficiency and performance. Fig. 2 presents power spectrum results.

References

[1] R. M. Roth, P. H. Siegel and A. Vardy, "High-order spectral-null codes - constructions and bounds," *IEEE Trans. Inform. Theory*, vol. 40, no. 6, pp. 1826-1840, Nov. 1994.

[2] L. M. G. M. Tolhuizen, K. A. S. Immink, and H. D. L. Hollmann, "Construction and properties of block codes for partial-response channel," *IEEE Trans. Inform. Theory*, vol. 41, no. 3, pp. 2019-2026, Nov. 1995.

[3] W. A. Gardner, *Statistical Spectral Analysis: A Non-Probabilistic Theory*. Prentice-Hall, Englewood Cliffs, New Jersey, 1988.

[4] I. J. Fair, W. D. Grover, W. A. Kryzmien, and R. I. MacDonald, "Guided scrambling: a new line coding technique for high bit rate fiber optic transmission systems," *IEEE Trans. Commun.*, vol. 39, no. 2, pp. 289-297, Feb. 1991.

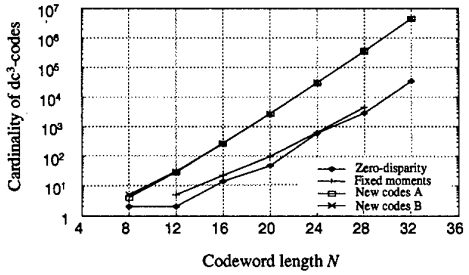


Fig. 1: Comparison of cardinality.

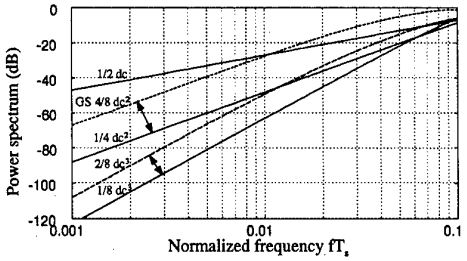


Fig. 2: Power spectrum of dc-, dc^2-, and dc^3-codes of zero-disparity scheme (solid lines) and new coding schemes (dash lines).

*This work was supported by the Natural Sciences and Engineering Research Council of Canada and TR*Labs*.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Distributions of the Output MAI of Linear MMSE Multiuser Receivers in DS-CDMA Systems

Junshan Zhang
School of ECE, Purdue Univ.
e-mail: junshan@ecn.purdue.edu

Edwin K. P. Chong[1]
School of ECE, Purdue Univ.
e-mail: echong@ecn.purdue.edu

David N. C. Tse[2]
Dept. EECS, U.C. Berkeley
e-mail: dtse@eecs.berkeley.edu

Abstract — **We establish the Guassianity of the output multiple-access interference (MAI) of linear MMSE receiver in a large DS-CDMA network.**

I. INTRODUCTION

Bit error probability (BEP) is an important performance measure in wireless communications, and is determined by the overall interference consisting of the MAI and background noise. In this paper, we study the behavior of MAI at the output of the minimum-mean-square-error (MMSE) receiver employed in a DS-CDMA system. We focus on systems with random spreading. The random signature model is applicable to many scenarios, for example, systems employing very long pseudo-random spreading sequences, and systems in which the signatures of the users are repeated from symbol to symbol, but they are randomly and independently selected initially. By exploiting results in martingale limit theory and random matrix theory, we show that as the processing gain increases, (1) the output MAI of the MMSE receiver is asymptotically Gaussian; and (2) for almost every realization of the signatures and received powers, the conditional distribution of the output MAI converges to the same Gaussian distribution as in the unconditional case. These results are quite general and are useful for performance analysis such as the calculation of the bit error probability. We note that Verdú and Shamai [2] obtained that for almost every choice of signatures, the output MAI of the conventional receiver converges to a Gaussian random variable, while Poor and Verdú [1] established the Gaussian nature of the MAI-plus-noise at the output of the MMSE receiver in several asymptotic scenarios (the output MAI vanishes in these scenarios).

II. MAIN RESULTS

Consider the following discrete-time model for the uplink of a synchronous CDMA system. The baseband received signal at the front end of the receiver is

$$Y^{(N)} = \sum_{i=1}^{K} \sqrt{P_i} b_i s_i + V,$$

where the b_i's are the information symbols, the P_i's are the received powers, and V is background noise that comes from the sampling of the ambient white Gaussian noise. We assume that users choose their signatures randomly and independently. We restrict our attention to binary signatures. The model for binary random signatures is as follows: $s_i = \frac{1}{\sqrt{N}}(s_{i1}, \ldots, s_{iN})^T$, where the s_{in}'s are i.i.d. with $P\{s_{in} = 1\} = P\{s_{in} = -1\} = \frac{1}{2}$, $n = 1, \ldots, N$, and $i = 1, \ldots, K$. Moreover, in a practical wireless system, fading is ubiquitous, making perfect power control impossible. Therefore, we assume that the received powers are random.

We consider user 1 without loss of generality. The MMSE receiver generates an output of the form of $c^t Y^{(N)}$, where c is chosen to minimize the mean square error

$$J = E\left[(c^t Y^{(N)} - b_1)^2 \,\middle|\, P_1, S\right],$$

where S is the collection of signatures of all the users. After some algebra, we can get the expressions for the linear MMSE receiver and hence the output MAI.

Our results are asymptotic in nature, with both K and N going to infinity, while keeping K/N fixed. First we impose the following assumptions on the received powers:

(3.B1) The empirical distribution function of $\{\mu_1, \ldots, \mu_K\}$ converges weakly to a distribution function F_μ;

(3.B2) The second moments of the received powers are bounded.

Theorem 2.1 *(Unconditional MAI) Suppose Conditions 3.B1 and 3.B2 hold. Then the output MAI of the MMSE receiver has a limiting Gaussian distribution (as $N \to \infty$).*

To establish the asymptotic Guassianity of the output MAI conditioned on the signatures and received powers, we need a stronger form of regularity on the received powers. The assumptions we impose on the received powers are as follows:

(3.C1) The joint empirical distribution function of $\{(P_1, \mu_1), \ldots, (P_K, \mu_K)\}$ converges weakly to a distribution function $F_{P,\mu}$ with probability one;

(3.C2) The P_i's are uniformly bounded above;

(3.C3) The μ_i's are bounded below by a positive number.

Theorem 2.2 *(Conditional MAI) Suppose Conditions (3.C1–3.C3) hold. Then the conditional distribution of the output MAI of the MMSE receiver, given the signatures and the receiver powers, converges almost surely (as $N \to \infty$) to the same Gaussian distribution as in the unconditional case.*

Based on the above theorems, we conclude that the overall interference is asymptotically Gaussian, and that from the viewpoints of detection and channel capacity, the signal-to-interference ratio (SIR) is the key parameter that governs the system performance.

[1] Supported by NSF through grant ECS-9501652.

[2] Supported by NSF Early CAREER Award under grant NCR-9734090.

REFERENCES

[1] H. V. Poor and S. Verdú, "Probability of Error in MMSE Multiuser Detection," *IEEE Trans. on Inform. Theory*, vol. 43, pp. 858–871, 1997.

[2] S. Verdú and S. Shamai, "Spectral Efficiency of CDMA with Random Spreading," *IEEE Trans. on Inform. Theory*, vol. 45, pp. 622–640, 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Alpha-stable Models of Multiuser Interference

Brian L. Hughes[1]
Center for Advanced Computing and Communication
Department of Electrical and Computer Engineering
North Carolina State University
Raleigh, NC 27695-7914
e-mail: blhughes@eos.ncsu.edu

Abstract — **We present a model for the interference generated by a collection of geographically-distributed, bursty transmitters. Transmitters begin transmission at random times and locations, determined by a Poisson process in space and time. As each transmitted signal propagates to the receiver, it is attenuated by a power-law path loss and shifted in phase by a random angle. We show that the combined interference of all transmitters can be represented as a moving average of Lévy motions — impulsive, α-stable random processes which are analogous to filtered white noise. Further, these results can be adapted to include the effects of fading, delay spread, Doppler, and different modulation schemes. The tools developed here may be useful for modeling other impulsive phenomena, such as automobile ignition noise, atmospheric noise, and radar clutter.**

I. Summary

In code-division multiple access (CDMA), transmitters share a common frequency band and are distinguished at the receiver on the basis of unique signature sequences. It often happens that these sequences are not orthogonal, so that a conventional correlation receiver passes not only the desired signal, but also co-channel interference due to the other active transmitters. When the number of interfering transmitters is small, this multiuser interference can be eliminated in principle with multiuser detection. For a large population of transmitters, however, this generally is not possible. Under these circumstances, multiuser interference is often the main factor limiting the performance of CDMA networks.

As with any type of interference, accurate and tractable models are essential in communication system design. It is not surprising then that there is an extensive literature on modeling multiuser interference. Most of this work deals with interference produced by a fixed population of equal (or nearly equal) power transmitters, and suggests that Gaussian-mixture models are often suitable. These assumptions are often appropriate for the reverse link in cellular CDMA, where power control prevents any one mobile from dominating.

A different perspective on multiuser interference is offered by Sousa and Silvester in [2], and in subsequent extensions and applications [3, 1]. In these papers, transmitters are distributed at random locations determined by a spatial Poisson process. There is no power control and so, due to different path losses, the signals of different transmitters arrive at the receiver with vastly different powers. These assumptions are appropriate for ad-hoc packet radio networks, where there is no central base station. Under these conditions, Sousa and Silvester [2] obtain non-Gaussian stable probability models for multiuser interference. Non-Gaussian stable probability densities are often regarded as models of impulsive phenomena, since their tails are heavier than those of the Gaussian density.

The results in [2, 3, 1] present a static, discrete-time model of multiuser interference. They essentially characterize the distribution of a single interference sample, after the process has been filtered and sampled. It is natural, however, to ask about the properties of the continuous-time interference that arrives at the receiver front-end. In fact, many fundamental communications questions are more naturally addressed in the context of continuous-time interference. For example, does linear filtering and sampling extract sufficient statistics for signal detection from the received signal? How does the interference evolve with time, and how is this time dependence affected by the modulation scheme and bandwidth of the interfering transmitters? How is it affected by vehicular motion? What is the dependence between interference at different frequencies, and how is it affected by channel delay spread? All of these questions suggest the importance of examining the continuous-time behavior of multiuser interference.

In this paper, we present a dynamic model for the continuous-time interference produced by a collection of geographically-distributed, bursty transmitters. Transmitters begin transmission at random times and locations, determined by a Poisson process in space and time. As each transmitted signal propagates to the receiver, it is attenuated by a power-law path loss and shifted in phase by a random angle. We show that the combined interference of all transmitters can be represented as a moving average of Lévy motions — impulsive, α-stable random processes which are analogous to filtered white noise. Further, these results can be adapted to include the effects of fading, delay spread, Doppler, and different modulation schemes. The tools developed here may be useful for modeling other impulsive phenomena, such as automobile ignition noise, atmospheric noise, and radar clutter.

[1]This work was supported in part by the National Science Foundation under grant CCR-9903107, and by the Center for Advanced Computing and Communication.

References

[1] J. Ilow, D. Hatzinakos, "Analytic alpha-stable noise modeling in a Poisson field of interferers or scatterers," *IEEE Trans. Sig. Proc.*, vol. 46, no. 6, pp. 1601-1611, June 1998.

[2] E. S. Sousa and J. A. Silvester, "Optimum transmission ranges in a direct-sequence spread-spectrum multihop packet radio network," *IEEE J. Selected Areas in Commun.*, vol. 8, no. 5, pp. 762-771, June 1990.

[3] E. S. Sousa, "Performance of a spread spectrum packet radio network link in a Poisson field of interferers," *IEEE Trans. Inform. Theory*, vol. 38, no. 6, pp. 1743-1754, Nov. 1992.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Asymptotic Performance of M-Estimator-Based Multiuser Detectors in Rayleigh Fading Non-Gaussian Channels

H. Vincent Poor[1]
Electrical Engineering Department
Princeton University
Princeton, NJ 08544
e-mail: poor@princeton.edu

Mario Tanda
Dip. di Ing. Elettronica e
delle Telecomunicazioni
Via Claudio 21, Napoli, Italy
e-mail: tanda@unina.it

Abstract — **This paper deals with the asymptotic performance analysis of M-estimator-based multiuser detectors designed for noncoherent detection of DPSK signals in fading non-Gaussian channels.**

I. Introduction

Multiple-access channels are inherently non-Gaussian in nature due to the presence in the channel of highly structured multiple-access interference. Moreover, for many multiple-access channels the ambient noise is known through experimental measurements to be decidedly non-Gaussian. The problem of joint mitigation of multiple-access interference (MAI) and non-Gaussian interference is a challenging one, since the reduction of MAI often relies on linear separating structures while the mitigation of impulsive noise typically relies on nonlinear detectors. Nevertheless, considerable progress has been made on this problem (see [2] for the additive-noise channel model and [1] for channels that exhibit fading). In this paper the asymptotic probability of error of the M-estimator-based multiuser detectors proposed in [1] for (differential) noncoherent detection of DPSK signals in fading non-Gaussian channels is derived under the assumption that the channel fading is Rayleigh distributed.

To introduce the M-estimator-based multiuser detector let us consider a synchronous CDMA system where the signal of each of K active users arrives at the receiver through an independent, single-path, slowly-fading channel. At the receiver, after complex basebanding, chip matched filtering, and chip rate sampling, the resulting discrete-time signal corresponding to the $i-$th signaling interval is given by

$$r_n(i) = \sum_{k=1}^{K} g_k(i) b_k(i) a_n^k + w_n(i) \qquad n = 1, \ldots, N \qquad (1)$$

where N is the processing gain, $a_1^k, a_2^k, \ldots, a_N^k$ is the normalized signature sequence of the $k-$th user, $g_k(i)$ is the $k-$th channel fading coefficient and the sequence of noise samples $\{w_n(i)\}$ is assumed to be a sequence of independent and identically distributed complex random variables whose in-phase and quadrature components are independent non-Gaussian random variables with a common probability density function f. The synchronous signal model (1) can be written in matrix notation as

$$\underline{r}(i) = \underline{H}\, \underline{\theta}(i) + \underline{w}(i) \qquad (2)$$

where the real vectors $\underline{r}(i)$, $\underline{w}(i)$ and $\underline{\theta}(i)$ are obtained by stacking the real and imaginary components of the corresponding complex vectors.

[1]This work was supported in part by the U.S. National Science Foundation under Grant CCR-99-80590.

The basic idea of M-estimator-based multiuser detection is to detect the symbols in (2) by first estimating the vector $\underline{\theta}(i)$, and then extracting symbol estimates from these continuous estimates. The required estimates of $\underline{\theta}(i)$ are obtained by using an estimator of the class of M-estimators proposed by Huber. These estimators minimize a function $\rho(\cdot)$ (called the *penalty function*) of the residuals:

$$\underline{\hat{\theta}}(i) = \arg \min_{\underline{\theta}(i) \in R^{2K}} \sum_{j=1}^{2N} \rho \left(r_j(i) - \sum_{l=1}^{2K} h_{jl} \theta_l(i) \right) \qquad (3)$$

where $r_j(i)$ and $\theta_k(i)$ are the $j-$th and the $k-$th element of the vectors $\underline{r}(i)$ and $\underline{\theta}(i)$, respectively, and h_{jk} is the $j,k-$th element of the matrix $\underline{H}$. Given such an estimator, the detected symbols are given by $\hat{b}_l(i) = \mathrm{sgn}\left\{ \Re \left[\hat{\theta}_l(i) \hat{\theta}_l^*(i-1) \right] \right\}$, where $\Re[\cdot]$ denotes real part and $\hat{\theta}_l(i) \triangleq \hat{\theta}_l(i) + j\hat{\theta}_{l+K}(i)$.

The asymptotic probability of error for large processing gain ($N \to \infty$) for the M-estimator-based multiuser detectors can be obtained taking into account that under certain regularity conditions, the M-estimators defined by (3) are consistent and asymptotically normal. Specifically, the asymptotic probability of error for the $l-$th user can be shown to be

$$P_l(e) = \frac{1}{2} \left(1 - \frac{\rho_l}{1 + \frac{\nu^2}{\sigma^2 SNR_l} \left[\underline{R}^{*-1} \right]_{ll}} \right) \qquad (4)$$

where ρ_l is the $l-$th channel fading correlation coefficient, $\nu^2 \triangleq E\left[\psi^2(x)\right] / E^2\left[\psi'(x)\right]$ with $\psi(\cdot) = \rho'(\cdot)$, $\left[\underline{R}^{*-1} \right]_{ll}$ denotes the $ll-$th component of the inverse of the cross-correlation matrix of the random infinite-length signature waveforms of the K users, σ^2 represents the variance of the in-phase and quadrature components of the noise samples and $SNR_l \triangleq E\left[|\, g_l(i) \,|^2 \right] / \sigma^2$. From (4) it follows immediately that the asymptotic error rate of the linear decorrelating detector (i.e., $\psi(x) = x$) with DPSK depends on the noise distribution only through its variance (as one would expect). Moreover, for sufficiently high values of SNR, (4) suggests that the M-decorrelators' performance present an error floor that depend mainly on the fading correlation coefficient. Specifically, the slower the fading rate, the lower the error floor.

References

[1] H. V. Poor and M. Tanda, "Multiuser Detection in Fading Non-Gaussian Channels," *In Proc. of 33rd Annual Conference on Information Sciences and Systems,* The Johns Hopkins University, Baltimore, MA, March 1999.

[2] X. Wang and H.V. Poor, "Robust Multiuser Detection in Non-Gaussian Channels," *IEEE Transactions on Signal Processing,* vol.47, Feb. 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Large System Error Probability of Multiuser Decision Feedback Receivers[1]

Rapeepat Ratasuk and Michael L. Honig
Department of Electrical and Computer Engineering
Northwestern University
2145 Sheridan Road
Evanston, IL, USA 60208-3118
e-mail: {ratasuk, mh}@ece.nwu.edu

Abstract — **The large system limits of the probability of error for multiuser Decision Feedback Detectors (DFDs) are evaluated for synchronous CDMA. Both Successive (S-) and Parallel (P-) DFDs are considered, where the filters are optimized according to the Minimum Mean Squared Error (MMSE) criterion. A comparison of the analytical results with simulation shows that the large system results accurately predict the performance of systems with spreading gain ≥ 128 over a wide range of error rates. The results also show that the P-DFD error rate approaches the single-user bound at high Signal-to-Noise-Ratios (SNRs).**

I. Summary

The multiuser DFD can potentially achieve higher spectral efficiencies than the linear MMSE receiver with little added complexity [1]. Here we are interested in the *average* performance (error probability) of the multiuser DFD for uncoded synchronous CDMA, where the average is over randomly assigned signature sequences. Even with fixed signature sequences, an exact analysis of error probability for a finite-size system is difficult due to error propagation. Averaging over the signatures further complicates the problem. Our approach is to study the large system limit of error probability, where this limit is defined by letting the number of users $K \to \infty$ and the processing gain $N \to \infty$ with $K/N = \alpha$ fixed. This approach has been used in [2] to evaluate the performance of linear MMSE receivers.

We assume the standard baseband CDMA model in which the received vector corresponding to symbol i is

$$\mathbf{r}(i) = \mathbf{P}\mathbf{b}(i) + \mathbf{n}(i) \tag{1}$$

where $\mathbf{P} = [\mathbf{p}_1, \cdots, \mathbf{p}_K]$ is the $N \times K$ matrix of random spreading codes with i.i.d. elements, $\mathbf{b}(i)$ is the vector of binary symbols across users, and $\mathbf{n}$ is the noise. Here we assume that the users are received with equal power, although our results can be generalized to arbitrary power distributions.

The output of the DFD is

$$\mathbf{y}(i) = \mathbf{F}^\dagger \mathbf{r}(i) - \mathbf{B}^\dagger \tilde{\mathbf{b}}(i) \tag{2}$$

where $\tilde{\mathbf{b}}(i)$ is the vector of tentative decisions, and $\mathbf{F}$ and $\mathbf{B}$ are the feedforward and feedback filters, selected to minimize the Mean Squared Error $E[\|\mathbf{b} - \mathbf{y}\|^2]$. For the P-DFD, the tentative decisions $\tilde{\mathbf{b}}(i) = \text{sgn}\left\{\mathbf{F}_{lin}^\dagger \mathbf{r}(i)\right\}$ where $\mathbf{F}_{lin}$ is the linear MMSE filter, and the final decision $\hat{\mathbf{b}}(i) = \text{sgn}\{\mathbf{y}(i)\}$.

[1]This work was supported by ARO under grant DAAD19-99-1-0288.

Our interest is in computing the probability of error $P_e = \Pr\{\hat{b}_k \neq b_k\}$.

We show that as $(K, N) \to \infty$, P_e for the P-DFD approaches the limit

$$P_{\text{P-DFD}} = Q\left(\frac{1}{\sqrt{4P_{\text{LIN}}\alpha + \sigma_n^2}}\right) \tag{3}$$

where P_{LIN} is the large system probability of error for the linear MMSE receiver.

For the S-DFD, users are decoded and cancelled successively. Hence, P_e depends on the user index k. To obtain the large system limit, we let $x = k/K$, where $k = xK \to \infty$ and $0 \leq x \leq 1$. The performance of user $k+1$ depends on the performance of users $1, \ldots, k$. Taking the large system limit gives the following expression for $P_{\text{S-DFD}}(x + dx)$ in terms of $P_{\text{S-DFD}}(v)$, $0 < v < x$,

$$P_{\text{S-DFD}}(x + dx) = 1 - Q\left(\frac{-\gamma_{-1}}{\sqrt{\gamma_{-2}\sigma_n^2 + \sigma_M^2 + \gamma_{-2}\alpha f(x)}}\right) \tag{4}$$

where $\gamma_i = \int \frac{1}{(\lambda+\sigma^2)^i} dG(\lambda)$, $G(\lambda)$ is the asymptotic eigenvalue distribution of the covariance matrix $\mathbf{R}_U = \mathbf{P}_U \mathbf{P}_U^\dagger$, where the columns of $\mathbf{P}_U$ are the spreading codes for the *undetected* users $k+1 < m < K$, and

$$f(x) = \frac{1}{x}\int_0^x P_{\text{S-DFD}}(v)\, dv. \tag{5}$$

The boundary condition is

$$P_{\text{S-DFD}}(0) = P_{\text{LIN}}(\alpha) \tag{6}$$

that is, P_e for the linear MMSE receiver with load α. The relations (4)-(6) can be numerically integrated to obtain $P_{\text{S-DFD}}(x)$ for $0 \leq x \leq 1$.

Comparisons with simulation results show that for $P_e > 10^{-3}$, the large system results accurately predict the performance of a finite-size system with $N \geq 32$. At high $\frac{E_b}{N_0}$'s (> 10 dB), the S-DFD can achieve close to ideal-feedback performance for loads up to $\frac{3}{4}$. At low loads ($\alpha < 0.5$), a lower $\frac{E_b}{N_0}$ (around 6 dB) suffices. For loads $\alpha < 1$, the P-DFD achieves near single-user performance at a sufficiently high $\frac{E_b}{N_0}$.

References

[1] P. Rapajic, M. Honig, and G. Woodward, "Multiuser Decision Feedback Detection: Performance Bounds and Adaptive Algorithms", *Proc. 1998 ISIT*, Cambridge, MA., August 1998.

[2] D. Tse and S. Hanley, "Linear Multiuser Receivers: Effective Interference, Effective Bandwidth and User Capacity," *IEEE Transactions on Information Theory*, vol. 45, pp.641–657, Mar, 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Second Order Asymptotic Optimality of Sequential Design and Change-Point Detection

Mikhail B. Malyutov
Department of Mathematics,
Northeastern University,
Boston MA 02115, USA;
e-mail:MLTV@neu.edu

Ivan I.Tsitovich
Institute for Information
Transmission Problems,
B. Karetny 19, Moscow 101447,
Russia; e-mail: cito@iitp.ru

Abstract — **Asymptotic bounds are derived involving second additive term of order $\sqrt{|\ln\alpha|}$ as $\alpha\to 0$ for the mean length of a controlled sequential discrimination strategy s between two statistical models in a general non-parametric setting. The parameter α is the maximal error probability of s.**

These results are applied to change-point detection.

I. Introduction

The aim of the present report is three-fold:

1. to construct second-order optimal sequential strategies strengthening the traditional ones;
2. to do this for a non-parametric setting with control, indifference zone and general loss of power growth at infinity;
3. to apply our constructions for change-point detection.

We continue [1] devoted to first order optimal tests.

Let $(X,\mathcal{B},\mu)$, $X\subset\mathbf{R}$, be a probability space, $(\mathcal{P},d(\cdot))$ be a metric space, where $\mathcal{P}$ is a subset of the set $\mathcal{A}$ of mutually absolutely continuous probability measures. The set $\mathcal{P}$ is partitioned into sets $\mathcal{P}_0$, $\mathcal{P}_1$ and the indifference zone $\mathcal{P}_+=\mathcal{P}\setminus(\mathcal{P}_1\cup\mathcal{P}_0)$ such that the distance between $\mathcal{P}_0$ and $\mathcal{P}_1$ is positive. We test $H_0: P\in\mathcal{P}_0$ versus $H_1: P\in\mathcal{P}_1$, every decision is good for $P\in\mathcal{P}_+$.

For an $\alpha>0$ introduce α- *strategies* s satisfying condition: $\max_{r=0,1}\sup_{P\in\mathcal{P}_r}\mathbf{P}_P(\delta=1-r)\le\alpha$.

Define $z(P,Q,x)=\log(\frac{dP}{dQ}(x))$, $I(P,Q)=\mathbf{E}_P z(P,Q,x)$, $I(P,\mathcal{R})=\inf_{Q\in\mathcal{R}}I(P,Q)$ for $\mathcal{R}\subset\mathcal{P}$; $A(P)=\mathcal{P}_{1-r}$ for $P\in\mathcal{P}_r$ as the alternative set in $\mathcal{P}$ for P. For $P\in\mathcal{P}_+$, if $I(P,\mathcal{P}_0)\le I(P,\mathcal{P}_1)$, then $A(P)=\mathcal{P}_1$, otherwise, $A(P)=\mathcal{P}_0$. Finally $c(P)=I(P,A(P))^{-1}$.

For a mixed control $\mathbf{u}=(\kappa_1,\dots,\kappa_m)$ on $U=\{1,\dots,m\}$, $P^{\mathbf{u}}$ is a mixture of measures $P^u, u\in U$, while $\mathcal{P}_k^{\mathbf{u}}, k=0,1$, are sets of corresponding distributions from $\mathcal{A}$ with a positive distance between them.

Define $I_{\mathbf{u}}(P,Q)=\sum_{i=1}^m\kappa_i I(P^i,Q^i)$ and introduce $k^*(P)=\max_{\mathbf{u}\in U^*}I_{\mathbf{u}}(P,A_{\mathbf{u}}(P)), c^*(P)=k^*(P)^{-1}$, and let $\mathbf{u}^*=\mathbf{u}^*(P)$ be a control such that $k^*(P)=I_{\mathbf{u}^*}(P,A_{\mathbf{u}^*}(P))$.

II. Non-parametric Second Order Bounds

C1. There is $c>0$ such that for all $P\in\mathcal{P},Q\in\mathcal{P}$, and $u\in U$ $\mathbf{E}_P^u\left(z(P^u,Q^u,X)\right)^2<c$.

C2. There exist $t>0$ and $f>0$ such that $\mathbf{E}_P\left(\sup_{Q\in\mathcal{P}}\exp(-tz(P,Q,X))\right)\le f$ for all $u\in U$ and $P\in\mathcal{P}$.

C3. $D=\int_X z_1(x)\left(a(x)b(x)\right)^{1/2}dx<\infty$, where $z_1(x)=\sup_{Q\in\mathcal{P}}\left|\frac{\partial z(P,Q,x)}{\partial x}\right|$, $\sup_{P\in\mathcal{P}}\int_{-\infty}^x p(t)\mu(dt)\le a(x)$, $\sup_{P\in\mathcal{P}}\int_x^\infty p(t)\mu(dt)\le b(x)$.

C4. There exist $b>0$ and $K_1=K_1(b)$ such that for every n the estimate $\hat{p}=\hat{p}_n$ for the density function of i.i.d.(P) observations $X_1,\dots,X_n$ exists with $\mathbf{E}_P(I(P,\hat{P}))\le K_1 n^{-b}$.

Theorem 1. i. *Under the condition C1 every α-strategy s for the no-control problem satisfies*

$$\mathbf{E}_P^s N\ge c(P)|\log\alpha|+O\left(\sqrt{|\log\alpha|}\right)\qquad(1)$$

for every $P\in\mathcal{P}$.

ii. *For controlled experiments and every $P\in\mathcal{P}$ the inequality* (1) *holds with $c^*(P)$ substituted instead of $c(P)$.*

Theorem 2. *For every $P\in\mathcal{P}$ under the conditions C1-C4 with $b\ge\frac{1}{2}$ there exists an α-strategy s^* such that $\mathbf{E}_P^{s^*}N\le c(P)|\log\alpha|+O\left(\sqrt{|\log\alpha|}\right)$.*

III. Non-parametric Testing with Control

C5. Suppose a sequence of mixed controls $\mathbf{u}_n(P)$, $c>0$ and $K_2=K_2(c)$ exist such that $\mathbf{u}_n(\hat{P}_n)$ is a measurable control for every n and i.i.d.(P) observations $X_1,\dots,X_n$, $P\in\mathcal{P}$ satisfying $\mathbf{E}_P|I_{\mathbf{u}_n(\hat{P}_n)}(P,A_{\mathbf{u}^*(P)}(P))-k^*(P)|\le K_2 n^{-c}$.

Theorem 3. *Under the conditions C1-C5 there exists an α-strategy S^* such that $\mathbf{E}_P^{S^*}N\le c^*(P)|\log\alpha|+O\left(|\log\alpha|^{1-\min(b,c)/2}\right)+O\left(\sqrt{|\log\alpha|}\right)$ for every $P\in\mathcal{P}$.*

IV. Change-Point Detection

Our strategy and bounds appear well-applicable for a non-parametric detection of abrupt change in the distribution of i.i.d. sequence *without* an indifference zone. We use the methodology outlined in [2].

Let the observations $X_1,\dots,X_n,\dots$ be independent, and for $n<\nu$ all have a distribution $P_0\in\mathcal{P}_0$, while all the X_n with $n\ge\nu$ have an unknown distribution $P_1\in\mathcal{P}_1$, where $\nu\ge 1$ is an unknown integer, and $I_1=I(P_1,\mathcal{P}_0)$.

Let N be a change-point estimate, and $a^+=a$, if $a\ge 0$, and $a^+=0$ otherwise. Following [2] we use the functional $\bar{\mathbf{E}}^s(N)=\sup_{\nu\ge1}\operatorname{ess\,sup}\mathbf{E}_{P_1}^s\left((N-\nu+1)^+|X_1,\dots,X_\nu\right)$ with $P_1\in\mathcal{P}_1$ suppressed as the optimality criterion of the strategy s under the restriction $\mathbf{E}_P^s(N)\ge\alpha^{-1}$.

Theorem 4. *Under the condition C1 for every α-strategy and sufficiently small α the following lower bound is valid* $\bar{\mathbf{E}}^s(N)\ge|\log\alpha|I_1^{-1}+O(\log|\log\alpha|)$.

Under the conditions C1-C4 there exists α-strategy s^* such that $\bar{\mathbf{E}}^{s^*}(N)\le|\log\alpha|I_1^{-1}+O\left(|\log\alpha|^{1-b/2}\right)+O\left(\sqrt{|\log\alpha|}\right)$.

References

[1] M.B. Malyutov and I.I. Tsitovich, "Asymptotically Optimal Sequential Testing Hypotheses," *Problems of Information Transmission* (To appear).

[2] G. Lorden, "Procedures for Reaching to a Change in Distribution," *Ann. Math. Statist.*, vol. 42,pp. 1897–1908, 1971.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Convex-Constrained Maximum-Likelihood Detection in CDMA

Peng Hui Tan
Chalmers University of Technology
Dept. of Computer Engineering
SE-412 96 Göteborg, Sweden
phtan@ce.chalmers.se

Lars K. Rasmussen
Chalmers University of Technology
Dept. of Computer Engineering
SE-412 96 Göteborg, Sweden
larsr@ce.chalmers.se

Teng Joon Lim
Centre for Wireless Communication
20 Science Park Rd, Teletech Park
Singapore 117674
cwclimtj@leonis.nus.edu.sg

Abstract — **In this paper we consider the constrained ML problem where the solution vector is restricted to lie within a convex set. An iterative algorithm for solving the convex-constrained ML problems is derived where special cases correspond to multistage interference cancellation structures.**

I. Summary

The detection strategy usually denoted optimal multiuser detection is equivalent to the solution of a (0,1)-constrained maximum-likelihood (ML) problem, a problem which is known to be NP-hard. Here we relax the constraints imposed on the solution vector in order to formalise lower complexity ML detectors [1]. Consider a K-user asynchronous CDMA system with additive white Gaussian noise (AWGN) of variance $\sigma^2 = N_0/2$. Each user transmits a block of L data symbols using BPSK. A minimal set of sufficient statistics of dimension LK is obtained through filtering matched to the received spreading code of the desired user $\mathbf{y} = \mathbf{Rd} + \mathbf{z}$ where $\mathbf{y}$ is the matched filter output vector and $\mathbf{R}$ is the correlation matrix.

The general constrained ML problem for asynchronous CDMA is described as

$$\mathbf{u} = \arg \min_{\mathbf{v} \in \mathbb{D}^{LK}} F(\mathbf{v}) = \arg \min_{\mathbf{v} \in \mathbb{D}^{LK}} \frac{1}{2}\mathbf{v}^{\mathsf{T}}\mathbf{R}\mathbf{v} - \mathbf{v}^{\mathsf{T}}\mathbf{y}. \quad (1)$$

For a closed convex set constraint, an iterative algorithm for solving the problem in (1) can be found by considering a variational inequality (VI) problem which has the same solution as (1).

Definition 1 *The VI problem $VI(G, \mathbb{C})$ is defined as finding a vector $\mathbf{u} \in \mathbb{C} \subset \mathbb{R}^{LK}$ such that*

$$(\mathbf{v} - \mathbf{u})^{\mathsf{T}} G(\mathbf{u}) \geq 0, \qquad \forall\, \mathbf{v} \in \mathbb{C}, \quad (2)$$

where G is a given continuous function from $\mathbb{C}$ to $\mathbb{R}^{LK}$ and $\mathbb{C}$ is a given closed convex set.

Letting $\mathbf{f}(\mathbf{v})$ be the derivative of $F(\mathbf{v})$, the solution to the problem is described in the following lemma.

Lemma 1 (Lemma 3.1 [2]) *Let $\mathbb{C}$ be a closed convex set, and let $\mathbf{f}(\mathbf{u})$ be a continuous function. Then $\mathbf{u}$ is a solution to $(\mathbf{v} - \mathbf{u})^{\mathsf{T}}\mathbf{f}(\mathbf{u}) \geq 0$, for all $\mathbf{v} \in \mathbb{C}$, if and only if*

$$\mathbf{u} = P_{\mathbb{C}}(\mathbf{u} - \omega \mathbf{f}(\mathbf{u})) \qquad \text{for some or all } \omega \geq 0. \quad (3)$$

In Lemma 1, $P_{\mathbb{C}}(\mathbf{y})$ is an orthogonal projection onto the constraining set, $P_{\mathbb{C}}(\mathbf{y}) = \arg\min_{\mathbf{x} \in \mathbb{S}} \|\mathbf{x} - \mathbf{y}\|$. The following iterative algorithm is proposed in [2] for solving a VI problem. Conditions for convergence are considered in [1].

Algorithm 1 *For any initial value $\mathbf{u}_0 \in \mathbb{C}$, let*

$$\mathbf{u}_{m+1} = \mu P_{\mathbb{C}}[\mathbf{u}_m - \omega \mathbf{E}(\mathbf{R}\mathbf{u}_m - \mathbf{y} + \mathbf{K}(\mathbf{u}_{m+1} - \mathbf{u}_m))] + (1 - \mu)\mathbf{u}_m, \quad (4)$$

where $0 < \mu \leq 1$, $\omega > 0$, $\mathbf{E}$ is any positive diagonal matrix, and $m = 0, 1, \ldots, M-1$ is the iteration index. If the orthogonal projection operation can be decoupled into independent element-wise projections, then $\mathbf{K}$ can be either strictly lower triangular, strictly upper triangular or equal to the null matrix $\mathbf{0}$. Otherwise, $\mathbf{K}$ must be equal to the null matrix $\mathbf{0}$.

Algorithm 1 has the form of generalised interference cancellation. The algorithm is serial (successive) in nature when $\mathbf{K}$ is strictly upper or lower triangular. When $\mathbf{K} = \mathbf{0}$, the algorithm becomes parallel in nature, as iteration m only depends on estimates from iteration $m-1$. Let $\mathbf{R}$ be partitioned such that $\mathbf{R} = \mathbf{D} + \mathbf{L} + \mathbf{U}$, where $\mathbf{D}$ is a diagonal matrix and $\mathbf{L}$ and $\mathbf{U}$ are strictly lower and upper triangular, respectively. Special cases of Algorithm 1 are equivalent to known successive and parallel interference cancellation structures. An M-stage successive interference cancellation (SIC) scheme is described as

$$\mathbf{u}_{m+1} = P_{\mathbb{C}}[\mathbf{D}^{-1}(\mathbf{y} - \mathbf{L}\mathbf{u}_{m+1} - \mathbf{U}\mathbf{u}_m)], \quad (5)$$

where $\mathbf{u}_0 = \mathbf{y}$. The relationship between the SIC and the general iterative algorithm is clear from substituting $\mathbf{K} = \mathbf{L}$, $\mathbf{E} = \mathbf{D}^{-1}$ and $\mu = \omega = 1$ into (4). Similarly, the M-stage weighted parallel interference canceller (PIC) is described as

$$\mathbf{u}_{m+1} = P_{\mathbb{C}}[\omega \mathbf{D}^{-1}\mathbf{y} + (\mathbf{I} - \omega \mathbf{D}^{-1}\mathbf{R})\mathbf{u}_m], \quad (6)$$

which can be derived from (4) by taking $\mathbf{K} = \mathbf{0}$, $\mathbf{E} = \mathbf{D}^{-1}$ and $\mu = 1$. Again $\mathbf{u}_0 = \mathbf{y}$.

The orthogonal projection operation, essential for the algorithm, clearly corresponds to the tentative decision function in a cancellation structure. For a box constraint, the orthogonal projection operation can be decoupled into independent element-wise orthogonal projections. Element i of the orthogonal projection vector is in this case

$$(P_{\mathbb{b}}(\mathbf{y}))_i = \begin{cases} y_i & \text{if } -1 < y_i < 1 \\ -1 & \text{if } y_i \leq -1 \\ +1 & \text{if } y_i \geq 1 \end{cases}. \quad (7)$$

The function $P_{\mathbb{b}}(\mathbf{y})$ is incidently identical to the clipped soft decision function suggested for interference cancellation [1].

References

[1] P. H. Tan, L. K. Rasmussen, and T. J. Lim, "Iterative interference cancellation as maximum-likelihood detection in CDMA," in *Proc. Int. Conf. Info., Commun., Sig. Proc. 99*, (Singapore), Dec. 1999.

[2] B. H. Ahn, "Iterative methods for linear complementary problems with upper bounds on primary variables," *Mathematical Programming*, vol. 26, no. 3, pp. 295–315, 1983.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

UMP, ALR and GLR Tests and Some Applications to Coherent Radar Detection

Mostafa Derakhtian, Mohammad M. Nayebi
Department of Electrical Engineering, Sharif University of Technology, Tehran, I.R.IRAN

Abstract – A necessary and sufficient condition for the equivalence of two test functions is stated, also a necessary and sufficient condition for the existance of UMP test is proposed. Then it is shown, for the first time, that in coherent radar detection, UMP test does not exist and ALR and GLR detectors are not equivalent.

I- Introduction

In several detection problems, we have a composite hypothesis test, i.e.a test that at least, a parameter characterizing one of the hypothesis is unknown.

first, we have discussed about the meaning of equivalence of two tests and have stated a necessary and sufficient condition for equivalence of two tests in scaler and vectorial cases and then we have discussed about the existance of UMP test in two- sided hypothesis tests and have found a necessary and sufficient condition for the existanse of UMP test and then by using of theorems we have shown that in the coherent radar detection in gaussian noise, UMP test does not exist and ALR and GLR detectors are not equivalent.

II - Equivalence of two tests

In this section, we propose the concept of equvialence of two tests and conditions of this equivalence. The test which result from the comparison of a function of observation (for example A(x)) with a thershold(η_a) is represented here by T(A), i.e.the test T(A) is a test with decision rule of $A(X) \underset{H_0}{\overset{H_1}{\gtrless}} \eta_a$.

Definition: two tests are equivalent iff they have the same critical region.

Theorem (1): If two test T(A) and T(B) are equivalent then:

$$\forall x_1,x_2: A(x_1)=A(x_2) \Leftrightarrow B(x_1)=B(x_2) \qquad (1)$$

On the other hand, if functions A and B are continuous and equation(1) is satisfied for them, the test T(A) will be equivalent either with T(B) or with T(-B) [1].

Remark (1): Theorem (1) is valid also when we deal with the vector form of observations (e.g. $A(\underline{x}) \underset{H_0}{\overset{H_1}{\gtrless}} \eta_a$) [1].

III - UMP test in two – sided hypothesis tests

UMP test is the most powerful test in the test class of its size. Unfortunately, in general there is not a theorem in literature that answers to this question that whether the UMP test exists in a given problem or not? In this section, we discuss about this problem in two – sided hypothesis tests and propose a way to check for the existance of the UMP.

lemma(1): Necessary and sufficient condition for the existance of UMP test in a two-sided hypothesis test (e.g. $\begin{cases} H_0:\theta=\theta_0 \\ H_1:\theta\neq\theta_0 \end{cases}$) is that the likelihood ratio, i.e. $LR(t;\theta) = \frac{L(t;\theta)}{L(t;\theta_0)}$ has two following properties[1]:

a) For any θ , solution of $LR(t_1;\theta) = LR(t_2;\theta)$ is independent of θ .

b) For any t, sign of $\frac{\partial LR(t;\theta)}{\partial t}$ is independent of θ .

Lemma (2): If in a test, likelihood ratio is in the form of $LR(\underline{x};\theta)=\frac{f(\underline{x};\theta)}{f(\underline{x};\underline{\theta}_0)}$ (in which $\underline{x}$ and $\underline{\theta}$ are n-dimensional and k-dimensional vectors, respectively), necessary and sufficient condition for existance of UMP test in two-sided hypothesis test, is[1]:

1) For any $\underline{\theta}$, solution of $LR(\underline{x}_1;\underline{\theta})=LR(\underline{x}_2;\underline{\theta})$ is independent of $\underline{\theta}$:

2) For $1\le i\le n$, sign of $\frac{\partial LR(\underline{x},\underline{\theta})}{\partial x_i}$ is independent of $\underline{\theta}$.

IV- Applications to coherent radar detection

Example (1): In the detection of coherent radar signals with unknown Doppler shift, we have the following hypothesis test:

$$\begin{cases} H_0:\underline{x}=\underline{n} \\ H_1:\underline{x}=\underline{s}+\underline{n} \end{cases} \qquad (2)$$

where $\underline{x}$, $\underline{s}$ and $\underline{n}$ are N-tuple vectors of observed data, signal and noise, respectively.Noise is assumed to be zero-mean gaussian, and

$$\underline{s}=v\exp(j\phi)\underline{\delta} \qquad (3)$$

where v is the amplitude, and ϕ is the initial phase of the signal and $\underline{\delta}=\left[1\; e^{j\Omega}\; e^{2j\Omega}\; \ldots\; e^{(N-1)j\Omega}\right]^T$, where Ω is the normalized Doppler frequency.

The vector $\underline{S}$ is considered as an unknown vector and we can rewrite the problem of hypothesis test as:

$$\begin{cases} H_0:\underline{s}=\underline{0} \\ H_1:\underline{s}\neq\underline{0} \end{cases}$$

The likelihood ratio equals[2]

$$LR(\underline{x};\underline{s})=\frac{f(\underline{x};\underline{s})}{f(\underline{x};\underline{\theta})}=\exp\left[-\underline{s}^H\underline{\Sigma}_{nn}^{-1}\underline{s}+2\,\mathrm{Re}(\underline{x}^H\underline{\Sigma}_{nn}^{-1}\underline{s})\right] \qquad (4)$$

where Σ_{nn} is the noise covariance matrix. According to Lemma(2), if the UMP test exists then the solution of the following equation should be independent of $\underline{s}$.

$$LR(\underline{x}_1;\underline{s})=LR(\underline{x}_2;\underline{s}) \Rightarrow \mathrm{Re}(\underline{x}_1^H\underline{\Sigma}_{nn}^{-1}\underline{s})=\mathrm{Re}(\underline{x}_2^H\underline{\Sigma}_{nn}^{-1}\underline{s}) \qquad (5)$$

But if $\underline{x}_2=\underline{x}_1+j\underline{\Sigma}_{nn}\underline{s}$ is selected, then this solution which is dependent of $\underline{s}$ satisfies the eq.(5). Therefore, the UMP test dose not exist.

Example(2): Here, we suppose that parameters Ω, ϕ and V in example(1), are unknown but Ω and ϕ are random variables with uniform distribution in the interval[$0,2\pi$) and V has Rayleigh distribution with paramater a, hence we can use ALR detector in this problem. ALR and GLR detectors, for this problem, are in the following form [2 - 4]:

$$LR(\underline{x},\Omega)=\frac{1}{1+2a\,\underline{\delta}^H\underline{\Sigma}_{nn}^{-1}\underline{\delta}}\exp\left(\frac{2a\left|\underline{x}^H\underline{\Sigma}_{nn}^{-1}\underline{\delta}\right|^2}{1+2a\,\underline{\delta}^H\underline{\Sigma}_{nn}^{-1}\underline{\delta}}\right) \qquad (6)$$

$$A(\underline{x}) = \int_0^{2\pi} LR(\underline{x},\Omega)\,d\Omega \;,\; G(\underline{x}) = \max_{\Omega}\,[LR(\underline{x},\Omega)] \qquad (7)$$

If it is supposed that N=2, $\underline{x}=(x_1,x_2)$ and $\Sigma_{nn}=I$. Above detectors will be in the following form:

$$A(\underline{x})=\frac{1}{2\pi(1+4a)}\exp\left[\frac{2a}{1+4a}(|x_1|^2+|x_2|^2)\right]I_0\left[\frac{4a|x_1||x_2|}{1+4a}\right] \qquad (8)$$

$$G(\underline{x})=\frac{1}{1+4a}\exp\left[\frac{2a}{1+4a}(|x_1|+|x_2|)^2\right] \qquad (9)$$

where $I_0(.)$ is the modified Bessel function. We see that $G(x_1,x_2)$ is costant over $|x_1|+|x_2|=$ cte, but $A(x_1,x_2)$ is not costant over $|x_1|+|x_2|=$ cte, therefore eq.(1) is not satisfy and consequently GLR and ALR detector are not equivalent.

References

[1] M. Derakhtian, "Investigations on the methods of composite hypothesis test", M. Sc. Thesis, Sharif University of Tecnnology, Tehran, Iran, 1998.

[2] M.M. Nayebi, M.R.Aref, M.H. Bastani, "Detection of Coherent Radar Signals with Unkown Doppler Shift", IEE Proc., Radar, Sonar and Navigation, vol. 143, no.2, April 1996, pp.79-86.

[3]L.E.Brennan, I.S.Reed, W.Sollfrey, "A comparison of Average – Likelihood Ratio and Maximum-Likelihood Ratio Tests for Detection of Radar Targets of Unknown Doppler Frequency", IEEE Trans. On Inf. Theory, vol. IT-14, no. 1968, pp. 104-110.

[4] M.M. Nayebi, et.al., "Investigations On The Equivalence of ALR and GLR In The Detection of Coherent Radar Signals With Unkown Doppler Shift", ISNIC. 98, Tokyo, pp 79-84.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Approximate Simultaneous Orthogonal Expansions. Applications to Mean-Square Estimation and Signal Detection Problems

Jesús Navarro-Moreno
Dep. of Statistics and O.R.
University of Jaén
23071 Jaén, Spain
e-mail: jnavarro@ujaen.es

Juan Carlos Ruiz-Molina
Dep. of Statistics and O.R.
University of Jaén
23071 Jaén, Spain
e-mail: jcruiz@ujaen.es

Antonia Oya
Dep. of Statistics and O.R.
University of Jaén
23071 Jaén, Spain
e-mail: aoya@ujaen.es

Abstract — **Approximate simultaneous orthogonal expansions of two second-order stochastic processes are defined and their convergence is showed. The technique is based on the Rayleigh-Ritz method to solve the homogeneous equation involving both covariance kernels simultaneously. Finally, two specific applications of these finite expansions are given: in the Gaussian estimation and detection problems.**

I. Introduction

This paper is concerned with the simultaneous diagonalization of two covariance kernels and its application to second-order stochastic processes. Several approaches have been developed to expand two processes simultaneously (e.g., [1]–[3]). These methodologies allow both processes to be expanded in the same set of functions with uncorrelated coefficients. A number of applications of such expansions can be found in the literature. For example, in [1] an extension of Shannon's definition for the information content of a Gaussian process in Gaussian noise is provided, Kadota gives a solution to the problem of estimating a Gaussian signal in noise [4], and Root [2] and Pitcher [5] apply them in the Gaussian detection problem.

From the practical standpoint, simultaneous orthogonal expansions of two stochastic processes are very limited because there is no standard method to find the eigenvalues and eigenfunctions of the operator involved. Kadota gives two examples illustrating an indirect method to obtain the expansion coefficients and the expanding functions [6]. However, this method requires computing the set of eigenfunctions of a covariance kernel, what is generally a difficult task and, sometimes, impossible.

Our aim is to provide a methodology overcoming the difficulty of computing the true simultaneous eigenvalues and eigenfunctions. For this purpose, we will apply the Rayleigh-Ritz method to solve numerically the homogeneous equation involving both covariances simultaneously. The result obtained is an approximate procedure allowing the simultaneous diagonalization of two covariance kernels and, as a consequence, the definition of the so-called approximate simultaneous orthogonal expansions of two stochastic processes.

II. Approximate Simultaneous Orthogonal Expansions

Since the most general solution for expanding two stochastic processes simultaneously is given in [3], we consider this approach as the basis of the present paper. We assume the conditions on the two covariance kernels imposed in the above work and the additional assumption of imperfect detection [2]. Thus, it can be shown that the approximate simultaneous eigenvalues and eigenfunctions, computed by applying the Rayleigh-Ritz method to the associated homogeneous equation, converge to the true ones. This result yields a way of approximating the expanding functions and the expansion coefficients. Moreover, it allows us to obtain an approximate method to diagonalize both covariances simultaneously and also, to define the approximate simultaneous orthogonal expansions of two stochastic processes. The convergence of these finite expansions are also shown. The results remain valid under differentiation. To conclude this section, the implementation of the method is illustrated by considering an example.

III. Applications

The first application considered is concerned with the problem of estimating the mth quadratic-mean derivative of a Gaussian signal in independent Gaussian noise. On the basis of Kadota's results [4], a suboptimal estimate approaching the optimal estimate as the length of the series goes to infinity is proposed and an expression of its error variance is given. Furthermore, it is shown that the sequence of mean-squared estimation errors resulting from the suboptimal estimate converges to the minimum error resulting from the optimal one.

The second application addresses the Gaussian nonsigular detection problem. Specifically, we propose an approximate log-likelihood ratio derived from the above finite expansions, which converges to the optimum detection statistic [2]. The advantage of such approaches is that they are computationally feasible.

References

[1] R.T. Huang and R.A. Johnson, "Information Transmission With Time-Continuous Random Processes," *IEEE, Trans. Information Theory*, vol. 9, pp. 84–94, 1963.

[2] W.L. Root, "Singular Gaussian Measures in Detection Theory," *Proc. Symposium on the Time Series Analysis*, John Wiley, N.Y., pp. 292–315, 1963.

[3] T.T. Kadota, "Simultaneous Diagonalization of Two Covariance Kernels and Application to Second Order Stochastic Processes," *SIAM J. Appl. Math.*, vol. 15, pp. 1470–1480, 1967.

[4] T.T. Kadota, "Optimum Estimation of Nonstationary Gaussian Signals in Noise," *IEEE, Trans. Information Theory*, vol. 15, pp. 253–257, 1969.

[5] T.S. Pitcher, "An Integral Expression for the Log Likelihood Ratio of Two Gaussian Processes," *SIAM J. Appl. Math.*, vol. 14, pp. 228–233, 1966.

[6] T.T. Kadota, "Simultaneously Orthogonal Expansion of Two Stationary Gaussian Processes–Examples," *Bell System Tech. J.*, vol. 45, pp. 1071–1096, 1966.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Maximal number of constant weight vertices of the unit n–cube contained in a k–dimensional subspace

R. Ahlswede, H. Aydinian, and
L. Khachatrian
University Bielefeld

I. Extended Summary

We introduce and solve a seemingly basic geometrical extremal problem.

The set of vertices of weight w in the unit cube of $\mathbb{R}^n$

$$E(n,w) = \{x^n \in \{0,1\}^n : x^n \text{ has } w \text{ ones}\}$$

can also be viewed as the set in which constant weight codes are studied in Information Theory. Another interest there is in linear codes. This was a motivation for studying the interplay between two properties: constant weight and linearity. In particular we wanted to know $M(n,k,w) \triangleq \max\{|U_k^n \cap E(n,w)| : U_k^n$ is a k–dimensional linear subspace of $\mathbb{R}^n\}$, that is, the maximal cardinality of a set of vectors in $E(n,w)$, whose linear span has a dimension not exceeding k. Here is our complete solution.

Theorem. *Let $w \le \frac{n}{2}$ and $k \le n$, then*

(a) $M(n,k,w) = M(n,k,n-w)$

(b) $$M(n,k,w) = \begin{cases} \binom{k}{w}, & \text{if (i) } 2w \le k \\ \binom{2(k-w)}{k-w} 2^{2w-k}, & \text{if (ii) } k < 2w < 2(k-1) \\ 2^{k-1}, & \text{if (iii) } 2(k-1) \le 2w \le n. \end{cases}$$

The key sets giving the lower bounds for $M(n,k,w)$ in the three cases are

(i) $\mathcal{S}_1 = E(k,w) \times \{0\}^{n-k}$

(ii) $\mathcal{S}_2 = E(2(k-w), k-w) \times \{10,01\}^{2w-k} \times \{0\}^{n-2w}$

(iii) $\mathcal{S}_3 = \{10,01\}^{k-1} \times \{1\}^{w-k+1} \times \{0\}^{n-w}$.

We also present an extension to multi–sets and explain a connection to the (simpler) Erdős–Moser problem.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Constant-Weight Code Bounds from Spherical Code Bounds

Erik Agrell
Department of Electrical Engineering
Chalmers Lindholmen University College
P.O. Box 8873, 40272 Göteborg, Sweden
agrell@chl.chalmers.se

Alexander Vardy
Department of Electrical Engineering
University of California at San Diego
La Jolla, CA 92093-0407, U.S.A.
vardy@montblanc.ucsd.edu

Kenneth Zeger
Department of Electrical Engineering
University of California at San Diego
La Jolla, CA 92093-0407, U.S.A.
zeger@ucsd.edu

Abstract — **We present new upper bounds on the size of constant-weight binary codes, derived from bounds for spherical codes. In particular, we improve upon the 1962 Johnson bound and the linear programming bound for constant-weight codes.**

I. Introduction

An (n, d, w) constant-weight code is a binary nonlinear code with length n and minimum Hamming distance d, where all codewords have the same number of ones, w. The maximum size of such a code is denoted $A(n, d, w)$. The value of $A(n, d, w)$ is in general not known, but a number of lower and upper bounds have been established. See [2–4] for summaries of the best bounds known today.

The new bounds presented here are based on concepts from Euclidean geometry, in particular, spherical codes. An (n, s) *spherical code* is a set of points on the n-dimensional unit sphere such that the inner product of any two points is at most s. Its maximum size is denoted by $A_S(n, s)$.

II. Improved Johnson Bound

Through an elementary mapping from binary space to Euclidean space, we obtain the following upper bound. It is equivalent to the well-known Johnson bound from 1962 [2] for $b > \delta/(n+1)$ and improves on it for $0 \le b \le \delta/(n+1)$.

Theorem 1. *Let $b = \delta - w(n-w)/n$. Then*

$$\begin{aligned} A(n, 2\delta, w) &\le \lfloor \delta/b \rfloor, && \text{if } b \ge \delta/n \\ A(n, 2\delta, w) &\le n, && \text{if } 0 < b \le \delta/n \\ A(n, 2\delta, w) &\le 2n-2, && \text{if } b = 0 \end{aligned}$$

Proof: Consider any constant-weight code $\mathscr{C}$ with parameters $(n, 2\delta, w)$ and map it into Euclidean space by replacing the binary components 0 and 1 with, respectively, 1 and -1. After translation and scaling, this yields an $(n-1, s)$ spherical code, where $s = 1 - \delta n/(w(n-w))$. Since its size is upper-bounded by $A_S(n-1, s)$, so is the size of $\mathscr{C}$. Applying known values of $A_S(n-1, s)$ for $s \le 0$ [1] completes the proof. ∎

Some values of $A(n, d, w)$ for which Theorem 1, in conjunction with known lower bounds [3], yields previously unknown exact values are $A(20, 10, 9) = 20$, $A(21, 10, 8) = 21$, $A(24, 10, 7) = 24$, $A(24, 12, 11) = 24$, $A(26, 12, 9) = 26$, and, somewhat surprisingly, $A(28, 14, 12) = A(28, 14, 13) = 28$.

III. Improved Linear Programming Bound

The *distance distribution* of any binary code $\mathscr{C}$ is defined as $A_i = \frac{1}{|\mathscr{C}|} \sum_{c \in \mathscr{C}} |\{c' \in \mathscr{C} \mid d(c, c') = i\}|$ for $i = 0, \ldots, n$, where $d(\cdot, \cdot)$ denotes the Hamming distance. The *linear programming* bound for a constant-weight code with $w \le n/2$ is $A(n, 2\delta, w) \le 1 + \max \sum_{i=\delta}^{w} A_{2i}$, where the maximum is taken over all $\{A_i\}$ that satisfy certain well-known constraints [2].

We propose an additional constraint in the maximization, which sharpens the bound. In the following theorem, $T'(w_1, n_1, w_2, n_2, d)$ and $T(w_1, n_1, w_2, n_2, d)$ denote the maximum size of an $(n_1 + n_2, d, w_1 + w_2)$ constant-weight code in which the number of ones in the first n_1 positions of all codewords is, respectively, at most w_1 and exactly w_1.

Theorem 2. *For all $i, j \in \{\delta, \delta+1, \ldots, w\}$ with $i \ne j$,*

$$\begin{aligned} P_{ji} A_{2i} + (P_i - P_{ij})\, A_{2j} &\le P_i P_{ji}, && \text{if } P_{ij}/P_i + P_{ji}/P_j > 1 \\ (P_j - P_{ji})\, A_{2i} + P_{ij} A_{2j} &\le P_j P_{ij}, && \text{if } P_{ij}/P_i + P_{ji}/P_j > 1 \\ P_j A_{2i} + P_i A_{2j} &\le P_i P_j, && \text{if } P_{ij}/P_i + P_{ji}/P_j \le 1 \end{aligned}$$

where P_i, P_j, P_{ij}, and P_{ji} are any numbers that satisfy

$$\begin{aligned} P_i &\ge T(i, w, i, n-w, 2\delta) \\ P_j &\ge T(j, w, j, n-w, 2\delta) \\ P_{ij} &\ge \min\{P_i, T'(w-\delta, j, \delta-w+i, n-w-j, \\ &\quad 2\delta - 2w + 2i)\}, && \text{if } i + j \le n - \delta \\ P_{ji} &\ge \min\{P_j, T'(w-\delta, i, \delta-w+j, n-w-i, \\ &\quad 2\delta - 2w + 2j)\}, && \text{if } i + j \le n - \delta \\ P_{ji} &= P_{ij} = 0, && \text{if } i + j > n - \delta. \end{aligned}$$

The entities T and T' can be upper-bounded using bounds for spherical codes and so-called *zonal spherical codes*. Details and proofs are given in [1], which also contains several other new bounds, a survey of known bounds on $A(n, d, w)$, and updated tables of $A(n, d, w)$ for $n \le 28$.

New upper bounds obtained through Theorem 2 include $A(20, 8, 9) \le 195$, $A(21, 8, 9) \le 320$, $A(22, 8, 10) \le 641$, $A(24, 8, 11) \le 2188$, and $A(23, 10, 9) \le 81$.

References

[1] E. Agrell, A. Vardy, and K. Zeger, "Upper bounds for constant-weight codes," *IEEE Trans. Inform. Theory*, submitted December 15, 1999, available online at www.chl.chalmers.se/~agrell.

[2] M.R. Best, A.E. Brouwer, F.J. MacWilliams, A.M. Odlyzko, and N.J.A. Sloane, "Bounds for binary codes of length less than 25," *IEEE Trans. Inform. Theory*, vol. 24, pp. 81–93, Jan. 1978.

[3] A.E. Brouwer, J.B. Shearer, N.J.A. Sloane, and W.D. Smith, "A new table of constant weight codes," *IEEE Trans. Inform. Theory*, vol. 36, pp. 1334–1380, Nov. 1990.

[4] R.L. Graham and N.J.A. Sloane, "Lower bounds for constant weight codes," *IEEE Trans. Inform. Theory*, vol. 26, pp. 37–43, Jan. 1980.

[1] This work was supported in part by the National Science Foundation and by the David and Lucile Packard Foundation.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On the Covering Radius of Ternary Negacyclic Codes with Length up to 26

Tsonka S. Baicheva[1]
Institute of Mathematics and
Informatics
Bulgarian Academy of Sciences
P.O.Box 323
5000 Veliko Tarnovo, Bulgaria
e-mail: lpmivt@vt.bia-bg.com

Abstract — **The covering radius of all ternary negacyclic codes of even length up to 26 is given. The minimal distances and weight spectra of all codes were recalculated. Seven of the open cases for the least covering radius of ternary linear codes were solved and for other three cases upper bounds were improved.**

I. Introduction

Constacyclic codes are linear codes which are closed under constacyclic shifts of codewords. A constacyclic shift of the n-tuple $(a_0, a_1, \ldots, a_{n-2}, a_{n-1})$ yields the n-tuple $(ca_{n-1}, a_0, a_1, \ldots, a_{n-2})$, where c is a fixed nonzero field element. Constacyclic codes share many of the well-known algebraic properties of cyclic codes [5, ch. 7]. In particular, one way of describing a constacyclic code C is as an ideal in the ring of polynomials $F[x]/(x^n - c)$, closed under polynomial addition and multiplication modulo $x^n - c$. It can be shown that C is a principal ideal, and as such, it contains a unique monic polynomial of minimum degree, denoted $g(x)$, that generates C, i.e. $C = \langle g(x) \rangle$. The generator polynomial $g(x)$ must be a divisor of $x^n - c$, and the degree r of $g(x)$ determines the redundancy of C, i.e. $\langle g(x) \rangle$ is an $[n, n-r]$ code. We will denote $n - k$ by k.

When $c = -1$ codes are called negacyclic [3, ch. 9]. In this case $g(x)$ is a divisor of $x^n + 1$. The polynomial $h(x) = (x^n + 1)/g(x)$ is the check polynomial of the code C.

As $x^n + 1 = (x^{2n} - 1)/(x^n - 1)$, roots of the polynomial $x^n + 1$ are these roots of $x^{2n} - 1$ which are not roots of the polynomial $x^n - 1$. If α is a primitive root of the polynomial $x^{2n} - 1$, its odd powers are all roots of the polynomial $x^n + 1$, i.e. the roots of the polynomial $x^n + 1$ are odd powers of the primitive $2n$-th root of unity. Therefore we can characterize the code C by its defining set, which is the collection of all j such that α^j is a zero of $g(x)$.

The covering radius $R(C)$ of the code C is defined as the smallest integer R, such that the spheres of radius R around the codewords cover the n-dimensional vector space F_q^n over $GF(q)$.

The function $t_q[n, k]$ is defined as the least value of R when C runs over the class of all linear $[n, k]$ codes over $GF(q)$ for a given q.

II. Ternary Negacyclic Codes with length up to 26

Table II-A from [4] was used as source for all ternary negacyclic codes of lengths up to 26. According to [3] two codes are equivalent, if their defining sets are the same up to multiplication with an integer coprime to their length. So, only nonequivalent codes were considered. Their minimal distances and weight spectra were recalculated. To determine $R(C)$, part of the codes were handled analytically and for the rest of them computer calculations by Method 1 and Method 2 as in [1] were used.

Bounds for the function $t_3[n, k]$ for ternary codes with $n \leq 27$ are given in [2, Table II]. Based on the determined in this work covering radii of ternary negacyclic codes we have obtained some exact values and upper bounds for $t_3[n, k]$.

Proposition

1) $t_3[20, 6] = 7 - 8$.
2) $t_3[20, 10] = t_3[20, 11] = t_3[21, 11] = 4$.
3) $t_3[24, 12] = t_3[25, 13] = 5$.
4) $t_3[21, 10] = t_3[22, 11] = 5$
5) $t_3[22, 10] = 5 - 6$.
6) $t_3[25, 12] = 5 - 6$.

References

[1] T. Baicheva, "The Covering Radius of Ternary Cyclic Codes with Length up to 25," *Designs, Codes and Cryptography*, vol.13, pp. 223-227, 1998.

[2] T. Baicheva and E.Velikova, "Covering Radii of Ternary Linear Codes of Small Dimensions and Codimensions," *IEEE Trans. Inform. Theory*, vol. 43, pp. 2057-2061, 1997.

[3] E. Berlekamp, *Algebraic Coding Theory*, McGraw-hill Book Company, 1968.

[4] F. R. Kschischang and S. Pasupathy, "Some ternary and quaternary codes and associated sphere packings," *IEEE Trans. Inf. Theory*, vol. 38, No 2, pp. 227-246, 1992.

[5] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, Amsterdam: North-Holland, 1977.

[1]This work was supported by a DFG Contract.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Multicovering Bounds from Relative Covering Radii

Iiro Honkala
Department of Mathematics
University of Turku
20014 Turku, Finland
honkala@utu.fi

Andrew Klapper[1]
Dept. of Computer Science
University of Kentucky
Lexington, KY, 40506-0046 USA
klapper@cs.uky.edu

I. Introduction and Definitions

The concept of multicovering radius was introduced by Klapper [2] in the context of studying the security of stream ciphers. Let C be a code of length n and m be a positive integer. The *m-covering radius of C* is the smallest integer r such that every set of m vectors in $\mathbf{F}^n$ is contained in at least one ball of radius r around a codeword in C.

We denote the m-covering radius of a code C by $R_m(C)$. Then $R(C) := R_1(C)$ is the covering radius of C. For results on the covering radius, see to the book by Cohen, et. al. [1].

In general we are interested in various extremal values associated with this notion: $R_m(\mathbf{F}^n)$:= the smallest m-covering radius among length n codes, $t_m(n,K)$:= the smallest m-covering radius among (n,K) codes.

The purpose of this paper is to derive new bounds by relating the multi-covering radii of a code to a relativized notion of covering radius. For generality, we define this notion for multi-covering radii, although we shall only use the ordinary covering radius version.

Definition 1 *Let C and S be codes of length n, and let m be a positive integer. Then the* k-covering radius of C relative to S, *$R_k(S,C)$, is the smallest integer r such that for every $c^1,\cdots,c^k \in C$ there is an $s \in S$ such that $d(c^i,s) \le r$ for all $i = 1,\cdots,k$. Also, $t_k(m,C) := \min\{R_k(S,C) : |S| = m\}$.*

Note that $t_k(m,\mathbf{F}^n) = t_k(n,m)$.

II. A Fundamental Identity

Let $\bar{S}$ denote the set of word-complements of elements of a code S.

Theorem 2 *If C is a code of length n then*

$$R_m(C) = n - t_1(m,C).$$

For $C = \mathbf{F}^n$ we obtain the following corollary, which is essentially a restatement of Theorem 19.4.4 of Cohen, et. al. [1] (cf. also Theorem 19.4.2).

Corollary 3 *For all natural numbers $n,m \ge 1$, $R_m(\mathbf{F}^n) = n - t_1(n,m)$.*

III. The 3-covering radius of Hamming codes

Let $\mathcal{H}_r$ denote the Hamming code of order r. It was shown by Klapper [2] that for any $m \ge 2$ and $r \ge 2$, $2^{r-1} \le R_m(\mathcal{H}_r) \le 2^{r-1} + c_m$, where c_m is a constant depending only on m. It was also shown that $R_m(\mathcal{H}_2) = 3$ for $m \ge 2$; for $r \ge 3$ we have $R_2(\mathcal{H}_r) = 2^{r-1}$; and for $m = 3,4,5$ we have $2^{r-1} \le R_m(\mathcal{H}_r) \le 2^{r-1}+1$. However, in this last case the precise value was unknown. In this section, using Theorem 2, we determine exactly the 3-covering radius of the Hamming codes.

[1]Project sponsored by the National Science Foundation under grant number NCR-9706078.

Theorem 4 *We have $t_1(3,\mathcal{H}_r) = \frac{1}{2}(n-1) = 2^{r-1} - 1$ and $R_3(\mathcal{H}_r) = \frac{1}{2}(n+1) = 2^{r-1}$.*

IV. Corollaries

It is known from Klapper [2] that for all $n \ge 3$ $R_2(\mathbf{F}^n) = R_3(\mathbf{F}^n) = \lceil n/2 \rceil$ and $R_4(\mathbf{F}^n) = R_5(\mathbf{F}^n) = \lceil (n+1)/2 \rceil$. Using Corollary 2.2 and known results about $K(n,R)$, the minimum cardinality of a binary code of length n and covering radius R, we can determine $R_6(\mathbf{F}^n)$ and $R_7(\mathbf{F}^n)$.

Theorem 5 *For all $n \ge 4$ we have $R_6(\mathbf{F}^n) = \lceil (n+1)/2 \rceil$ and $R_7(\mathbf{F}^n) = \lceil (n+2)/2 \rceil$.*

Since $t_1(n,2^k)$ is bounded above by the covering radius of any binary linear code of length n and dimension k, we also obtain many bounds on multicovering radius by using known bounds on binary linear codes. The resulting tables of bounds are omitted from this abstract.

Using Corollary 2.2 and the results in Section 12.5 of Cohen, et. al. [1] we obtain asymptotic results on $R_m(\mathbf{F}^n)$. For instance, using Theorems 12.5.1 (sphere-covering bound) and 12.5.10. (from Lovász, Spencer and Vesztergombi [3]) we obtain the following theorem.

Theorem 6 *For all n and m, $R_m(\mathbf{F}^n) \le n/2 + \sqrt{n \log_2 m \ln 2/2}$. For all n and m, $R_m(\mathbf{F}^n) \le n/2 + 12\sqrt{m}$.*

We obtain bounds on $t_1(m,C)$ by counting vectors in balls. If $|S| = m$, $R_1(S,C) = t_1(m,C)$, and k is the maximum number of vectors of C in any ball of radius $t_1(m,C)$, then $km \ge |C|$. Thus $t_1(m,C)$ must be large enough that $k \ge |C|/m$. When $m < |C|$, we must have $k \ge 2$. If d_0 is the largest minimum distance among the $(m+1)$-element subcodes of C, then any ball of radius at most $(d_0-1)/2$ contains at most one element of C. Thus if $t_1(m,C) \le (d_0-1)/2$, then $k = 1$, which is false. Therefore $t_1(m,C) > (d_0-1)/2$. That is, $t_1(m,C) \ge d_0/2$. Hence $R_m(C) \le n - d_0/2$. In particular,

Theorem 7 *If the minimum distance of C is d, then $R_m(C) \le n - d/2$.*

References

[1] G. Cohen, I. Honkala, S. Litsyn and A. Lobstein, Covering Codes. Elsevier, Amsterdam, 1997.

[2] A. Klapper, "The Multicovering radii of codes," *IEEE Trans. Info. Theory* vol. 43, pp. 1372–1377, 1997.

[3] L. Lovász, J. H. Spencer and K. Vesztergombi, "Discrepancy of set-systems and matrices," *European J. Combinatorics*, vol. 7, pp. 151–160, 1986.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

A Simple Decoding Algorithm for the [24,12,8] extended Golay Code

I. Boyarinov
Institute for System Analysis
of Russian Academy of Sciences
60 years of October av., 9
Moscow 117312, Russia
e-mail: i.boyarinov@mtu-net.ru

I. Martin
Communications Research Centre
Lancaster University
Lancaster LA1 4YR
United Kingdom
e-mail: i.martin@lancs.ac.uk

B. Honary
Communications Research Centre
Lancaster University
Lancaster LA1 4YR
United Kingdom
e-mail:
b.honary@lancaster.ac.uk

Abstract — **A simple decoding algorithm for the [24,12,8] extended Golay code, based on the $| a+x | b+x | a+b+x |$ Turyn construction is described.**

I. Introduction

In this paper we propose a simple high-speed decoding algorithm for the [24,12,8] extended Golay code, based on the $| a+x | b+x | a+b+x |$ Turyn construction [1]. The algorithm can be easily realized in combinational circuits. Futhermore we show that [24,12,8] Golay code can correct simultaneously all patterns of three or fewer random errors as well as certain patterns of quadruple errors such as 4-bit cyclic single-burst and two-dimensional byte errors.

II. The Decoding Algorithm for Random Errors

Let C_1 be the binary cyclic [7,4,3] Hamming code with the generator polynomial $g_1(x) = x^3 + x + 1$ over $GF(2)$ and let C_2 be formed by reversing the code words of C_1. Let V_1 and V_2 be the [8,4,4] codes obtained by adding an overall parity check to C_1 and C_2. The code C, consisting of all vectors $c = | a+x | b+x | a+b+x |$, where $a, b \in V_1$ and $x \in V_2$, is the [24,12,8] extended Golay code G_{24} (Turyn [1],pp. 587-588).

Let $z = c + e$ be a received word, c be a code word of the Golay code and e be an error word. Represent the words z and e as $z = | z_0 | z_1 | z_2 |$ and $e = | e_0 | e_1 | e_2 |$, where $z_0 = a + x + e_0$, $z_1 = b + x + e_1$, $z_2 = a + b + x + e_2$. Under decoding we define $u_{01} = z_0 + z_1 = a + b + e_0 + e_1$, $u_{02} = z_0 + z_2 = b + e_0 + e_2$, $u_{12} = z_1 + z_2 = a + e_1 + e_2$, $u_{012} = z_0 + z_1 + z_2 = x + e_0 + e_1 + e_2$. Calculate the syndromes of these words and overall parity checks λ_i of the words $z_i, i = 0, 1, 2$. For an error word e of the weight $wt(e) < 8$ the syndromes $S(u_{02}) = S(u_{12}) = S(u_{012}) = 0$ if and only if $e = 0$. $S(z) = (S(u_{02}), S(u_{12}), S(u_{012}))$ is called the syndrome of z. Let $z^{(1)} = c^{(1)} + e^{(1)}$ and $z^{(2)} = c^{(2)} + e^{(2)}$ where $c^{(1)}$ and $c^{(2)}$ are words of the Golay code C and $e^{(1)}$, $e^{(2)}$ are error words. If $e^{(1)} \neq e^{(2)}$ and $wt(e^{(1)}) \leq 3$, $wt(e^{(2)}) \leq 4$, then $S(z^{(1)}) \neq S(z^{(2)})$. Use the syndrome $S(z)$ and overall parity checks λ_i in order to find the syndrome $S_\cap(z_\cap)$ of the word $z_\cap$ of the intersection code $V_1 \cap V_2$ that is the extended BCH code of the minimum distance 8. Then using the decoding algorithm for this code we define locators α_j, $\alpha_j \in GF(2^3)$, $j = 0, 1, 2, \ldots, 7$ of errors in the words z_0, z_1 and z_2.

The described algorithm for random errors is suitable for implementation in combinational curcuits. We estimate the number of gates of the decoder and the decoding delay. We show that the combinational decoder of the [24,12,8] extended Golay code needs no more than 295 XOR, 234 AND, 101 OR and 63 NOT gates and no more than 24 gate delays for calculating the output word.

III. Correction of single-burst and two-dimensional byte errors

We will represent the Golay code as a generalized array code [2]. Then the code word $c = | a + x | b + x | a + b + x |$ of the Golay code C is represented as following array

$$c = \begin{matrix} c_{00} & c_{01} & c_{02} & c_{03} & c_{04} & c_{05} & c_{06} & c_{07} \\ c_{10} & c_{11} & c_{12} & c_{13} & c_{14} & c_{15} & c_{16} & c_{17} \\ c_{20} & c_{21} & c_{22} & c_{23} & c_{24} & c_{25} & c_{26} & c_{27}. \end{matrix}$$

The error word array e is called a 4-bit cyclic single-burst error if for some i, j (where i and j are the row and column indexes of the array, respectively) the symbols $e_{i,j}, e_{i+1,j+1}, e_{i+2,j+2}, e_{i+3,j+3}$ may be equal to 1 and all other symbols of the error word e are equal to 0. The indexes i and j are taken mod 3 and mod 8 respectively. If $e_{i,j} = e_{i+1,j+1} = e_{i+2,j+2} = e_{i+3,j+3} = 1$, the error word e is called a 4-bit cyclic solid single-burst error. As the Golay code corrects all patterns of three or fewer errors we consider only 4-bit cyclic solid single-burst errors. We show that all 4-bit cyclic solid single-burst errors have different syndromes, that differ also from the syndromes of all error words of weight ≤ 3.

The error word e is called a 4-bit two-dimensional single-byte error if for some $i = 0, 1, 2$ and $j = 0, 2, 4, 6$ the symbols $e_{i,j}, e_{i,j+1}, e_{i+1,j}, e_{i+1,j+1}$ may be equal to 1 and all other symbols of the error word e are equal to 0. The index i is taken by mod 3. If $e_{i,j} = e_{i,j+1} = e_{i+1,j} = e_{i+1,j+1} = 1$, the error word e is called a 4-bit two-dimensional solid single-byte error. We show that all 4-bit two-dimensional solid single-byte errors have different syndromes, that also differ from the syndromes of all words of weight ≤ 3 and 4-bit cyclic solid single-burst errors.

Acknowledgments

The authors would like to thank The Royal Society, UK, in their support of Dr. I. Boyarinov during his stay with the Communications Research Centre at Lancaster University.

References

[1] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam: North-Holland, 1977.

[2] B. Honary and G. Markarian, *Trellis Decoding of Block Codes. A Practical Approach*. Boston/Dordrecht/ London: Kluwer Academic Publishers, 1997.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Limited-Trial Generalized Minimum Distance Decoding with Fixed Erasing

Jos H. Weber
Delft University of Technology
P.O. Box 5031, 2600 GA Delft
The Netherlands
J.H.Weber@ITS.TUDelft.NL

Khaled A.S. Abdel-Ghaffar[1]
University of California
Davis, CA 95616
USA
ghaffar@ece.ucdavis.edu

Abstract — **A framework is presented for generalized minimum distance (GMD) decoding with a limited number of decoding trials and fixed erasing. The realizable distance for this technique is studied.**

Generalized Minimum Distance (GMD) decoding, as introduced by Forney [1], permits flexible use of reliability information in algebraic decoding algorithms for error correction. In subsequent trials, an increasing number of the most unreliable symbols in the received sequence is erased, and the resulting sequence is fed into an algebraic error-erasure decoder, until the decoding result and the received sequence satisfy a certain distance criterion. In Forney's original algorithm, the unique codeword (if one exists) satisfying the distance criterion is found in at most $\lceil d/2 \rceil$ trials, where d is the Hamming distance of the code.

Kovalev [2] considered GMD decoding algorithms in which the maximum number of trials is limited to a certain number $l \geq 1$. This restriction may decrease the error correction capabilities compared to Forney's algorithm. Still, it is worthwhile investigating limited-trial GMD decoding, since its reduction of the delay (in case of a *serial* implementation) or the number of required error-erasure decoders (in case of a *parallel* implementation) may more than compensate for the (slightly) worse performance.

We assume the following situation. A codeword $\mathbf{c} = (c_1, \ldots, c_n)$ from a q-ary code $\mathcal{C}$ of length n and Hamming distance d is transmitted over a q-ary channel. The output of the channel consists of the received q-ary vector $\mathbf{r} = (r_1, \ldots, r_n)$ and an associated reliability vector $\alpha = (\alpha_1, \ldots, \alpha_n)$, where all α_i are from a set $\mathcal{R}$ which is a subset of the real interval $[0, 1]$ containing $\{1\}$, i.e., $\{1\} \subseteq \mathcal{R} \subseteq [0, 1]$. The higher α_i, the more reliable is the symbol r_i. The *generalized distance* between the received word $\mathbf{r}$ with reliability vector α and a q-ary vector $\mathbf{z} = (z_1, \ldots, z_n)$ is defined as

$$d_{\mathrm{G}}(\mathbf{z}, \mathbf{r}, \alpha) = \sum_{i: z_i = r_i} (1 - \alpha_i)/2 + \sum_{i: z_i \neq r_i} (1 + \alpha_i)/2. \quad (1)$$

In the GMD decoder, some of the most unreliable received symbols, i.e., r_i with lowest α_i, are erased. In this work, where we consider fixed erasing, the erasing procedure is based on a fixed set $\mathcal{I} = \{i_1, \ldots, i_l\}$, which is independent of the received reliability vector α. In trial j, the i_j most unreliable received symbols are erased, after which the resulting vector $\mathbf{r}_j$ is fed into an error-erasure decoding algorithm for the code $\mathcal{C}$ with the property that it returns the original codeword whenever the numbers of erasures s and of errors t are such that $2t + s < d$. This leads to (at most) l codewords $\hat{\mathbf{c}}_j$, among which one with smallest $d_{\mathrm{G}}(\hat{\mathbf{c}}_j, \mathbf{r}, \alpha)$, is chosen as the final decoding result $\hat{\mathbf{c}}$.

For a code of Hamming distance d and length n, a reliability vector α of length n, and an erasing set $\mathcal{I}$, let $d_{\mathrm{r}}(d, \alpha, \mathcal{I})$ be defined as the largest real number d_{r} for which the following assertion holds: for any transmitted codeword $\mathbf{c}$ and any received vector $\mathbf{r}$ of length n with reliability vector α such that $d_{\mathrm{G}}(\mathbf{c}, \mathbf{r}, \alpha) < d_{\mathrm{r}}/2$, the original codeword $\mathbf{c}$ is delivered by the GMD decoder based on erasing set $\mathcal{I}$. For a code of Hamming distance d and length n, a reliability set $\mathcal{R}$, and a fixed erasing set $\mathcal{I}$, let the *realizable distance* of the associated GMD decoder be defined as the infimum of $d_{\mathrm{r}}(d, \alpha, \mathcal{I})$ over all $\alpha \in \mathcal{R}^n$.

The realizable distance is an important figure of merit for a limited-trial GMD decoder. For any $\mathcal{R}$, Forney [1] has shown that by erasing $2j - 1 - d + 2\lfloor d/2 \rfloor$ most unreliable symbols in the j^{th} trial ($j = 1, \ldots, \lceil d/2 \rceil$), the realizable distance is (at least) d, i.e., the full Hamming distance d is exploited. For $\mathcal{R} = [0, 1]$ and fixed erasing, Kovalev [2] calculated the loss of distance compared to Forney's algorithm in case the maximum number of decoding trials is restricted ($l < \lceil d/2 \rceil$). Here, we extend Kovalev's result to the case that $\mathcal{R}$ is any subset of $[0, 1]$.

For a code $\mathcal{C}$ of Hamming distance d and length n, a reliability set $\mathcal{R}$ with infimum μ, and a fixed erasing set $\mathcal{I}$ satisfying $-i_1 = i_0 \leq 0 \leq i_1 < \cdots < i_l < i_{l+1} = d + 1$ and $d - i_j \equiv 1 (2)$ for all j, the realizable distance can be shown to equal

$$d + 1 - \mu i_1 + \frac{(\mu - 1)}{2} \max_{k=0,\ldots,l} (i_{k+1} - i_k). \quad (2)$$

Note that the realizable distance depends on the code $\mathcal{C}$ only by its Hamming distance d and on the reliability set $\mathcal{R}$ only by its infimum μ. For given $\mathcal{C}$, $\mathcal{R}$, and $l \geq 1$, the maximum realizable distance among all erasing sets $\mathcal{I}$ of size l can be shown to equal

$$\begin{cases} g(l\lceil \frac{d+1}{2l+1} \rceil) & \text{if } 0 \leq \mu \leq \frac{1}{2l+1} \\ & \text{and } \lceil \frac{d+1}{2l+1} \rceil \leq \lfloor \lceil \frac{d}{2} \rceil / l \rfloor, \\ g(l\lfloor \lceil \frac{d}{2} \rceil / l \rfloor) & \text{if } \frac{1}{2l+1} < \mu < \frac{1}{2\lceil \frac{d}{2} \rceil - 2l\lfloor \lceil \frac{d}{2} \rceil / l \rfloor + 1} \\ & \text{and } \lceil \frac{d+1}{2l+1} \rceil \leq \lfloor \lceil \frac{d}{2} \rceil / l \rfloor, \\ g(\lceil \frac{d}{2} \rceil) & \text{otherwise,} \end{cases} \quad (3)$$

where $g(x) = 2\mu x + (1 - \mu)(d + 1 - \lceil x/l \rceil)$.

References

[1] G.D. Forney, Jr., "Generalized minimum distance decoding," *IEEE Trans. Inform. Theory*, vol. 12, pp. 125-131, April 1966.

[2] S.I. Kovalev, "Two classes of minimum generalized distance decoding algorithms," *Problemy Peredachi Inform.*, vol. 22, no. 3, pp. 35-42, 1986.

[1]This author was supported by NSF Grant CCR-96-12354.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

An Improvement to GMD-like Decoding Algorithms

Hitoshi Tokushige
Nara Institute of Science and Technology
E-mail: hitosh-t@is.aist-nara.ac.jp

Takuya Koumoto
NTT DoCoMo
E-mail: koumoto@nw.yrp.nttdocomo.co.jp

Tadao Kasami
Hiroshima City University
E-mail: kasami@cs.hiroshima-cu.ac.jp

Abstract — **For binary linear block codes, we introduce "multiple GMD decoding algorithm", where GMD-like decoding is iterated around a few appropriately selected search centers. Compared with the original GMD decoding by Forney [1], this decoding algorithm provides better error performance with increasing the number of iterations of erasure and error correction moderately. To reduce the number of iterations, we derive new effective sufficient conditions on the optimality of decoded codewords.**

1. Definitions: Suppose a binary linear (N, K) block code C with minimum weight $d_{\min}$ is used over the AWGN channel using BPSK signaling. Each codeword is transmitted with the same probability. For a positive integer n, let V^n denote the set of all binary n-tuples. For a received sequence $\boldsymbol{r} = (r_1, r_2, \ldots, r_N)$, the hard-decision sequence $\boldsymbol{z} = (z_1, z_2, \ldots, z_N)$ of $\boldsymbol{r}$ and an N-tuple $\boldsymbol{u} \in V^N$, define $L(\boldsymbol{u}) \triangleq \sum_{i \in D_{-1}(\boldsymbol{u})} |r_i|$,where $D_{-1}(\boldsymbol{u}) \triangleq \{i : u_i \neq z_i$, and $1 \leq i \leq N\}$. For nonempty $U \subseteq V^N$, let $\underline{L}[U]$ be defined as $\min_{\boldsymbol{u} \in U} L(\boldsymbol{u})$. Let $\boldsymbol{v}[U]$, called the best in U, denote an N-tuple in U such that $L(\boldsymbol{v}[U]) = \underline{L}[U]$. For integers $1 \leq i \leq j \leq N$, $\boldsymbol{u}$ and $\boldsymbol{v} \in V^N$, let $d_{H,i,j}(\boldsymbol{u}, \boldsymbol{v})$ denote the Hamming distance between $\boldsymbol{u}$ and $\boldsymbol{v}$ from the i-th bit to the j-th bit.

2. Multiple GMD decoding: For $\boldsymbol{v} \in V^N$, a GMD-like decoding with search center $\boldsymbol{v}$, denoted GMD($\boldsymbol{v}$), is defined as the iterative decoding algorithm consisting of $\rho \triangleq \lfloor (d_{\min} + 1)/2 \rfloor$ stages whose j-th stage is an algebraic decoding which corrects $2j - p - 1$ erasures in the least reliable $2j - p - 1$ components and $\rho - j$ or less errors in the remaining components of input $\boldsymbol{v}$ for $1 \leq j \leq \rho$. The region which has not been searched (for candidate codewords) yet up to the j-th stage of GMD($\boldsymbol{v}$), denoted $\bar{R}_p(\boldsymbol{v}, j)$, is given by $\bar{R}_p(\boldsymbol{v}, j) = \{\boldsymbol{x} \in V^N : d_{H,2j'-p,N}(\boldsymbol{x}, \boldsymbol{v}) > \rho - j'$ for $1 \leq j' \leq j\}$. Define $\bar{R}_{\mathrm{GMD}(\boldsymbol{v})} \triangleq \bar{R}_p(\boldsymbol{v}, \rho)$.

For a positive integer h, h-GMD decoding is defined as an iterative decoding algorithm which consists of successive GMD($\boldsymbol{v}^{(1)}$), GMD($\boldsymbol{v}^{(2)}$), ..., GMD($\boldsymbol{v}^{(h)}$). Here, $\boldsymbol{v}^{(i)} \in V^N$ is called the i-th search center of the h-GMD decoding, and $\boldsymbol{v}^{(1)} = \boldsymbol{z}$ and other $\boldsymbol{v}^{(i)}$ is chosen as the best N-tuple in the region which has not been searched by $(i-1)$-GMD decoding, that is, $\boldsymbol{v}^{(i)} = \boldsymbol{v}\left[\bigcap_{i'=1}^{i-1} \bar{R}_{\mathrm{GMD}(\boldsymbol{v}^{(i')})}\right]$. For $1 \leq i \leq h$ and $1 \leq j \leq \rho$, the j-th stage of the i-th GMD($\boldsymbol{v}^{(i)}$) decoding is called the (i, j)-th stage. Let $\boldsymbol{c}^{(i)}_{\mathrm{best}}(j)$ be the best candidate codeword generated up to the (i, j)-th stage, if it exists. After the (h, ρ)-th stage, $\boldsymbol{c}^{(h)}_{\mathrm{best}}(\rho)$ is output as the decoded codeword, unless the decoding fails.

3. New Early Termination Conditions: Just after the (i, j)-th stage, $\bar{R}(i, j) \triangleq (\bigcap_{i'=1}^{i-1} \bar{R}_{\mathrm{GMD}(\boldsymbol{v}^{(i')})}) \cap \bar{R}_p(\boldsymbol{v}^{(i)}, j)$ is the region which has not yet been searched for candidate codewords. For $\boldsymbol{v} \in V^N$, $\bar{O}_{d_{\min}}(\boldsymbol{v}) \triangleq \{\boldsymbol{x} \in V^N : d_{H,1,N}(\boldsymbol{x}, \boldsymbol{v}) \geq d_{\min}\}$. The following condition is a sufficient condition on the optimality of $\boldsymbol{c}^{(i)}_{\mathrm{best}}(j)$:

$$\mathrm{Cond}^{(i)}_S(j) : L(\boldsymbol{c}^{(i)}_{\mathrm{best}}(j)) \leq \underline{L}\left[\bar{R}(i, j) \cap \bar{O}_{d_{\min}}(\boldsymbol{c}^{(i)}_{\mathrm{best}}(j))\right].$$

$\mathrm{Cond}^{(i)}_S(j)$ is stronger than $\mathrm{Cond}_{\mathrm{TP}}$ introduced by Taipale-Pursley [2], because $\bar{R}(i, j)$ is taken into account.

4. Simulation Results: Figure 1 shows simulation results of block error probabilities of the extended (128, 85) BCH code, denoted EBCH(128, 85). For comparison, the block error probabilities for bounded distance-t_0($\triangleq \lfloor (d_{\min} - 1)/2 \rfloor$) decoding and Chase decoding algorithm II [3] are shown.

The reduction rate of 3-GMD decoding is defined as the ratio of the number of iterations of erasure and error correction stage to the maximum 3ρ. Since sufficient conditions can be used only when at least one candidate codeword has been generated, rates μ_{TP} and μ_{NEW} denote the averages of reduction rates by using $\mathrm{Cond}_{\mathrm{TP}}$ and $\mathrm{Cond}^{(i)}_S(j)$, respectively, as early termination conditions over all the trials where at least one candidate codeword is generated. Table 1 lists μ_{TP} and μ_{NEW} in percentage for EBCH(64, 24) and EBCH(128, 85) at $E_b/N_0 = 2.0$dB and 4.0dB.

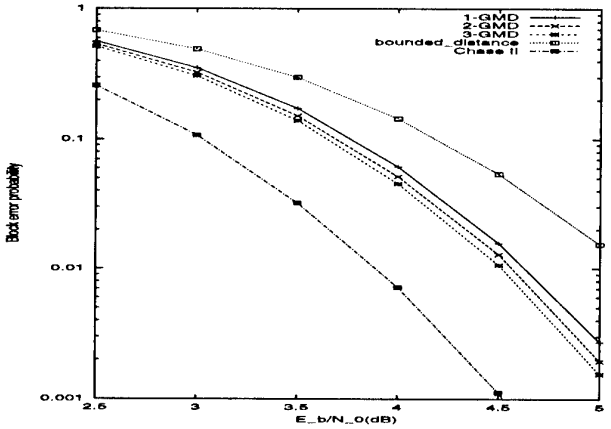


Figure 1: Block error probability of EBCH(128, 85)

Table 1: The average of reduction rate of 3-GMD decoding

Code	$E_b/N_0 = 2.0$dB		$E_b/N_0 = 4.0$dB	
	μ_{TP}	μ_{NEW}	μ_{TP}	μ_{NEW}
EBCH(64, 24)	66.7%	61.6%	23.6%	19.8%
EBCH(128, 85)	78.4%	74.3%	21.1%	18.1%

Acknowledgments: The authors are heartily grateful to Dr. Y. Tang for collaboration on deriving an efficient evaluation of $\mathrm{Cond}^{(i)}_S(j)$.

References

[1] G. D. Forney, Jr., "Generalized Minimum Distance Decoding," *IEEE Trans. Inform. Theory*, vol. IT-2, pp. 125–181, Apr. 1966.

[2] D. Taipale and M. B. Pursley, "An Improvement to Generalized Minimum-Distance Decoding," *IEEE Trans. Inform. Theory*, vol. 37, pp. 167–172, Jan. 1991.

[3] D. Chase, "A class of algorithms for decoding block codes with channel measurement information," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 170–182, Jan. 1972.

[4] H. Tokushige, Y. Tang, T. Koumoto and T. Kasami "An Improvement to GMD-like Decoding Algorithms," *IEICE Trans. Fundamentals*, Oct. 2000. (to appear)

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Totally Self–Checking Decoders for Hamming SEC Codes

I.M. Boyarinov
Institute for System Analysis
of Russian Academy of Sciences
60 years of October av., 9
Moscow 117312, Russia
e-mail: i.boyarinov@mtu-net.ru

Abstract — **It is shown that there exist totally self-checking (TSC) combinational decoders for (n,k) Hamming SEC codes if and only if $n = 2^r - 1, r = n - k$. For shortened (n,k) Hamming SEC codes the modified combinational totally self-checking decoders with minimum testing delay $2 \leq \mu < (n-k)$ are suggested.**

I. Introduction

The most natural architecture for on-chip error-correcting is to place a single-error-correcting code along each row of the memory [1]. To maintain the high level of reliability, faults of the decoder as well as faults of the memory chips must be detected. The effective means of of the achievment of these purposes are self-checking circuits. In this paper the problem of constructing totally self-checking decoders for Hamming SEC codes is considered. It is shown that there exist totally self-checking combinational decoders for (n,k) Hamming SEC codes if and only if $n = 2^r - 1, r = n - k$. For shortened (n,k) Hamming SEC codes the modified combinational totally self-checking decoders with minimum testing delay $2 \leq \mu < (n-k)$ are suggested.

II. Totally Self-Checking Circuits

We consider a combinational circuit that produces an output vector $y(x,f)$, which is a function of the intput vector x from the intput set X and a fault $f \in F$. The standard single stuck-at fault model is assumed ([2, pp. 249-248]). A circuit C is fault-secure for an input set X and a fault set F if for any input x in X and for any fault f in F, $y(x,f) \notin Y$ or $y(x,f) = y(x,\lambda)$ where λ is the null fault. A circuit C is self-testing for an input set X and a fault set F if for every fault f in F there is some input x in X such that $y(x,f) \notin Y$. An input x for which $y(x,f) \notin Y$ is called a testing pattern for f. A circuit C is totally self-checking (TSC) if it is both self-testing and fault-secure ([3, pp. 392-394]). Self-testing is a rather difficult condition to satisfy perfectly. With this difficulty in mind, the concepts of strongly fault secure logic networks [4] and totally self-checking circuits with minimum testing delay [5] were proposed. A TSC circuit is TSC with minimum testing delay $\mu = 1$.

III. Modified Self-Checking Decoders for Hamming SEC codes

The decoder of the Hamming SEC code comprises the syndrome generator (SG), the syndrome decoder (SD) and the corrector (COR). It is supposed that the decoder is a combinational circuit. SG and COR are composed entirely of XOR gates. SD is constructed by AND gates and NOT gates.

Let $X = \{x : x = v + e, v \in V, wt(e) \leq 1\}$ be an input set and $Y = \{y : y = y(x,\lambda) = v, x \in X, v \in V\}$ be an output set of a combinational decoder of a systematic (n,k) Hamming SEC code V in the absence of faults. We show that the decoder of V is totally self-checking if and only if $n = 2^r - 1, r = n - k$.

Most of the codes for semiconductor memory applications are shortened codes. For $n < 2^r - 1$ we construct totally self-checking decoders with minimum testing delay $2 \leq \mu < (n-k)$. We show that for any shortened (n,k) Hamming SEC code there exists a parity-check matrix such that a decoder of this code is TSC with minimum testing delay $\mu = 2$.

Totally self-checking code checker can be constructed for the combinational totally self-checking decoder with testing delay μ of a systematic Hamming SEC code. This checker consists of the regenerator of syndrome pairs and multi-input two-rail code checker. The description of the syndrome regenerator and multi-input two-rail code checker can be found in [3, pp. 443-444, 459-466]. We show that the decoder can be modified such that the complexity of the checker is becoming significantly less.

References

[1] R.M. Goodman and M. Sayano,"The realibility of semiconductor RAM memories with on-chip error-correcting coding", *IEEE Transactions on Information Theory,* vol. IT-37, 884-896,no.3, part II, 1991.

[2] E.J. McCluskey, *Logic design principles.* Englewood Cliffs,NJ: Prentice-Hall, Inc., 1986.

[3] T.R.N. Rao and E. Fujiwara, *Error-control coding for computer systems.* Englewood Cliffs, NJ: Prentice-Hall, Inc., 1989.

[4] J.E. Smith and G.Metze,"Strongly fault secure logic networks", *IEEE Transactions on Computers,* vol. C-27 (6), pp. 491-499, June 1978.

[5] I.M. Boyarinov,"Totally self-checking decoders with test delay for shortened Hamming SEC codes", *Proceedings of Seventh Joint Swedish-Russian International Workshop on Information Theory", St.-Petersburg, Russia,* pp. 49-52, 1995.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On Decoding Bit Error Probability for Binary Convolutional Codes

Rolf Johannesson
Dept of Inform Techn
Information Theory Group
Lund University
P.O. Box 118
SE-221 00 LUND, Sweden
email: rolf@it.lth.se

James L. Massey
Dept of Inform Techn
Information Theory Group
Lund University
P.O. Box 118
SE-221 00 LUND, Sweden
JamesMassey@compuserve.com

Per Ståhl[1]
Dept of Inform Techn
Information Theory Group
Lund University
P.O. Box 118
SE-221 00 LUND, Sweden
email: per.stahl@it.lth.se

Abstract — **An explanation is given for the paradoxical fact that, at low signal-to-noise ratios, the systematic feedback encoder results in fewer decoding bit errors than does a nonsystematic feedforward encoder for the same code. The analysis identifies a new code property, the *d-distance weight density* of the code. For a given d-distance weight density, the decoding bit error probability depends on the number of taps in the realization of the encoder inverse. Among all encoders for a given convolutional code, the systematic one has the simplest encoder inverse and, hence, gives the smallest bit error probability.**

I. Introduction

It is well-known that the free distance of a convolutional code is the principle determiner of the burst error probability (first-event error probability) for large signal-to-noise ratios when maximum-likelihood decoding is used [1]. Since the free distance is a code parameter, the burst error probability is the same whether the convolutional code was encoded by a nonsystematic feedforward encoder or by a systematic feedback encoder. The decoding bit error probability, however, depends on the encoder used. Typically at high signal-to-noise ratios where most of the decoding burst errors are made to codewords at the free distance from the transmitted codeword, the systematic feedback encoder results in more bit errors than a nonsystematic encoder. We now explain the paradoxical fact, often observed in practice, that, at low signal-to-noise ratios, the systematic feedback encoder results in fewer bit errors than does a nonsystematic feedforward encoder.

II. d-distance weight density

Our analysis is based on consideration of what we call the *d-distance weight density* of the code, p_d, and define as the fraction of 1's in the "detours" of weight d in the binary convolutional code. We use this parameter in a model of the internal codeword structure, together with the structure of the encoder inverse, to estimate the number of information bit errors that result from each 1 in a burst error that forms a codeword of weight d. The weights of codewords are code parameters, not encoder parameters, and hence these estimates reveal which convolutional encoders give the best bit error probability performance. At low signal-to-noise ratios, i.e., at code rates close to channel capacity, error bursts are typically very long so that the codewords with weights substantially larger than the free distance of the code primarily determine the decoding bit-error probability.

[1]This research was supported by the Foundation for Strategic Research - Personal Computing and Communication under Grant PCC-9706-09.

Consider all codewords of weight d in a rate $R = b/c$ fixed binary convolutional code. For small d, the number of codewords of weight d, n_d, is also small and the value of p_d fluctuates widely. For larger d, however, the number of codewords of weight d increases rapidly and the value of p_d stabilizes. One finds that p_d tends towards an asymptotic value as d increases. This asymptote is slightly memory dependent. For small memory, m, the asymptotic value is larger than for large m. As m grows, however, p_d quickly decreases to its asymptotic value, which we denote by p_∞. The d-distance weight density, p_d, also depends on the code rate, the lower the rate, the higher the value of p_d. To determine the asymptote p_∞, we analyzed randomly chosen rate $R = b/c$, time-varying binary convolutional codes. We calculated the following values of p_∞ for some interesting rates: $p_\infty = 0.29$ for $R = 1/2$, $p_\infty = 0.37$ for $R = 1/3$ and $p_\infty = 0.40$ for $R = 1/4$.

III. Bit Error Probabilities via Encoder Inverses

We now compare the decoding bit error probability for systematic and nonsystematic encoders. For a particular encoder, let q_d denote the arithmetic average of the number of decoding bit errors per codeword 1 taken over all codewords of weight d. Somewhat surprisingly, q_d turns out to be an affine function of d with a slope that depends on the encoder type. The different slopes can be explained using an argument involving encoder inverses.

We model the appearance of 1's within a codeword of weight d by a binary memoryless source which outputs a 1 with probability p_d. For brevity, we consider here only rate $R = 1/2$ codes. For systematic encoders, whose encoder inverse has only one tap, the average number of bit errors per codeword 1 is then $q_d = 1/2$. This is reasonable since one would expect that half of all codeword 1's occur in the systematic bit-stream and thus create information bit errors. For quick-look-in encoders whose encoder inverses have two taps [2], we obtain $q_d = 1 - p_d$. Inserting the asymptote $p_\infty = 0.293$ for $R = 1/2$, we get $q_d = 0.71$. As the number of taps in the encoder inverse increases, q_d increases monotonically to its asymptotic value of 0.85. This explains why the average number of bit errors per codeword at distance d is larger for nonsystematic encoders than for the systematic ones.

References

[1] R. Johannesson and K. Sh. Zigangirov, *Fundamentals of Convolutional Coding*, IEEE Press, Piscataway, N.J., 1999.

[2] J. L. Massey and D. J. Costello, Jr., "Nonsystematic Convolutional Codes for Sequential Decoding in Space Applications," *IEEE Trans. Comm. Tech.*, Vol. Com-19, pp. 806-813, Oct. 1971.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

An Analytical Technique for Exact Error State Probability in Soft Decision Viterbi Decoding

Hideki Yoshikawa† Ikuo Oka‡ Chikato Fujiwara‡
†Suzuka National College of Tech.
Suzuka 510-0294, Japan
hyoshi@info.suzuka-ct.ac.jp
‡Faculty of Engineering
Osaka City University
Osaka 558-8585, Japan

I. Introduction

Although Viterbi decoding is widely used in practical systems, only a few studies have been made for exact analysis of error probability. In [2], we already proposed analytical technique for exact analysis of error state probability of 2-state soft decision Viterbi decoding. The extension to bit error probability analysis is possible with error state probability[3]. In this paper, this technique is extended to exact error state probability in 4-state soft decision Viterbi decoding. This employs an iterative calculation of probability density function of path metric.

II. Model for Analysis

Let us consider that the model for analysis is consisted of 4-state convolutional encoder of rate 1/2 with generator polynomial matrix given by $[1+D+D^2, 1+D^2]$ and signal set mapper of binary phase shift keying(BPSK). In this case, we assume that an output vector of the encoder $(b_1, b_2) \in \{0,1\}$ is transmitted as a BPSK modulated vector $u = (u_1, u_2) \in \{+1, -1\}$, where $u_i = 1 - 2b_i$, $i = 1, 2$.

III. Pdf of Path Metric and Error State Probability

For soft decision decoding, we assume the memoryless additive white Gaussian noise(AWGN) channel with zero mean and variance σ_0^2. The received vector $v = (v_1, v_2)$ can be expressed by Gaussian random variables. The conditional pdf of v assuming u is given by

$$f(v|u) = \frac{1}{2\pi\sigma_0^2} \exp\left[-\frac{(v_1-u_1)^2+(v_2-u_2)^2}{2\sigma_0^2}\right]. \quad (1)$$

The branch metric $M(b_1, b_2)$ is defined by the logarithm of (1), and we can express the metric as [1]

$$M(b_1, b_2) = \ln f(v|u) = A(u_1v_1 + u_2v_2) + B\,, \quad (2)$$

where A and B are independent of the paths, because these constants are the same for the paths compared, and path metric is additive. Thus, we can redefine $M(b_1, b_2) = u_1v_1 + u_2v_2$ as the branch metric.

Let us assume that an input sequence of encoder is all zero, that is, $b_1 = b_2 = 0$ and $u_1 = u_2 = 1$. The trellis diagram is given by Fig.1 where symbols u_1 and u_2 are both one, and branch metrics are shown with $x = v_1 + v_2$, $y = -v_1 + v_2$. In this figure, S_0, S_1, S_2, and S_3 indicate the encoder states. Here, S_0 is a correct state, S_1, S_2 and S_3 are error states, and their path metrics are 0, k_1, k_2, and k_3, respectively. After v_1 and v_2 are received, the path metrics become $\alpha_0 = \max\{x, k_2 - x\}$, $\alpha_1 = \max\{-x, k_2 + x\}$, $\alpha_2 = \max\{k_1+y, k_3-y\}$, and $\alpha_3 = \max\{k_1-y, k_3+y\}$, respectively. The conditional pdf of four random variables α_0, α_1, α_2, and α_3 is given by a product of $f(\alpha_0, \alpha_1|k_2)$, and $f(\alpha_2, \alpha_3|k_1, k_3)$.

$$f(\alpha_0, \alpha_1, \alpha_2, \alpha_3|k_1, k_2, k_3) = f(\alpha_0, \alpha_1|k_2) f(\alpha_2, \alpha_3|k_1, k_3) \quad (3)$$

In order to renew the metrics of correct and error states by subtracting the metric of correct state per a transition, we define difference path metrics $z_1 = \alpha_1 - \alpha_0$, $z_2 = \alpha_2 - \alpha_0$, and $z_3 = \alpha_3 - \alpha_0$, respectively. The conditional pdf of z_1, z_2, and z_3 is obtain by convolutional integral of (3) to eliminate α_0.

$$f(z_1, z_2, z_3|k_1, k_2, k_3) = \int_{-\infty}^{\infty} f(\alpha_0, z_1+\alpha_0, z_2+\alpha_0, z_3+\alpha_0|k_1, k_2, k_3) d\alpha_0 \quad (4)$$

The pdf of z_1, z_2, and z_3 after j transitions is given by

$$f^{(j)}(z_1, z_2, z_3) = \iiint f(z_1, z_2, z_3|k_1, k_2, k_3) f^{(j)}(k_1, k_2, k_3) dk_1 dk_2 dk_3 . \quad (5)$$

The initial path metric $\kappa_1, \kappa_2, \kappa_3$ is constant, and its pdf is represented by $f^{(1)}(k_1, k_2, k_3) = \delta(k_1 - \kappa_1, k_2 - \kappa_2, k_3 - \kappa_3)$. We begin to calculate the pdf $f^{(1)}(z_1, z_2, z_3)$. Then, the resultant z_1, z_2, and z_3 become the input to the next trellis, which it rewritten by k_1, k_2, and k_3 in (5), since we calculate iteratively. Finally, the pdf in a stationary condition $\hat{f}(z_1, z_2, z_3)$ is obtained by iterative calculation of (5), that is,

$$\hat{f}(z_1, z_2, z_3) \triangleq \lim_{j\to\infty} f^{(j)}(z_1, z_2, z_3). \quad (6)$$

Error state probability is defined as a probability that metric of one or more error states are larger than metric of the correct state. In Fig.1, S_0 is a correct state, S_1, S_2, and S_3 are error states. In this case, error state probability is given by

$$\Pr[\mathcal{S} \neq S_0] = 1 - \int_{-\infty}^{0}\int_{-\infty}^{0}\int_{-\infty}^{0} \hat{f}(z_1, z_2, z_3) dz_1 dz_2 dz_3. \quad (7)$$

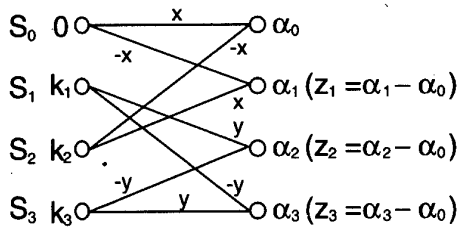


Fig. 1: Redefined trellis diagram

References

[1] A. J. Viterbi, "Convolutional Codes and Their Performance in Communication Systems," *IEEE Trans. Commun.* , vol. COM-19, pp. 751–772, Oct. 1971.

[2] H. Yoshikawa, I. Oka, and C. Fujiwara, "Exact Error Probability for Convlutional Codes with Soft Decision Viterbi Decoding," *Proc. IEEE ISIT'97* , p.426, Ulm, Germany, Jul. 1997.

[3] Y. Hayashi, H. Yoshikawa, I. Oka, C. Fujiwara, and Y. Daido, "Exact Analysis of Bit Error and Burst Error Probability for 2-state Soft Decision Viterbi Decoding," Submitted to *AEÜ Int. J. Electron. Commun.*

0-7803-5857-0/00/$10.00 ©2000 IEEE.

AWGN Channel Convolutional Decoding is Less Complex than BSC Decoding

John B. Anderson
Department of Information Technology
Lund University
Box 118
S-221 00 Lund, Sweden
e-mail: anderson@it.lth.se

Abstract — **The storage complexity of bounded distance decoding for binary-channel convolutional codes over the BSC is $\approx (2^{1-R}-1)^{-t}$, where up to t errors are corrected. We show that the path storage becomes $\approx 2^{2Rt}$ over the AWGN channel, which is significantly lower. Thus Gaussian convolutional coding is not only 3 dB more energy efficient, but its decoding is simpler as well.**

Earlier it has been demonstrated [1, 2] that breadth-first binary convolutional decoders that correct up to t errors over a BSC must store a number of trellis paths that grows exponentially with t according to

$$M \approx (2^{1-R}-1)^{-t}, \tag{1}$$

in which M is the number of paths and R is the code rate in data bits per channel use. We derive the exponential law that applies when the channel is instead an additive white Gaussian noise (AWGN) one. A more attractive law replaces (1), namely

$$M \approx 2^{2Rt}. \tag{2}$$

We assume that the breadth-first decoder is the M-algorithm, so that the M in (1) becomes the M needed in that algorithm, but the wider meaning of M is that of worst-case storage. A bounded distance decoder (BDD) is one for which a distance criterion Δ, or alternately an error correction criterion t, is specified: The BDD must correct any channel disturbance $\leq \Delta$ or t. We assume further that a certain stage far into the trellis has been reached and that paths have been deleted if they merge state or exceed the BDD criterion.

Let $x[1], x[2], \ldots, x[n] \in \{\pm 1\}$, be a word of an ordinary convolutional code of rate $R = (\log_2 \beta)/c$, where β is the branching factor at each trellis node and there are c binary symbols on each trellis branch. When two codewords lie at Hamming distance d_H^2 from each other, they lie at Euclidean distance $D_E^2 = 4d_H^2 E_s$ under binary antipodal transmission. Normalized to the data bit rate, this is $d_E^2 = 4d_H^2 E_s/2E_b = 2Rd_H^2$. Here E_b is the energy per data bit and E_s is the energy per channel bit. A bounded distance decoder working on these codewords guarantees correction of noises of normalized Euclidean square size δ^2 up to a limit

$$d_{E,free}^2/4 = Rd_{H,free}^2/2. \tag{3}$$

The first event error probability is

$$P_e \leq Pr\{|\,\eta\,| > \Delta\} = Q(\delta\sqrt{4E_b/N_o}) \leq (1/2)\, e^{-2\delta^2 E_b/N_o}$$

For AWGN channel convolutional BDD decoding at simple rates such as 1/2 or 1/3, the required survivor number M precisely doubles with each increase by 1/2 in the normed square distance criterion δ^2. This phenomenon has been observed in various forms during the 1990s. The law holds for δ^2 up to the $Rd_{H,free}^2/2$ limit in (3). The needed M in terms of d_H^2 is therefore $M = 2^{\lfloor Rd_H^2 \rfloor}$.

The general law for a BDD at δ in AWGN is actually

$$M = \beta^{\lfloor 2\delta^2/\log_2 \beta \rfloor}. \tag{4}$$

With d_H^2 set to $2t$, the asymptotic form of this in t is $M \approx 2^{2Rt}$. The source of law (4) is the fact that the words of a convolutional code occupy the vertices of a hypercube in signal space. The worst case storage of a breadth-first BDD decoder at δ is the largest number of signal points that can be enclosed by a ball in signal space with radius δ. Let a Kc-dimensional hypercube be made up from the symbols in the last K stages of the code trellis. The normalized Euclidean distance to any cube vertex is $\sqrt{KcR/2}$; the cube comprises β^K code points. Thus a $\sqrt{KcR/2}$-ball encloses at least these many. From these facts, (4) is at least an underbound. For any sensible code, it turns out that the ball will not enclose more points than (4): For this to happen, all codewords must take the same symbol value in one or more positions.

From the BSC law (1) we can form an approximate ratio for the survivors needed to make full use of a d_H^2 over the BSC, compared to full use of the same d_H^2 over the AWGN channel, where full use means that $\lfloor (d_H^2 - 1)/2 \rfloor$ or fewer errors are guaranteed never to occur. It is

$$\left[\frac{1}{2^R\sqrt{2^{1-R}-1}}\right]^{d_H^2}. \tag{5}$$

Thus the AWGN improvement in complexity grows exponentially with free distance. For example, at rate 1/2 a code with free distance 12 needs $(1.099)^{12} = 3.1$ times more survivor storage if works with a BSC rather than an AWGN model.

References

[1] J.B. Anderson, "Limited search trellis decoding of convolutional codes," *IEEE Trans. Information Theory*, vol. IT-35, pp. 944–955, Sept. 1989.

[2] R. Johannesson and K. Sh. Zigangirov, "Towards a theory for list decoding of convolutional codes," *Problems of Information Transmission*, No. 1, 1996.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Symbol Reliability Estimation Using Code Trellis Degeneration for QLI Codes

Masato Tajima, Atsushi Hatano, Keiji Takida, and Zenshiro Kawasaki
Dept. of Intellectual Info. Sys. Engineering
Faculty of Engineering, Toyama University
3190 Gofuku, Toyama 930-8555, Japan
e-mail: tajima@ecs.toyama-u.ac.jp

Abstract — **We clarify the relation between trellis degeneration (TDG) and symbol reliability estimation using the bidirectional Viterbi algorithm (BIVA) for the case of Quick Look-In (QLI) codes.**

I. Introduction

Based on an observation that the syndrome sequence corresponding to a received sequence z contains many segments with value 0 (i.e., *zero-strings*) under high SNR conditions, TDG can be realized for a syndrome trellis. Here, "degeneration" means to identify the error-free interval for each zero-string and to exclude such intervals from the normal decoding. In connection with this fact, we showed that TDG is also possible for a code trellis, if *Scarce State Transition* (SST) Viterbi decoding is applied to QLI codes. It is shown that the hard-decision input to the main decoder in an SST Viterbi decoder is just the syndrome in the case of QLI codes. This fact enables the code trellis corresponding to the main decoder to be degenerated. On the other hand, it is known that symbol reliability values are obtained by computing a *Viterbi algorithm* (VA) in two directions over a block of coded symbols. We call this scheme the *Soft-BIVA* (this is equivalent to the *Max-Log-MAP*). Then we showed that in the case of QLI codes, the symbol reliability values are obtained by applying the BIVA either to the code trellis for the main decoder or to the corresponding syndrome trellis [1]. As a result, a new problem of finding the relation between TDG and symbol reliability estimation using the Soft-BIVA has become crucial. In this paper, we show that the TDG process can be effectively utilized for symbol reliability estimation.

II. TDG and Symbol Reliability Estimation (1)

In the TDG process for a zero-string $[t, t']$, forward decoding is performed from each state at level t and backward decoding is performed from each state at level t'. Assume that TDG is successful and the sub-interval $[\tau, \tau']$ in which the *maximum-likelihood* (ML) path surely passes through state (0) (the *all-zero state*) has been identified. Then the *ML bits* (i.e., information bits on the ML path) corresponding to $[\tau, \tau']$ can be regarded as early detected information bits in the sense of Frey and Kschischang [2]. Note that if the degenerated sections are cut out of the original trellis, the remaining trellis sections are divided into sub-trellises terminated with state (0) at both ends. In this case, the reliability values for the ML bits which are contained in the part of a sub-trellis **not affected** by the TDG process are obtained by applying the Soft-BIVA to the sub-trellis under consideration.

III. TDG and Symbol Reliability Estimation (2)

Next, consider an interval $[t, t']$ **affected** by the TDG process. Note that the TDG process can be viewed as *trellis integration*. Hence, it is reasonable to evaluate the reliability value not for each ML bit but for the *integrated ML branch*. Assume that TDG is successful and the degenerated sub-interval $[\tau, \tau']$ has been identified. Let X_m^*(state $i_0 \rightarrow$ state j_0) be the integrated ML branch for $[t, t']$. Then the reliability value for X_m^* can be evaluated by

$$\Delta^* \equiv \ln[\mu(z, X_1^* + X_m^* + X_2^*)] - \max_{m' \neq m} \ln[\mu(z, X_3^* + X_{m'} + X_4^*)], \tag{1}$$

where $X_{m'}$ is any integrated branch other than X_m^*, and $X_1^*(X_3^*)$ and $X_2^*(X_4^*)$ are the best paths linked with $X_m^*(X_{m'})$ obtained by performing forward decoding and backward decoding, respectively. Since all the integrated branches pass through state (0) in $[\tau, \tau']$, Δ^* can be reduced to

$$\min\{(\alpha_{i_0} + \gamma'_{i_0 0}) - \max_{i \neq i_0}(\alpha_i + \gamma'_{i0}), (\gamma''_{0 j_0} + \beta_{j_0}) - \max_{j \neq j_0}(\gamma''_{0j} + \beta_j)\}, \tag{2}$$

where α_i and β_j denote the metrics of the best paths for state i at level t and state j at level t' obtained using forward decoding and backward decoding, respectively, and γ'_{i0} and γ''_{0j} denote the metrics for the path segments $i \rightarrow (0)(at\ \tau)$ and $(0)(at\ \tau') \rightarrow j$, respectively. Note that γ'_{i0} and γ''_{0j} are obtained when the TDG process for $[t, t']$ terminates. Also, α_i and β_j are obtained when the Soft-BIVA is applied to each sub-trellis after TDG. Hence, no extra computations are required for calculating the reliability value Δ^* for X_m^*.

IV. Relationship between Reliability Values for an ML Branch and ML Bits

Let X_m^* be the integrated ML branch for $[t, t']$. Let k be any level between t and t'. Also, let x^a be the path with $u_k \neq u_k^*$ which attains the reliability value Δ_k^* for the ML bit u_k^*. Note that the restriction of x^a to $[t, t']$ does not necessarily belong to a class of integrated branches for $[t, t']$. Then let s_t and $s_{t'}$ be the states which x^a passes through at levels t and t', respectively. Denote by X^a the best path connecting s_t and $s_{t'}$. In this case, if $X^a \neq X_m^*$ holds, then Δ_k^* is lower-bounded by the reliability value Δ^* for X_m^*.

References

[1] M. Tajima, K. Takida, and Z. Kawasaki, "Symbol reliability estimation using the bidirectional Viterbi algorithm with a code trellis and a syndrome trellis for QLI codes," *in Proc. ISIT'98*, p.204, Aug. 1998.

[2] B. J. Frey and F. R. Kschischang, "Early detection and trellis splicing : Reduced-complexity iterative decoding," *IEEE J. Selected Areas in Commun.*, vol.16, no.2, pp.153-159, Feb. 1998.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Snake-in-the-Box Codes as Robust Quantizer Index Assignments[1]

Sungill Kim and David L. Neuhoff
EECS Department, University of Michigan
Ann Arbor, MI 48109
{sungillk,neuhoff}@eecs.umich.edu

Abstract — **A good assignment of binary codewords to cells is necessary for a scalar quantizer to be robust to channel errors. We investigate a redundant assignment method that uses Snake-in-the-Box codes, which have a desirable distance-preserving property.**

I. Introduction and System Description

An index assignment (IA) associates length n binary codewords $w_1, \ldots, w_N$ to the cells, $S_1, \ldots, S_N$ of a scalar quantizer. A source sample x is encoded into the w_i corresponding to the cell S_i in which x lies; w_i is sent over a binary symmetric channel (BSC) with error probability ϵ; and a decoder produces $E\{X|r\}$ as the reproduction $\hat{x}$ of x, where r is the BSC output word.

This paper considers redundant IA's, i.e. $n > \log_2 N$. One approach is to use a set of codewords with as large minimum distance (d_{min}) as possible, so that some channel errors can be corrected, and then to assign codewords to cells to minimize the effects of uncorrectable error patterns, *cf.* [1]. Another approach, pursued here, is to allow $d_{min} = 1$, but use IA's that mitigate rather than correct channel errors, *i.e.* a few such errors should cause only a small error in $\hat{x}$. Snake-in-the-box (SIB) codes (also called circuit codes) can be used to make IA's of this type.

An (n, s, N) SIB code has the distance preserving properties that $d_H(w_i, w_{i+1}) = 1$, and $d_H(w_i, w_j) < s \Rightarrow |i - j| = d_H(w_i, w_j)$, where d_H is Hamming distance, and $s \geq 2$ is an integer called the spread of the code. This allows it to mitigate $\lfloor \frac{s-1}{2} \rfloor$ errors. SIB codes were first introduced as robust index assignments for A/D converters [2]. Over the years, the family of known SIB codes has gradually enlarged, *cf.* [3]. However, they have never been studied as general purpose index assignments for noisy channel quantizers. This paper presents the initial results of such a study.

II. Comparing SIB Codes to Other Approaches

Representative results are given in Fig. 1, which for an $N = 32$ level quantizer, compares the source SNR (SSNR) due to an (8,3,32) SIB index assignment to that due to other IA's, all computed using conventional means. The source sample is Gaussian, and the quantizer is optimized for it, assuming no channel errors. Because the various IA's cannot all be chosen to have the same codelengths n, to make fair comparisons, instead of fixing the BSC error probability ϵ, we fix an underlying analog channel (AWGN or AWGN plus Rayleigh fading) and use the ϵ that results from BPSK modulation. The channels are parameterized by their CSNR, defined as E_S/N_0, where E_S is the average received energy per data sample, and $N_0/2$ is the PSD of the white Gaussian noise.

In addition, the figure shows the SSNR resulting from using the [9,5] shortened Hamming code, which is an interesting comparison because it corrects single errors, whereas spread-3 SIB codes mitigate single errors. Also, shown is the SSNR due to the nonredundant natural binary code (NBC) index assignment, and that due to the NBC index assignment followed by a Hamming code, whose input length is not constrained to match the output length of the NBC. Note that the latter is a tandem system rather than an index assignment. (For the Rayleigh channel, only the [3,1] Hamming code results are shown, since they turned out to be best.)

One may see from Fig. 1 that the SIB index assignment is better than all other strategies, except at high CSNR for the AWGN channel, where the tandem Hamming codes are a little better. In our view, the SIB approach represents the better overall strategy because it is significantly better at small CSNR, while only slightly worse at high CSNR. In particular, as CSNR decreases, the channel error mitigation strategy leads to a more graceful degradation of SSNR than does the channel error avoidance strategy.

III. Conclusion

SIB codes have much potential to be used as an IA for joint source-channel coding. Their distance-preserving property protects against channel induced distortion, in a "bend-but-don't-break" fashion.

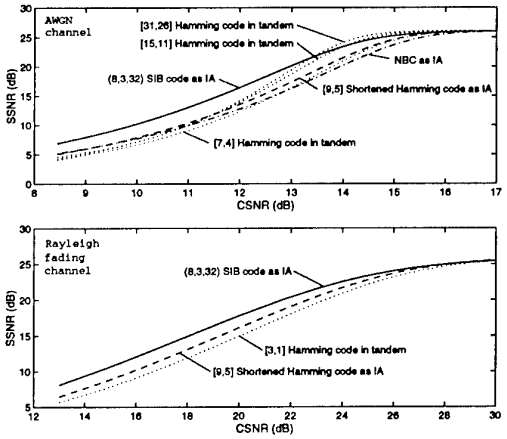


Fig. 1: Gaussian Source, 32 level SQ.

References

[1] G.A. Wolf, G. R. Redinbo, "The optimal mean-square estimate for decoding binary block codes," *IEEE Trans. Inf. Thy.*, 20, pp. 344-51, 1974.

[2] W.H. Kautz, "Unit-distance error-checking codes," *IRE Trans. Electr. Comp.*, EC-7, pp. 179-180, 1958.

[3] K.G. Paterson, J. Tuliani, "Some new circuit codes," *IEEE Trans. Inf. Thy.*, 44, pp. 1305-9, 1998.

[1]This work was supported by NSF grant NCR-9415754.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

VQ-Based Hybrid Digital–Analog Joint Source–Channel Coding

Mikael Skoglund[1]
Signals, Sensors, and Systems
Royal Institute of Technology
SE-100 44 Stockholm, Sweden
skoglund@s3.kth.se

Nam Phamdo
Dept. of ECE
State University of New York
Stony Brook, NY 11794-2350, USA
phamdo@ece.sunysb.edu

Fady Alajaji[2]
Dept. of Math. and Statistics
Queen's University
Kingston, ON K7L 3N6, Canada
fady@mast.queensu.ca

I. Introduction

Consider a system designed for conveying a d-dimensional random source vector, $\mathbf{X}$. A sample, $\mathbf{x}$, from the source is fed to the *encoder* ε, producing an index $i = \varepsilon(\mathbf{x}) \in \{0, \ldots, N-1\}$, where $N = 2^L$. The L bits of i are then fed to a binary symmetric channel (BSC), resulting in the output j producing a codevector $\mathbf{y}_j$ from the *decoder codebook* $\{\mathbf{y}_j\}_{j=0}^{N-1}$. We assume that the BSC corresponds to a Gaussian channel with noise variance σ^2 and with binary input in $\{\pm 1\}$.

At the transmitter, the index i also chooses a codevector $\mathbf{z}_i$ from the *encoder codebook*, $\{\mathbf{z}_i\}_{i=0}^{N-1}$, and the residual vector $\mathbf{e} = \mathbf{x} - \mathbf{z}_i$ is then formed. This vector is scaled by the constant α and transmitted over a discrete-time analog-amplitude Gaussian channel. (The scaling constant α regulates the transmission power.) The received vector $\mathbf{u} = \alpha \cdot \mathbf{e} + \mathbf{w}$, where $\mathbf{w}$ is zero-mean Gaussian with independent components of variance σ^2, is multiplied by a re-scaling constant β and then added to the codevector $\mathbf{y}_j$, resulting in an estimate of the transmitted source vector according to

$$\hat{\mathbf{x}} = \beta \mathbf{u} + \mathbf{y}_j.$$

Hence, the reproduction $\hat{\mathbf{x}}$ is *based on information transmitted both via a digital and an analog channel.* This is the key principle behind the work of this paper. Related previous work can be found in, e.g., [1, 2].

II. System Design and Performance

We will now present optimality criteria for the described HDA system, resulting in a design algorithm striving to minimize the distortion $D \triangleq E\|\mathbf{X} - \hat{\mathbf{X}}\|^2$ under a constraint on the transmitted power P_a per channel use in the analog channel. More precisely, the aim of the design is to find $\varepsilon(\mathbf{x})$, $\{\mathbf{z}_i\}$, $\{\mathbf{y}_j\}$ and β such that D is minimized, under the constraint that α is chosen such that $P_a = 1$ is satisfied at all times.

Optimality for a fixed encoder. Assume that $\varepsilon(\mathbf{x})$ is known and fixed, and define

$$\tilde{\mathbf{x}}(j) \triangleq E[\mathbf{X}|J=j], \; f_{kj} \triangleq \sum_{i=0}^{N-1} \Pr(I=i|J=j)\Pr(J=k|I=i)$$

and the matrices

$$\mathbf{Y} \triangleq [\mathbf{y}_0 \cdots \mathbf{y}_{N-1}], \; \tilde{\mathbf{X}} \triangleq [\tilde{\mathbf{x}}(0) \cdots \tilde{\mathbf{x}}(N-1)], \text{ and } (\mathbf{F})_{kj} = f_{kj}.$$

Then the optimal encoder and decoder codebooks, $\{\mathbf{z}_i\}$ and $\{\mathbf{y}_j\}$, can be *jointly* determined, by solving the equation

$$\mathbf{Y} \cdot (\mathbf{I}_N - \gamma \mathbf{F}) = (1-\gamma)\tilde{\mathbf{X}},$$

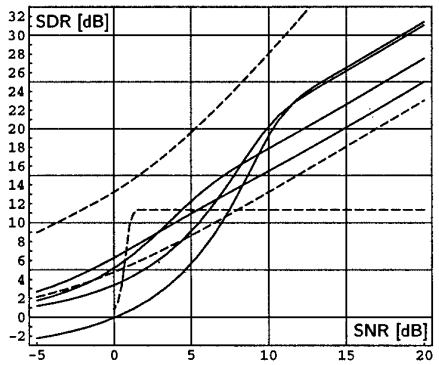
where $\mathbf{I}_N$ is the $N \times N$ unity matrix and $\gamma \triangleq \alpha\beta$, and then letting $\mathbf{z}_i = \mathbf{m}_y(i) \triangleq E[\mathbf{y}_J|I=i]$. Furthermore, the optimal β can be found (independently) as $\beta = \alpha^{-1}/(1+\sigma^2)$.

Optimality for a fixed decoder codebook. Now assume that $\{\mathbf{y}_j\}$ is given, that $\{\mathbf{z}_i\}$ is chosen as $\mathbf{z}_i = \mathbf{m}_y(i)$, and that $\beta = \alpha^{-1}/(1+\sigma^2)$, as above. The optimal encoder then is

$$\varepsilon(\mathbf{x}) = \arg\min_l \left\{(1-\gamma)\cdot\|\mathbf{x} - \mathbf{m}_y(l)\|^2 + g_l\right\},$$

where $g_i \triangleq E[\|\mathbf{y}_J\|^2|I=i] - \|\mathbf{m}_y(i)\|^2$. Based on these results, the system can be (locally) optimized *at an assumed channel* SNR, $1/\sigma^2$, using an iterative approach similar to the well-known generalized Lloyd algorithm for VQ design.

Motivated by a broadcast scenario, we illustrate below the performance (signal-to-distortion ratio versus SNR) of employing a *fixed encoder* and an *adaptive decoder* (adapts to a varying SNR), denoted by FE$_*$AD where $*$ is the design SNR of the encoder. We also illustrate some benchmark schemes. All systems use a rate of two channel uses per source sample. The source is Gauss-Markov with correlation 0.9.



Dashed lines from above at SNR = 15 dB: The Shannon bound (distortion-rate function evaluated at channel capacity); a purely analog system (transmits each source sample twice, minimum mean-square error receiver); a purely digital tandem system (source-optimized VQ with $d = 8$ and $L = 8$, rate–1/2 Turbo code with $(n,k) = (2048, 1024)$ and generators $(37, 21)$). *Solid lines from above* at SNR = 15 dB: A HDA system with source-optimized VQ, and; HDA-FE$_*$AD systems with $* = 10$, 5, 0 dB. All HDA systems use $d = 8$ and $L = 8$.

We observe that the HDA systems outperform the tandem system and the analog system (at high SNRs). In particular we note the *graceful improvement* of the HDA systems, as opposed to the *leveling-off* in performance of the tandem system. We also observe that the performance can be improved at low SNRs using the optimization procedure.

References

[1] U. Mittal and N. Phamdo, "Joint source–channel codes for broadcasting and robust communications," *Submitted to IEEE Transactions on Information Theory*, Nov. 1998.

[2] S. Shamai, S. Verdú, and R. Zamir, "Systematic lossy source/channel coding," *IEEE Transactions on Information Theory*, vol. 44, pp. 564–579, Mar. 1998.

[1]The work of M. Skoglund was supported in part by the Swedish Research Council for Engineering Sciences.

[2]The work of F. Alajaji was supported in part by the Natural Sciences and Engineering Research Council of Canada

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Optimal Linear Labelling for the Minimisation of both Source and Channel distortion

Jean-Claude Belfiore
ENST, 46, rue Barrault
75013 Paris
e-mail: belfiore@com.enst.fr

Xavier Giraud
ENST, 46, rue Barrault
75013 Paris
e-mail: giraud@com.enst.fr

Jorge Rodriguez-Guisantes
ENST, 46, rue Barrault
75013 Paris
e-mail: rodrigez@com.enst.fr

Abstract — **In [1], it was proved that distortion due to a binary symmetric channel is minimized by a linear labelling. In this paper, we show how to obtain an asymptotically optimal linear labelling which also minimizes the source distortion for Gaussian sources. This linear labelling is based on the notion of component diversity which can be obtained by algebraic constructions derived from Number Theory [3].**

I. Problem statement

In this work, we present, an approach for Joint Source-Channel Coding based on the minimisation of, first, channel distortion and then, source distortion. This problem has been traditionnally treated from the source coding point of view [2]. First, the source codebook is matched to the source statistics in order to minimize distortion due to the source, and then, the labelling, i.e. the mapping between the source codebook and the channel codebook, is optimized in order to minimize distortion due to the channel. Our approach follows the channel point of view. We propose to optimize, first, the channel distortion and then, the source distortion.

In [1], it has been proved that, on binary symmetric channels, the channel distortion is minimized if the vector quantizer can be expressed as a linear transform of a hypercube. We propose to extend this approach by finding a set of linear transforms which minimizes the channel distortion,along with the distortion of Gaussian sources.

II. Linear labelling to minimize channel distortion

By constraining the labelling to be linear, we solved the problem of minimisation of the channel distortion. Now, we are concerned with the problem of source distortion minimisation. We focus our investigation to the case of a memoryless zero-mean Gaussian source with variance σ_s^2. With our assumptions, one can express points of the source codebook $\vec{y}$ as a linear function of the points of the hypercube

$$\vec{y} = \mathbf{G}\vec{h},$$

with $\mathbf{G}$ being a matrix representing the linear transform. $\mathbf{G} = [g_{i,j}]$ has d rows and n columns.

III. Minimisation of source distortion (Gaussian sources)

By looking at the expression of the components of $\vec{y}$,

$$y_i = \sum_{j=1}^{n} g_{i,j} h_j \quad i=1,2,\ldots,d$$

we can see that, in order to mimic a memoryless Gaussian source, $\vec{y}$ must have the same distribution. To obtain this distribution, we need to apply the central limit theorem to the independent random variables h_j. In order to insure the Gaussianity of $\vec{y}$, we need that all components $g_{i,j}h_j$ of the summation be nonzero, for any vector $\vec{h}$.

This property can be obtained with "maximum component diversity" constellations [3]. Let $\mathbf{M}$ be the $n \times n$ generator matrix of a "maximum component diversity" constellation. Then we can obtain the previous property by taking $\mathbf{G}$ equal to any set of d rows of $\mathbf{M}$.

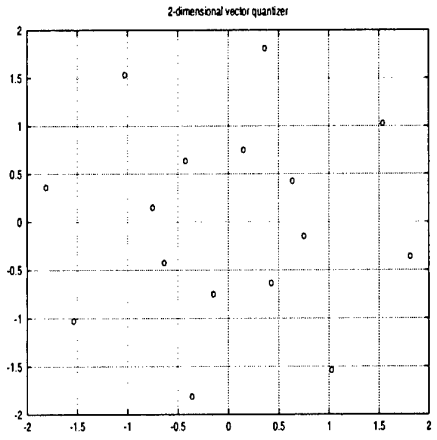
We can show how to construct full diversity rotations of dimension $n = 2^m$, m being a positive integer. As an example, we construct a full diversity rotation matrix with $m = 2$. In this case, we obtain

$$\mathbf{M} = \frac{\mathbf{1}}{\sqrt{2}} \begin{bmatrix} \omega_3 & \omega_9 & \omega_{15} & \omega_{21} \\ \omega_7 & \omega_{21} & \omega_3 & \omega_{17} \\ \omega_{11} & \omega_1 & \omega_{23} & \omega_{13} \\ \omega_{15} & \omega_{13} & \omega_{11} & \omega_9 \end{bmatrix}$$

with

$$\omega_l = \cos\left(\frac{\pi}{2^{(m+2)}} \cdot l\right)$$

Assume that we need a quantizer of dimension, let us say, 2. Take, as an example the first and third line of $\mathbf{M}$ to obtain the codebook represented below,



References

[1] P. Knagenhjelm, and E. Agrell, "The Hadamard Transform - A Tool for Index Assignment," *IEEE Trans. on Information Theory*, vol. IT 42, pp. 1139-1151, July 1996.

[2] N. Farvardin and V. Vaishampayan, "Optimal Quantizer design for Noisy Channels : an approach to combined Source-Channel Coding," *IEEE Trans. on Information Theory*, vol. IT 33, pp. 827-838, Nov. 1987.

[3] X. Giraud, E. Boutillon, and J.-C. Belfiore, "Algebraic Tools to Build Modulation Schemes for Fading Channels," *IEEE Trans. on Information Theory*, vol. IT 43, pp. 938-952, May 1997.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Robust Signal Compression using Joint Fixed- and Variable-length Coding

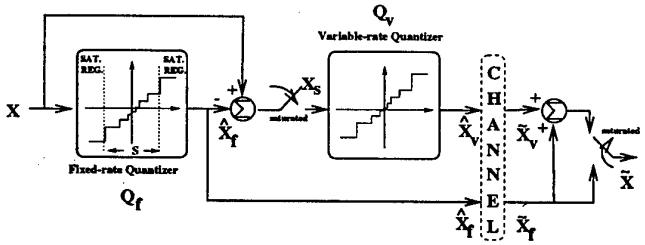
A. Aydın Alatan
ECE Dept., NJCMR
New Jersey Institute of Technology
Newark NJ 07102
e-mail: alatan@oak.njit.edu

John W. Woods
ECSE Dept., CIPR
Rensselaer Polytechnic Institute
Troy NY 12180-3590
e-mail: woods@ecse.rpi.edu

Abstract — **A transmitted signal is decomposed into two parts which are then encoded using fixed- and variable-length coding, respectively. Compared to conventional variable-length codewords with synchronization-symbols or fixed-length coding strategies, the proposed method enjoys a better distortion-rate performance on particular channels.**

I. Joint Fixed- and Variable-length Coding

A fixed-length coding strategy is optimal for a uniformly distributed (flat) source probability density function (pdf). For a zero-mean memoryless Gaussian source, it is possible to find an approximately flat region centered around the origin of its pdf. This region can be encoded using fixed-length codewords while slightly losing from compression efficiency. In the mean time, it is still possible to encode the tail of this distribution by a variable-length coding scheme. A typical system is shown below.

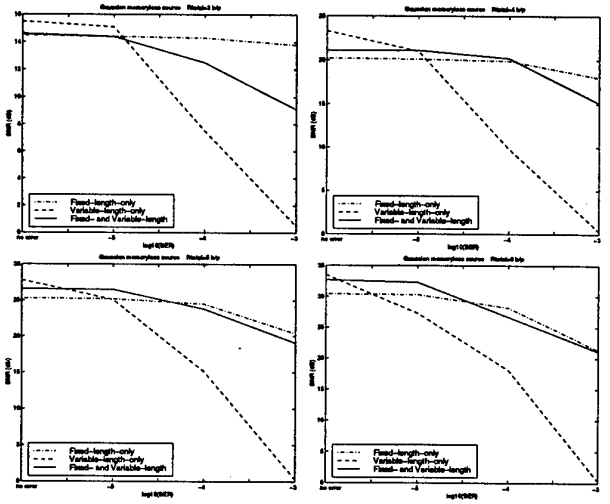


In this system, when a signal value, x, saturates in the fixed-length coded quantizer, $\mathbf{Q_f}$, x is subtracted from its fixed-length quantized version, $\hat{x}_f$ and the switch between fixed and variable-length quantizers is closed. The difference is then passed to the residual stage, where this saturation offset, x_s is quantized by variable-length quantizer, $\mathbf{Q_v}$, and the quantized residue $\hat{x}_v$ is encoded using a variable-length code. After transmission of $\hat{x}_f$ and $\hat{x}_v$, the receiver checks whether a signal value is saturated or not, using the received fixed-length coded part, $\tilde{x}_f$, and if so, it will decode and add the received quantized difference, $\tilde{x}_v$, on top of $\tilde{x}_f$.

S-parameter gives the width of the reserved non-saturating region of the signal pdf and R_{fixed} denotes the bit rate reserved for the fixed-length quantizer, $\mathbf{Q}_f$, from the overall total rate, R_{total}. For a given channel and R_{total} value, our design goal is to find the optimal (S, R_{fixed}) pair so that the distortion of the reconstructed signal at the receiver is minimized. Since, in noisy channels, an analytical distortion analysis for variable-length coded data is not possible, the "best" (S, R_{fixed}) pair, rather than the optimal, is found by the using operational rate-distortion characteristics.

II. Simulations

The fixed-length quantizer utilized in the simulations is a derivative of Lloyd-Max quantizer (LMQ) [1]. The variable-length coded or saturated component is quantized using an ECSQ [2], whose output indices are entropy coded using Huffman coding. This variable-length bit-stream is protected from error propagation by carving it up into slices and adding end-of-slice (EOS) markers. The simulated channel is taken to be a simple binary symmetric channel (BSC) and simulations are conducted for different bit error-rates (BER).



SNR vs. BER : Gaussian memoryless source for fixed-length, variable-length and joint fixed and variable-length coding (solid line) for (left-to-right) R_{total} = 3, 4, 5 and 6 b/p.

III. Conclusion

For some BER range (between 10^{-4} and error-free), separating a symbol into two (saturating and non-saturating) parts and encoding these parts appropriately, is advantageous compared to variable- or fixed-length-only strategies. The most attractive property of this approach is its capability for dividing any source into subsources with different error immunities. Hence, unequal channel error protection is possible in the symbol level for any source.

References

[1] A. Gersho and R. M. Gray, *Vector Quantization and Signal Compression*, Kluwer Academic Press, 1992.

[2] P. A. Chou, T. Lookabaugh and R. M. Gray,"Entropy Constrained Vector Quantization", *IEEE Trans. on ASSP*, vol. 37, no. 1, pp. 31–42, Jan 1989.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

ARQ Protocols for the Gaussian Collision Channel

G. Caire and D. Tuninetti
Institut Eurécom
Sophia-Antipolis, France
e-mail: caire, tuninett @eurecom.fr

Abstract — **In next generation wireless communication systems, packet-oriented data transmission will be implemented in addition to standard mobile telephony. Designing efficient schemes for packet transmission on top of an existing connection-oriented CDMA system will be a challenge for system designers. In this work, we take an information-theoretic view of some simple protocols for reliable packet communication based on "hybrid ARQ".**

In order to support new sevices (e.g., wireless mobile access to the Internet), next generation wireless communication systems will implement packet-oriented data transmission in addition to standard mobile telephony. This implies bursty sporadic communication from a large population of users, that may require instantaneous large data rates and very small error probabilities for a short time. On the other hand, next generation systems will be based mainly on CDMA, which is suited to continuous-mode transmission and (at least in its current conventional implementation [1]) it requires closed-loop power control. Then, a challange for future system designers is to implement efficient schemes for packet transmission on top of an existing connection-oriented CDMA system, preserving the uncoordinated access flexibility of the latter. In essence, next generation wireless systems should be regarded as "composite" systems where several subsystems with very different power, rate, reliability and delay constraints will coexist, sharing the same bandwidth.

Motivated by the above consideration, we take an information-theoretic view of some simple protocols for reliable packet communication based on "hybrid ARQ", i.e., on combining *channel coding* and *Automatic Retransmission reQuest* (ARQ). We model low-power low-rate continuous-mode traffic as background white Gaussian noise for the high-rate high-power bursty users. Random user activity prevents closed-loop power control and user coordination. Then, we assume that users transmit their signal *bursts* at very high instantaneous power and in a completely uncoordinated way. The receiver is formed by a bank of conventional single-user decoders, and does not implement joint decoding. We refer to this model as the *Gaussian collision channel* [3]. The transmission of each user is governed by an hybrid ARQ protocol, designed in order to achieve very low error probability.

We consider a slotted multiple access Gaussian channel with fading. We study the system performance in terms of throughput (total bit/s/Hz) and average delay for three simple idealized hybrid ARQ protocols: a coded version of Aloha, a repetition scheme with maximal-ratio packet combining and an incremental redundancy scheme with general coding. By applying the *renewal-reward* thereom [4], we obtain a closed-form throughput formula under a delay constraint (time-out) and code rate constraint. Since we consider random coding and typical set decoding, our results are independent of the particular coding/decoding technique and should be regarded as a limit in the information theoretic sense. Then, we study asymptotic behaviors with respect to various system parameters. The system throughput is compared to that of a conventional CDMA with conventional decoding. Interestingly, the ARQ system is not interference-limited even if no multiuser detection or joint decoding is used (arbitrarily high throughput can be obtained by increasing the user transmit power), as opposed to conventional CDMA.

As a byproduct of this analysis, we provide a stronger operational meaning to the information outage probability of block-fading channels and we obtain the closed form probability distribution of signal-to-interference plus noise ratio (SINR) with Rayleigh fading and a Poisson-distributed number of interferers, extending the result of [5].

In the full paper [2], we give all the details of the proofs and a wide range of numerical results illustrating the performances of the examined ARQ protocols, as well as a comparison with conventional CDMA (another form of "collision channel") which shows that especially for high SNR the slotted ARQ system provides great potential advantages. In fact, it is well-known that conventional CDMA is interference limited while the slotted ARQ system is not.

As a conclusion, we can say that as far as packed data communication is concerned, it is more useful to spend the feedback channel to provide ACK/NACK for the ARQ protocol rather than to provide power control commands.

References

[1] A.J.Viterbi. *CDMA principles of Spread Spectrum Communication.* Addison-Wesley, New York, 1995.

[2] G.Caire and D.Tuninetti. ARQ protocols for the Gaussian collision channel. *submitted to IEEE Trans. on Inform. Theory*, 1999. Downloadable from http://www.eurecom.fr/ caire/

[3] E.Leonardi G.Caire and E.Viterbo. Modulation and coding for the Gaussian collision channel. *Accepted for pubblication in IEEE Trans. on Inform. Theory*, 1999.

[4] R.Wolff. *Stochastic modeling and the theory of queues.* Prentice-Hall, Upper Saddle River, New York, 1989.

[5] S.Shamai(Shitz) and A.D.Wyner. Information-theoretic considerations for symmetric, cellular, multiple-access fading channels - Part II. *IEEE Trans. on Inform. Theory*, 43(6):1895-1911, November 1997.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Capacity of Time-Slotted ALOHA Systems

Muriel Médard[1]
MIT
e-mail: medard@mit.edu

Sean P. Meyn[1] Jianyi Huang[1]
University of Illinois
Urbana-Champaign

Andrea J. Goldsmith[2]
Stanford University

Abstract —

We establish a region of reliably received rates for time-slotted ALOHA systems. We combine concepts from multiple-access channels and broadcast channels to determine a capacity region for a single transmission of a packet (which is long enough to achieve capacity) in an ALOHA system and determine capacity-achieving strategies.

I. Introduction

The flexibility of ALOHA systems, which were first proposed in 1970 by Abramson, makes them an attractive option for wireless data applications. In the original ALOHA system, if a collision among packets occurs at the receiver, those packets are discarded and the users retransmit those packets. Several coding schemes have been proposed for ALOHA packets to allow at least part of the data in the packets to weather out one or several collisions. Depending on the presence or absence of other users, each user will be able to achieve different rates. Since some transmitted bits will be lost owing to collisions, we consider a maximum *reliably received* rate region rather than maximum *reliably transmitted* rate region ([4]).

II. Single packet system.

We consider a time-slotted ALOHA system with two users. Users, at each time slot, determine according to a Bernoulli process whether to transmit. A packet occupies one time slot, which is long enough so that Shannon capacity is approximately achieved over that time slot (i.e. the slot duration is long enough so that Pe is approximately zero when transmitting at the Shannon rate). The users share an AWGN channel with noise variance σ_N^2. Users 1 and 2 have average power constraints σ_1^2 and σ_2^2.

We combine concepts from rate splitting for multiple-access communications ([5]) and broadcast channels ([1], [2]). The rationale behind our approach springs from the following observation. In multi-access channels, rate splitting achieves capacity by creating virtual users and decoding all users using interference cancellation. In a degraded AWGN broadcast channel, the low resolution code is decoded by considering the high resolution code as noise. Hence, there is similarity between the decoding mechanism for achieving capacity in multiple-access and in degraded broadcast channels ([3]). In the system we consider, a user codes to transmit over two possible channels- a channel with the other user present and a channel without the other user.

We begin by presenting a coding scheme. As for rate splitting, we divide user 1 into two users, U_1' and U_1'', which send independent WGN signals with variance $\beta\sigma_1^2$ and $(1-\beta)\sigma_1^2$, respectively. User 2 maps to a single user, U_2. As in broadcast channels, each of the users we constructed sends two messages on two separate signals. U_1' sends signal LR_1' and HR_1', which are independent WGN signals with variance $\alpha_1'\beta\sigma_1^2$ and $(1-\alpha_1')\beta\sigma_1^2$, respectively. U_1'' sends signal LR_1'' and HR_1'', which are independent WGN signals with variance $\alpha_1''(1-\beta)\sigma_1^2$ and $(1-\alpha_1'')(1-\beta)\sigma_1^2$, respectively. U_2 sends signal LR_2 and HR_2, which are independent WGN signals with variance $\alpha_2\sigma_2^2$ and $(1-\alpha_2)\sigma_2^2$, respectively. Note that all αs and β are in $[0,1]$. We decode signals (performing interference cancellation) in the order: first LR_1', second LR_2, third LR_1'', fourth HR_1'', fifth HR_2 and sixth HR_1'. Our arguments can easily be extended to more than two users. Our rate region is defined as the achievable rates for the cases wher we have both users, user 1 only, user 2 only, and no users. Our coding scheme achieves the rate region.

III. Expected rate.

We may select the αs and βs to maximize the expected achievable rate, when the users' energies and probabilities of transmission are fixed. An interesting special case arises when both users transmit with equal probability. Our results show that, regardless of whether we operate at high SNR or low SNR, when the users have SNRs which are comparable, then we do not need to split the users between HR and LR. When we have highly asymmetrical SNRs, then for low enough transmission probability, such splitting is required to achieve the capacity region.

IV. Conclusions.

We have determined a capacity region (where capacity region refers to the rates achievable under the four scenarios described above) for an ALOHA system in the case of a single time slot with very long length, such that we can achieve capacity over a single packet transmission. We may extend our results to several time slots.

Instead of considering a single transmission, we can consider several transmissions. In the limit as the number of transmissions is arbitrarily large, preliminary results show that our system is stable: if the average rate arriving to the system is below the expected rate, that rate can be reliably received. Another interesting area of further research is maximizing the expected rate when the average power (determined by the product of the average per-time slot power given by σ^2 and the probability of transmission) is fixed.

References

[1] T.M. Cover, "Broadcast Channels", *IEEE Trans. on Info. Theory*, IT-18, pp. 2-14, 1972.

[2] T.M. Cover, "An Achievable Rate Region for the Broadcast Channel", *IEEE Trans. on Info. Theory*, IT-21, pp. 399-404, 1975.

[3] T.M. Cover, "Comments on Broadcast Channels", *IEEE Trans. on Info. Theory*, vol. 44, pp. 2524-2530, 1998.

[4] M. Effros, A. Goldsmith, "Capacity Definitions and Coding Strategies for General Channels with Receiver Side Information", *Proc. of ISIT 98*, pg. 39, 1998.

[5] B. Rimoldi and R. Urbanke, "A Rate Splitting Approach to the Gaussian Multiple-access Channel", *IEEE Trans. Info. Theory*, vol. 42, pp. 364-375, 1996.

[1]This work was supported by Grant NSF Grant CCR 99-79381.
[2]ONR Young Investigator award N00014-99-1-0578 and ONR award N00014-99-1-0698.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On stability of DS-CDMA data networks with code combining

Rajiv Vijayakumar
EECS Department
University of Michigan
Ann Arbor, MI 48109-2122, USA
e-mail: rvijayak@eecs.umich.edu

Kimberly M. Wasserman[1]
EECS Department
University of Michigan
Ann Arbor, MI 48109-2122, USA
e-mail: wass@eecs.umich.edu

Abstract — **An equation is derived whose solution(s) yield the number of transmitting mobiles in the equilibrium state(s) for a DS-CDMA network employing code combining(CC). Numerical results for a simple form of CC show that while there may exist multiple equilibria, these are typically clustered together, and do not cause a significant degradation in throughput. The results also show that CC is capable of eliminating bistability, and of having a single equilibrium state at which the throughput is slightly better than that at the desirable equilibrium state for the corresponding DS-CDMA network employing automatic repeat request.**

I. Introduction

Code combining is known to enhance throughput over point-to-point links. A receiver operating under code combining does not discard information from a transmission received in error; instead it requests an additional transmission and combines information from the new transmission with that from the original one with the goal of increasing the probability of successful reception. We investigate the effect of using code combining as the link layer protocol on the stability of a direct-sequence code division multiple access (DS-CDMA) network. Details may be found in [1].

II. Model

Consider a DS-CDMA packet data network consisting of a single base station and M mobiles. Each mobile transmits fixed length packets with a spreading gain of N chips per bit. The time-axis is divided into contiguous equal-length slots, each of which has a duration equal to the time required to transmit a single packet. Mobiles initiate transmissions only at the beginning of time slots. The spreading code used by a mobile is assumed to change from slot to slot (*e.g.*, IS-95), so that the outcomes of the transmission attempts of the active mobiles are assumed to be mutually independent, both within a slot, and across time slots. Perfect power control is assumed.

Each mobile has a buffer of size one. If a mobile has a packet in its buffer, it is considered "active"; otherwise, it is "idle". In any given time slot, all active mobiles transmit, and each idle mobile generates a packet with probability λ. The receivers at the base station are assumed to be of the conventional matched filter type. Neglecting the effect of thermal noise, the bit-energy-to-interference density ratio at the receiver for any given mobile becomes $\mathcal{E}_b/I_0(j) = \frac{N}{(j-1)}$, where j is the number of active mobiles. The probability of a successful packet transmission by an active mobile is a non-decreasing function of the $\mathcal{E}_b/I_0$ at the receiver throughout the packet transmission time.

[1]This work was supported in part by the U.S. Army Research Office under grants DAAH04-96-1-0377 and DAAH04-96-1-0177.

III. Equilibrium states

We assume that there is some maximum number E of transmissions attempts that may be made for a given data packet. A packet is discarded after E attempts; higher layer protocols will treat it as lost, and take the appropriate action. Define the random sequence $S = \{S_n; n \in \mathbb{Z}_+\}$, where $S_n = (\boldsymbol{x}_n, \boldsymbol{h}_n)$, $\boldsymbol{x}_n = (x_n^1, x_n^2, \ldots, x_n^E)$, and $\boldsymbol{h}_n = (h_n^1, h_n^2, \ldots, h_n^E)$. Here $x_n^j \in [0,1]$ is that fraction of all mobiles which, in slot n, are making their j^{th} attempt at transmitting some data packet, and $h_n^j = \sum_{k=1}^{E} x_{n-j+1}^k$ is that fraction of all mobiles that are active in slot $n-j+1$. The vector $\boldsymbol{h}_n$ represents the interference history of active mobiles. Call S_n the state of the network at time n, $n \in \mathbb{Z}_+$. It follows from the modeling assumptions in Section II that S forms a Markov chain.

Denote a typical state of the network by $\boldsymbol{s}$, where $\boldsymbol{s} = (\boldsymbol{x}, \boldsymbol{h})$, $\boldsymbol{x} = (x^1, \ldots, x^E)$, and $\boldsymbol{h} = (h^1, \ldots, h^E)$. Write $x = x^1 + \cdots + x^E$ for the total fraction of mobiles that are active. Let $p^j(\boldsymbol{h})$ denote the probability of successful reception for packets being transmitted for the j^{th} time when the network is in state $\boldsymbol{s} = (\boldsymbol{x}, \boldsymbol{h})$.

Equilibrium states are those states $\boldsymbol{s}$ for which $E[S_{n+1} \mid S_n = \boldsymbol{s}] = \boldsymbol{s}$. Solving this system of equations yields $h^j = x$, $x^j = \lambda(1-x)\prod_{k=1}^{j-1}\left(1-p^k(\boldsymbol{h})\right)$, $j = 1, 2, \ldots, E$, and $x = \lambda(1-x)\left(1 + \sum_{j=2}^{E}\prod_{k=1}^{j-1}\left(1-p^k(\boldsymbol{h})\right)\right)$.

Thus—although the state space is multi-dimensional—for a given arrival rate λ, the equilibrium states $\boldsymbol{s}$ are *uniquely* determined by the fraction x of mobiles that are active in those states. Further, given λ, the values of x corresponding to the equilibrium states are given by the solutions of the equation $\lambda = \frac{x}{(1-x)\left(1+\sum_{j=2}^{E}\prod_{k=1}^{j-1}\left(1-p^k((x,x,\ldots,x))\right)\right)}$, $0 \le x \le 1$.

As the number of mobiles and the spreading gain tend to infinity (with their ratio held constant), the evolution of the stochastic system, by the law of large numbers, converges to a deterministic trajectory. If this deterministic trajectory is globally asymptotically stable, then the steady state probability distribution of the fraction of mobiles that are active converges to a point mass at the unique equilibrium. It is not known whether the deterministic system is globally asymptotically stable in general; finding the appropriate Lyapunov function remains an open problem.

IV. Numerical results

Numerical results show that the use of CC can eliminate the undesired equilibrium state present in conventional DS-CDMA networks, thereby significantly improving throughput. In cases for which CC has multiple equilibria, the numerical results show that these equilibria are typically close together and do not significantly degrade throughput.

References

[1] R. Vijayakumar and K. M. Wasserman, "On stability of DS-CDMA wireless data networks," Tech. Rep. CGR 99-02, EECS Dept., University of Michigan, 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Buffer Control for Communication over Fading Channels

Randall Berry Robert Gallager [1]
Laboratory for Information and Decision Systems
Massachusetts Institute of Technology
77 Massachusetts Avenue, Rm. 35-303
Cambridge, MA 02139
e-mail: randy1@mit.edu, gallager@lids.mit.edu

Abstract — **We consider a user communicating over a flat fading channel. The user wishes to reliably communicate bursty data over this channel while minimizing both the average power and the average delay incurred. We formulate a buffer control problem which illustrates the trade-off between these quantities. This model is analyzed using dynamic programming techniques. The asymptotic performance is shown and asymptotically optimal buffer control policies are given.**

I. Introduction

Motivated by wireless communication, channel models where the output conditionally depends on a time-varying channel state have received much attention. Cases where either the transmitter or receiver have access to channel state information (CSI) have been well studied. Using the CSI, the transmitter can allocate communication resources over time in an effort to combat the fading. In this work, we study such resource allocation problems for a single user in a flat fading channel when both the transmitter and the receiver have perfect CSI. The goal is to minimize the transmission power required to provide the user with an acceptable quality of service. Minimizing power is an important consideration since mobile users rely on batteries with limited energy.

If the user simply required a long term average rate, then minimizing the average power needed to communicate reliably is equivalent to characterizing the channel's capacity. This has been well studied for a large class of fading channels. Approaching the capacity of a fading channel, typically requires the use of codewords whose length is long enough to average over the channel statistics. We consider the situation where in addition to an average rate, the user requires a given average delay. When delay constraints limit codeword lengths, then capacity may not be a *useful* performance criterion; *i.e.* one can not get an acceptable probability of error at rates near capacity while satisfying the delay constraint. This is the motivation behind the work on outage capacity and delay-limited capacity. We also assume that messages arrive from a higher layer protocol in a bursty manner and are placed into a transmission buffer. Delay requirements may prevent one from removing this burstiness through source coding.

We consider the following model. Assume that the messages are fixed length packets of $\log M$ bits which arrive from some higher layer application and are placed into a transmission buffer. Let A_n be the number of packets that arrive at time n, where $\{A_n\}$ is an ergodic Markov chain with steady-state average arrival rate $\bar{A}$. Periodically, the transmitter removes a packet from the buffer, encodes it into one of M codewords of infinite length, and begins transmitting the codeword over a fading channel. Assume the channel is a complex, additive white Gaussian noise channel with a time-varying gain $H_n \in \mathbb{C}$. The process $\{H_n\}$ is also modeled as an ergodic Markov chain. While transmitting, the transmitter can adjust the transmission energy by scaling the input by an adjustable gain. This decision is based on the channel state, the buffer occupancy and the current source state. Once the receiver can decode the message with an acceptable probability of error, the transmitter stops transmitting the packet and proceeds to the next packet. We formulate a new buffer model where the buffer occupancy corresponds to the amount of error exponent required by each packet; this is a variation of the model used in [1]. At each time U_n, the amount of exponent to be transmitted, is chosen. A given choice of U_n requires $P(H_n, U_n)$ average transmission energy.

We consider the problem of minimizing the average transmission power subject to a given average delay constraint. Let $P^*(D)$ be the minimum average power required for the average delay to be less that D. We show that $P^*(\cdot)$ is always a non-increasing convex function. Each point of $P^*(D)$ can be found by minimizing

$$\lim_{n\to\infty} \frac{1}{m} \sum_{i=1}^{m} P(H_n, U_n) + \beta \frac{S_n}{\bar{A}}$$

for an appropriate choice of β. Here S_n corresponds to the buffer occupancy at time n. This corresponds to solving an average cost dynamic programming problem where the cost is a weighted sum of the average power and average delay.

We study the behavior of $P^*(D)$ as $D \to \infty$. Our approach to this problem is similar to the work in [2] on buffer control for variable rate lossy compression. The mathematical structure underlying these problems has many similarities. Let $\mathcal{P}(\bar{A})$ denote the limiting value of $P^*(D)$. We characterize $\mathcal{P}$ and show that $P^*(D) - \mathcal{P}(\bar{A}) = \Theta(1/D^2)$. Finally a sequence of *simple policies* is given which exhibit this optimal convergence rate. These policies have the characteristic that the transmission rate is a function only of the the channel state and in which of two regions the current buffer state lies.

[1]This work was supported by the Army Research Office under grant DAAG55-97-1-0305.

References

[1] E. Telatar and R.G. Gallager, "Combining Queuing Theory with Information Theory for Multi-access," *IEEE Journal on Sel. Areas in Comm.*, Vol. 13, No. 6, pp. 963–969, Aug. 1995.

[2] D. Tse, *Variable-rate Lossy Compression and its Effects on Communication Networks*, PhD Thesis, MIT, Cambridge, MA 02139, Sep. 1994.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Capacity of PPM on Gaussian and Webb Channels*

Sam Dolinar, Dariush Divsalar, Jon Hamkins, and Fabrizio Pollara
Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA
e-mail: {sam,dariush,hamkins,fabrizio}@shannon.jpl.nasa.gov

Abstract — **We compare the capacities of M-ary pulse position modulation (PPM) on Gaussian and Webb channels, which are often used to model optical channels with avalanche photodiode (APD) detectors. Both types of channels exhibit the same brickwall thresholds on minimum signal-to-noise ratio per information bit (bit-SNR) for different values of M.**

Consider a symmetric channel with input signals $\mathbf{x}$ restricted to an M-ary orthogonal constellation (such as PPM) and no restriction on the channel outputs $\mathbf{y}$. The maximum mutual information between $\mathbf{x}$ and $\mathbf{y}$ is achieved with an equiprobable distribution on the inputs, and the channel capacity can be evaluated as

$$C = \log_2 M - E_{\mathbf{v}|\mathbf{x}_1} \log_2 \sum_{j=1}^{M} \frac{p(\mathbf{v}|\mathbf{x}_j)}{p(\mathbf{v}|\mathbf{x}_1)} \tag{1}$$

where $\mathbf{v}$ is any random vector obtained from $\mathbf{y}$ via an invertible transformation.

For a standard additive white Gaussian noise channel (AWGN-1), the components of the channel output vector $\mathbf{y}$, given one of the orthogonal inputs $\mathbf{x}_j$, are conditionally independent Gaussian random variables, identically distributed except for y_j: y_i is $N(0, \sigma^2)$, $i \neq j$, and y_j is $N(m, \sigma^2)$. The capacity is evaluated from (1), using $v_j \triangleq y_j/\sigma$ and $\rho \triangleq m^2/\sigma^2$:

$$C(\rho) = \log_2 M - E_{\mathbf{v}|\mathbf{x}_1} \log_2 \sum_{j=1}^{M} \exp\left[\sqrt{\rho}(v_j - v_1)\right] \tag{2}$$

A "double" AWGN channel (AWGN-2) adds greater noise to the orthogonal component in the direction of the signal. The components of the channel output $\mathbf{y}$, given one of the orthogonal inputs $\mathbf{x}_j$, are conditionally independent Gaussian random variables, identically distributed except for y_j: y_i is $N(m_0, \sigma_0^2)$, $i \neq j$, and y_j is $N(m_1, \sigma_1^2)$, with $m_1 > m_0$ and $\sigma_1 > \sigma_0$. The capacity evaluated from (1) is

$$C(\rho, \gamma) = \log_2 M - E_{\mathbf{v}|\mathbf{x}_1} \log_2 \sum_{j=1}^{M} \exp\left[\gamma\sqrt{\rho}(v_j - v_1) + (1-\gamma)(v_j^2 - v_1^2)/2\right] \tag{3}$$

where the (conditional) statistics of $v_j \triangleq (y_j - m_0)/\sigma_0$, and hence the capacity, depend on two parameters $\rho \triangleq (m_1 - m_0)^2/\sigma_0^2$ and $\gamma \triangleq \sigma_0^2/\sigma_1^2 < 1$, rather than on four parameters $m_0, \sigma_0, m_1, \sigma_1$.

An optical channel with APD detectors can be modeled as a "double" Webb channel (Webb-2), plus additional Gaussian thermal noise [1]. A Webb random variable $W(m, \sigma^2, \delta^2) = m + w\sigma$ is a scaled-and-translated version of a standardized Webb random variable $w \triangleq W(0, 1, \delta^2)$ having probability density $p(w; \delta^2) = \frac{1}{\sqrt{2\pi}}(1 + w/\delta)^{-3/2} e^{-w^2/2(1+w/\delta)}$, $w > -\delta$. For a pure Webb-2 channel, the components of the channel output $\mathbf{y}$, given one of the orthogonal inputs $\mathbf{x}_j$, are conditionally independent Webb random variables, identically distributed except for y_j: y_i is $W(m_0, \sigma_0^2, \delta_0^2)$, $i \neq j$, and y_j is $W(m_1, \sigma_1^2, \delta_1^2)$, with $m_1 > m_0$, $\sigma_1 > \sigma_0$, and $\delta_1 > \delta_0$. The optical APD channel model imposes an additional interrelationship $\gamma = \delta_0^2/\delta_1^2$. The capacity is then evaluated from (1) in terms of $\Delta \triangleq \delta_1^2 - \delta_0^2$ as

$$C(\rho, \gamma, \Delta) = \log_2 M - E_{\mathbf{v}|\mathbf{x}_1} \log_2 \sum_{j=1}^{M} \frac{p\left(\sqrt{\gamma}(v_j - \sqrt{\rho}); \frac{\Delta}{1-\gamma}\right) p(v_1; \frac{\gamma\Delta}{1-\gamma})}{p\left(\sqrt{\gamma}(v_1 - \sqrt{\rho}); \frac{\Delta}{1-\gamma}\right) p(v_j; \frac{\gamma\Delta}{1-\gamma})} \tag{4}$$

where v_j, ρ, and γ have the same definitions (in terms of the Webb-2 channel variables) as for the AWGN-2 model.

We evaluated the M-dimensional expectations in (2), (3), and (4) accurately via Monte Carlo simulation. Some results are plotted in Fig. 1 for the AWGN-1 and Webb-2 channels for different PPM orders M. The abscissa in this figure is a normalized bit-SNR, $\rho_b \triangleq \rho/(2C)$. Along each Webb-2 curve, the two independent variables held constant are $\Delta = 60.8$ and $\rho\gamma/(1-\gamma) = 17.6$, which correspond to a representative optical APD problem with $\eta n_s = 38$ detected signal photons per PPM word and an excess noise factor $F = 2.16$. The Webb-2 capacity curves for each M exhibit the same brickwall thresholds on minimum ρ_b as the AWGN-1 capacity curves. For different M, these thresholds are offset from each other by a factor $M/(M-1)$, representing the penalty for using orthogonal signals instead of a simplex signal set. In the limit as $M \to \infty$, the minimum ρ_b approaches (for both AWGN-1 and Webb-2) the well-known bit-SNR threshold of -1.59 dB for a standard AWGN channel with no restriction on the channel inputs.

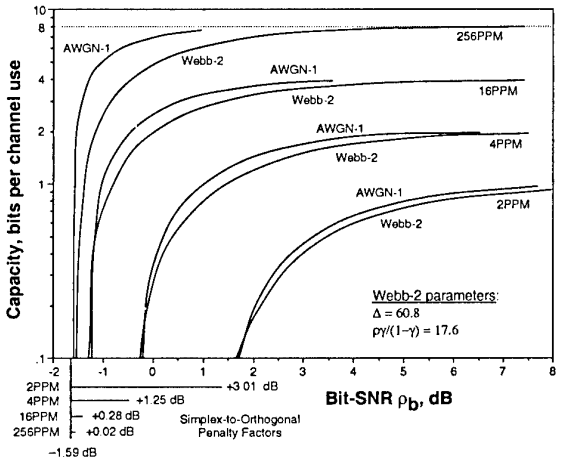


Fig. 1: Capacity of M-ary PPM on AWGN-1 and Webb-2 channels.

*This work was funded by the TMOD Technology Program and performed at the Jet Propulsion Laboratory, California Institute of Technology under contract with the National Aeronautics and Space Administration.

Reference

[1] P. P. Webb, R. J. McIntyre and J. Conradi, "Properties of Avalanche Photodiodes," RCA Review, vol. 35, June, 1974, pp. 234-278.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Capacity of multiple-antenna Rayleigh channel with a limited transmit diversity

Alexei Gorokhov
Philips Research Laboratories DSP Group WY-8.58
Prof. Holstlaan 4 5656 AA Eindhoven The Netherlands
Email: Alexei.Gorokhov@philips.com

Abstract — **The capacity of a wireless link is studied when multiple transmit and receive antennas are used. Under the assumption of a narrow-band link and a rich scattering environment, the propagation medium is modeled as a Rayleigh flat fading with a good receive diversity. By contrast to the previous works, the assumption of decorrelated transmit antennas is relaxed. This enables a study of some common scenarios where the transmit antennas occupy a limited volume. For an arbitrary correlation between the transmitting antennas, tight capacity bounds are calculated and an optimal signaling scheme is derived.**

I. Introduction

Recently, Foschini *et al.* studied the capacity of a narrow-band wireless link between multiple transmit and receive antennas and nearly optimal transmission schemes when the propagation channel is assumed Rayleigh and flat with *i.i.d.* coefficients [1]. Such a modeling is rather inaccurate when multiple transmit antennas occupy a limited volume which is situated far away from the receive antennas. The independence condition is relaxed here so that the channels corresponding to different transmit antennas may exhibit an arbitrary correlation. A tight lower bound of channel capacity, presented in this work, yields an optimal transmission scheme. This bound shows that a limited transmit volume is characterized by a limited capacity; this capacity may be achieved with a finite number of transmit antennas when the received signal is due to a local scattering in the receiver vicinity.

II. Main results

Consider a flat fading channel between m transmitting and M receiving antennas such that

$$\boldsymbol{x}_t = \boldsymbol{H}\,\boldsymbol{s}_t + \boldsymbol{n}_t, \qquad t \in \mathbb{R}, \tag{1}$$

where $\boldsymbol{s}_t$ is the $m \times 1$ vector of the transmit antenna outputs, $\boldsymbol{x}_t$ is the $M \times 1$ vector of the received signals, $\boldsymbol{H}$ is the $M \times m$ channel matrix and $\boldsymbol{n}_t$ is the $M \times 1$ vector of the AWGN. Assume that each entry of $\boldsymbol{s}_t$ is an *i.i.d.* series and that these entries may be mutually correlated with fixed total power: $\mathbb{E}\{\boldsymbol{s}_t\,\boldsymbol{s}_t^H\} = \sigma_s^2\,\boldsymbol{C}$, $\mathrm{tr}\,(\,\boldsymbol{C}\,) = 1$. Define $\varrho^2 = (\sigma_s^2/\sigma^2)$ the signal-to-noise ratio (SNR). According to [2], the channel capacity (in bits per second per hertz) is given by

$$C = \log_2 \det\,(\,\mathrm{I}_M + \varrho^2\,\boldsymbol{H}\,\boldsymbol{C}\,\boldsymbol{H}^H\,)\,. \tag{2}$$

The Rayleigh channel model is assumed so that the elements of $\boldsymbol{H}$ are jointly complex circular Gaussian. Assume arbitrary correlations of the transmit antennas specified by a normalized correlation matrix $\boldsymbol{R}_T = \mathbb{E}\{\boldsymbol{H}_{k,:}^T\,\overline{\boldsymbol{H}_{k,:}}\}$, $1 \le k \le m$ whereas the received antennas are decorrelated (*i.e.*, $\boldsymbol{R}_R = \mathbb{E}\{\boldsymbol{H}_{:,l}\boldsymbol{H}_{:,l}^H\} = \mathrm{I}_M$, $1 \le l \le M$). To introduce the core result, we define the eigendecomposition $\{\boldsymbol{U}, \boldsymbol{\Lambda}^2\}$ of $\boldsymbol{R}_T^{\frac{1}{2}}\boldsymbol{C}\boldsymbol{R}_T^{\frac{1}{2}}$ such that $\boldsymbol{R}_T^{\frac{1}{2}}\boldsymbol{C}\boldsymbol{R}_T^{\frac{1}{2}} = \boldsymbol{U}\boldsymbol{\Lambda}^2\boldsymbol{U}^H$ with a diagonal $\boldsymbol{\Lambda} = \mathrm{diag}\{\boldsymbol{\Lambda}_k\}_{k=1}^m$ and a unitary $\boldsymbol{U}$. Then the capacity in (2) admits an accurate lower-bound $C_* \le C$ such that

$$C_* = \sum_{k=1}^{m} \log_2\left(1 + \varrho^2\boldsymbol{\Lambda}_k^2\;\chi_{M-k+1}^2\right), \quad \boldsymbol{\Lambda}_1 \ge \ldots \ge \boldsymbol{\Lambda}_m. \tag{3}$$

where the random quantities χ_{M-k+1}^2 are Gamma distributed with $(M-k+1)$ degrees of freedom. This bound is shown to be tight at high and moderate SNR and big M. The bound in [1] is a particular case of (3) when $\boldsymbol{R}_T = \mathrm{I}_m$ and $\boldsymbol{C} = (1/m)\,\mathrm{I}_m$.

The optimal signaling is derived that maximizes the approximate expected value of the capacity in (3). An accurate approximation is due to Jensen's inequality: $\mathbb{E}\{C_*\} \le C_\infty$,

$$C_\infty = \sum_{k=1}^{m} \log_2\left(1 + \varrho^2\boldsymbol{\Lambda}_k^2(M+1-k)\right), \quad \boldsymbol{\Lambda}_1 \ge \ldots \ge \boldsymbol{\Lambda}_m. \tag{4}$$

The capacity C_* is also shown converging in probability to C_∞ when M and m are big. This capacity may be reached when $\boldsymbol{C}$ has the eigenbasis $\boldsymbol{U}$ with the eigenvalues that obey the *water pouring* distribution for a given set $\{\varrho^2\boldsymbol{\Lambda}_k^2(M+1-k)\}_{k=1}^m$.

III. Numerical example

Consider a WLAN scenario in the 5.2GHz band; 6 transmit and 8 receive linear antenna arrays of size 30cm are separated by 30m. Major scatterers are uniformly distributed in the receiver vicinity. In Fig.1, solid lines show the empirical capacity obtained from 10000 random trials of a physical propagation model that assumes free space path loss. The empirical capacity driven by a stochastic model (specified by $\boldsymbol{R}_T$), its stochastic bound C_* and the deterministic approximation C_∞ are depicted by dashed lines, dash-dotted and vertical lines correspondingly, for optimal (water pouring) and uniform power loading. The "*i.i.d.* bound" stands for the capacity predicted by [1], under the assumption $\boldsymbol{R}_T = \mathrm{I}_m$.

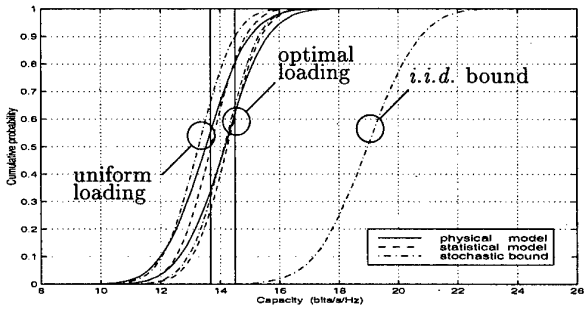


Fig.1. Cumulative probability of the capacity: $M = 8$, $m = 6$, $\varrho^2 = 10$dB.

References

[1] G.J. Foschini and M.J. Gans, "On limits of wireless communications in a fading environment when using multiple antennas", *Wireless Pers. Comm.*, vol. 6, No. 3, pp. 311–335, March 1998.

[2] E. Telatar, "Capacity of multiantenna Gaussian channels", *AT&T-Bell Lab. Internal Tech. Memo.*, June 1995.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Channel Capacity in Evenly Correlated Rayleigh Fading with Different Adaptive Transmission Schemes and Maximal Ratio Combining

Ranjan K. Mallik
Department of Electrical Engineering
Indian Institute of Technology, Delhi
Hauz Khas, New Delhi 110016, India
e-mail: rkmallik@ee.iitd.ernet.in

Moe Z. Win
Wireless Systems Research Department
AT&T Labs - Research, NSL 4-147
100 Schulz Drive, Red Bank, NJ 07701-7033, U.S.A.
e-mail: win@research.att.com

Abstract — **We present closed-form expressions for the single-user capacity over slow nonselective correlated Rayleigh fading channels having equal branch powers and the same correlation between any pair of branches. Maximal ratio combining (MRC) is used and three adaptive transmission schemes are analyzed: (1) optimal simultaneous power and rate adaptation, (2) optimal rate adaptation with constant transmit power, (3) channel inversion with fixed rate.**

I. Introduction

Consider the coherent reception of some digitally modulated signal with L diversity branches and predetection MRC. Let γ_i, $i = 1, \ldots, L$, denote the instantaneous signal-to-noise ratio (SNR) of the ith diversity branch. The random variables $\sqrt{\gamma_1}, \ldots, \sqrt{\gamma_L}$ are identically distributed, each having a marginal distribution which is Rayleigh with second moment $2\sigma^2$ ($\sigma > 0$); the covariance between any pair γ_i, γ_j, $i \neq j$, is $4\rho^2\sigma^4$ ($0 < \rho < 1$), and therefore the *correlation coefficient* between γ_i and γ_j is ρ^2. Such a correlation model is appropriate when we use space diversity with closely packed diversity antennas. The total instantaneous received SNR using MRC is given by $\gamma = \sum_{i=1}^{L} \gamma_i$. Denoting $a = \frac{1}{2\sigma^2(1+[L-1]\rho)}$, $b = \frac{1}{2\sigma^2(1-\rho)}$, we obtain from the charactersitic function of γ the following expression for its probability density function:

$$f_\gamma(v) = ab^{L-1}\left[\frac{e^{-av}}{(b-a)^{L-1}} - e^{-bv}\sum_{k=1}^{L-1}\frac{v^{k-1}}{(b-a)^{L-k}(k-1)!}\right], \quad v \geq 0.$$

The case of i.i.d. branches ($\rho = 0$) has been analyzed in [1].

II. Channel Capacity

Under the condition of *optimal simultaneous power and rate adaptation*, the channel capacity C_{opra} (in bits/sec) is given by [2] [1] $C_{opra} = \frac{B}{\ln 2}\int_{\gamma_0}^{\infty} \ln\left(\frac{v}{\gamma_0}\right) f_\gamma(v)\, dv$, where B (in Hz) is the channel bandwidth and γ_0 is the optimal cutoff SNR satisfying $\int_{\gamma_0}^{\infty}\left(\frac{1}{\gamma_0} - \frac{1}{v}\right) f_\gamma(v)\, dv = 1$.

Denoting the *exponential integral of order one* by $E_1(c) = \int_1^\infty \frac{e^{-cv}}{v}\, dv$, $c \geq 0$, and the *Poisson distribution* by $P_k(c) = e^{-c}\sum_{n=0}^{k-1}\frac{c^n}{n!}$, we get the following closed-form expression for the capacity per unit bandwidth (in bits/sec/Hz):

$$\frac{C_{opra}}{B} = \frac{1}{\ln 2}\left[E_1(a\gamma_0)\left(\frac{b}{b-a}\right)^{L-1} - E_1(b\gamma_0)\left\{\left(\frac{b}{b-a}\right)^{L-1} - 1\right\} + \sum_{n=1}^{L-2}\frac{P_n(b\gamma_0)}{n}\left\{\left(\frac{b}{b-a}\right)^{L-n-1} - 1\right\}\right].$$

Since the transmission in suspended when $\gamma < \gamma_0$, there is an outage probability which is given by

$$P_{out} = 1 - \left(\frac{b}{b-a}\right)^{L-1} e^{-a\gamma_0} + \frac{a}{b}\sum_{k=1}^{L-1}\left(\frac{b}{b-a}\right)^{L-k} P_k(b\gamma_0). \quad (1)$$

In the case of *optimal rate adaptation with constant transmit power*, the channel capacity is given by [3] [2] [1] $C_{ora} = \frac{B}{\ln 2}\int_0^\infty \ln(1+v)\, f_\gamma(v)\, dv$, which yields the following expression for the capacity per unit bandwidth:

$$\frac{C_{ora}}{B} = \frac{1}{\ln 2}\left[\left(\frac{b}{b-a}\right)^{L-1} e^a E_1(a) - \frac{a}{b}\sum_{k=1}^{L-1}\left(\frac{b}{b-a}\right)^{L-k} \times \left\{P_k(-b)E_1(b) + \sum_{m=1}^{k-1}\frac{1}{m}P_m(b)P_{k-m}(-b)\right\}\right].$$

In the case of *channel inversion with fixed rate*, there are two schemes: *truncated* channel inversion with fixed rate, and channel inversion with fixed rate *without truncation*. With the truncation scheme, the channel capacity per unit bandwidth is expressed as [1]

$$\frac{C_{tifr}}{B} = \frac{1}{\ln 2}\ln\left(1 + \frac{1}{\int_{\gamma_0}^\infty \frac{1}{v} f_\gamma(v)\, dv}\right)(1 - P_{out}), \quad (2)$$

where P_{out} is given by (1). The cutoff level γ_0 can be chosen either to achieve a specific outage probability P_{out}, or to maximize (2). A closed-form expression for the capacity can be obtained from (2). If we set $\gamma_0 = 0$ in (2), we get $\frac{C_{cifr}}{B}$, the capacity for channel inversion with fixed rate and without truncation. In this case, $P_{out} = 0$.

III. Numerical Results

From plots of the channel capacity per unit bandwidth, we find that the capacity increases with increase of diversity order L and increase of average received SNR per branch $\mathbf{E}[\gamma_i] = 2\sigma^2$, as expected. While the capacities C_{ora}/B, C_{cifr}/B and C_{tifr}/B decrease with increase of ρ, the capacity C_{opra}/B increases sharply with ρ for small positive values of ρ, reaches a maximum, and then decreases as ρ increases further. It is also to be noted that the decrease in capacity with increase in ρ is much sharper in the case of optimal power and rate adaptation as compared to the other schemes. In the case of truncated channel inversion, the cuoff SNR γ_0 which maximizes the capacity decreases with increase of ρ. A comparison of the plots for the different schemes shows that for the same channel bandwidth B, $C_{opra} > C_{ora} > C_{tifr} > C_{cifr}$.

References

[1] M.-S. Alouini and A. J. Goldsmith, "Capacity of Rayleigh fading channels under different adaptive transmission and diversity-combining techniques," *IEEE Transactions on Vehicular Technology*, vol. 48, no. 4, pp. 1165–1181, July 1999.

[2] A. J. Goldsmith and P. P. Varaiya, "Capacity of fading channels with channel side information," *IEEE Transactions on Information Theory*, vol. 43, no. 6, pp. 1986–1992, November 1997.

[3] C. G. Günther, "Comment on: Estimate of channel capacity in Rayleigh fading environment [by W. Y. C. Lee, IEEE T-VT, vol. 39, no. 3, pp. 187–189, August 1990]," *IEEE Transactions on Vehicular Technology*, vol. 45, no. 2, pp. 401–403, May 1996.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Capacity of nearly-decomposable Markovian fading channels under asymmetric receiver-sender side information

Muriel Médard
MIT
e-mail: medard@mit.edu

R. Srikant
University of Illinois
e-mail: rsrikant@uiuc.edu

Abstract — **In modeling wireless channels, slow and fast fades are generally decoupled. We show that the difference between true capacity and that obtained assuming independence of fast and slow channel fades is $O(\epsilon log(\epsilon) log(-\epsilon log(\epsilon)))$, where ϵ is the ratio between the average duration of fast and slow fades.**

Our purpose in this work is to explicitly take into account, in the capacity computation for time-varying fading channels, the fact that slow fades and fast fades are not truly decoupled. Decoupling slow fades from fast fades has generally been used as a first-order approximation. We consider the case where the sender channel side information (SCSI) is a coarse representation of the receiver channel side information (RCSI). In many circumstances, RCSI and SCSI are asymmetric, although related. In particular, when the channel is rapidly varying, providing full feedback from the receiver to the sender may be onerous and inefficient. Recent work in this area has considered the case where the SCSI is a deterministic function of the RCSI [1]. In [1], exact capacity results are given for the case when the SCSI remains Markov. If the SCSI and the RCSI can indeed be decoupled, in such a way that both remain Markov, then the results of [1] apply directly.

We consider a discrete-time finite-state Markov channel (FSMC). The RCSI, which we term the micro states, is a full description of the FSMC. The SCSI, which we term the macro states, is a coarser representation of the states: the sender only knows that the current state is within one of a set of states. The macro states represent the long-term behavior of the channel, i.e. the slow fades. Note that fades are possible while we are in the good macro state and, conversely, energy surges are possible while we are in the bad macro state. Although the model of [1] does not apply, we suspect that, as the spread between the speed of the slow fades and that of the fast fades grows, the results of [1] should become an increasingly good approximation to the true capacity. Our results support this intuition and quantify the effect of the spread between the speed of the slow fades and that of the fast fades. However, our results also show that convergence is very slow.

We consider a nearly decomposable model ([2]) for our FSMC. Consider a discrete-time Markovian fading process defined by the stochastic matrix $A + \epsilon B$, where A is block-diagonal with M blocks and the i^{th} block (which is also a stochastic matrix) is denoted by A_i. We call the set of fading states associated with the i^{th} block a macro state and denote it by S_i. We assume the RCSI is the current micro state of the channel whereas the SCSI is the current macro state. Let $\pi^{(i)}$ be the stationary probability vector associated with A_i, i.e., $\pi^{(i)} A_i = \pi^{(i)}$. Define an $M \times M$ matrix P as follows: the (i,j) entry of P is given by $P_{ij} = \sum_{k \in S_i} \sum_{l \in S_j} \pi_k^{(i)} B^{kl}, \quad i \neq j,$ and $P_{ii} = 1 - \sum_{j \neq i} P_{ij}$. Note that P is also a stochastic matrix and let p be its stationary probability vector, i.e., $p = pP$. We can interpret P as being the long-term transition probabilities among macro-states and p_i as approximating the long-term probability of being in S_i, i.e., $p_i(\epsilon) = p_i + O(\epsilon)$, where $p_i(\epsilon)$ is the actual probability of being in micro-state i.

Let $T(n)$ denote the random variable corresponding to the micro-state at time n and define $S(n)$ to be random variable corresponding to the macro-state at time n. The sample values of $T(n)$ is denoted by $t(n)$. Further, let $\sqrt{G(T(n))}$ be the random variable corresponding to the signal attenuation at time n. The received signal at time n is given by the random variable $Y(n) = \sqrt{G(T(n))} X(n) + W(n)$, where $X(n)$ is the transmitted signal and $W(n)$ is AWGN with variance σ^2. Our coding theorem follows.

Theorem 1 *Define*

$$C := \max_{\{P(i)\}} \frac{1}{2} \sum_{i=1}^{M} p_i \sum_{t \in \mathcal{M}_i} \log\left(1 + \frac{P(i)G(t)}{\sigma^2}\right) \pi_t^{(i)} \text{ subject}$$

to $\sum_{i=1}^{M} p_i(\epsilon) P(i) \leq \mathcal{P}$, *where* $\mathcal{P}$ *is the power constraint on the sender.*

Given $R < C$ *and* $\delta > 0$, *we can find an* $\epsilon^*(R)$ *and* $n(\delta)$ *such that for all* $\epsilon < \epsilon^*$, *there exists a* $(n/\epsilon, 2^{nR/\epsilon})$ *code whose maximal probability of error is less than* δ. *(Note that* ϵ^* *is independent of* δ.*)*

Define $C_{true}(\epsilon) = \lim_{n \to \infty} \frac{1}{n} \max_{p(x^n|s^n)} I(X^n; \{Y^n, T^n\})$, *where* $p(x^k|s^n) = p(x^k|s^k)$, *for all* $k \leq n$. *Then,* $C_{true}(\epsilon) = C + O(\epsilon \log(\epsilon) log(-\epsilon \log(\epsilon)))$.

Suppose for some $R > 0$, *we have the following property: for every* $\delta > 0$, *we can find* $\epsilon^*(R)$ *and* $n(\delta)$ *such that for all* $\epsilon < \epsilon^*$, *there exists a* $(n/\epsilon, 2^{nR/\epsilon})$ *code whose maximal probability of error is less than* δ. *Then,* $R < C$.

References

[1] G. Caire, S. Shamai, "On the Capacity of Some Channels with Channel State Information", *IEEE Transactions on Information Theory*, September 1999, vol. 45, no. 6, pp. 2007–2020.

[2] R.G. Phillips, P.V. Kokotovic, "A Singular Perturbation Approach to Modeling and Control of Markov Chains", *IEEE Transactions on Automatic Control*, vol. AC-26, no. 5, October 1981, pp. .

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Rényi Information Divergence via Measure Transformations on Minimal Spanning Trees

Alfred O. Hero[1]
Dept. EECS
University of Michigan
1301 Beal Avenue
Ann Arbor, MI 48109-2122 USA
hero@eecs.umich.edu

Olivier J.J. Michel
Laboratoire de Physique,
URA-1325 CNRS,
École Normale Supérieure de Lyon,
46 allée d'Italie,
69364 Lyon Cedex 07, France
omichel@physique.ens-lyon.fr

Abstract — **We apply the results of [2] to estimation of Rényi I-divergence between an unknown distribution and a known reference distribution using power weighted pruned minimal graphs spanning a random sample of n points from the unknown distribution. In particular we establish that the weight of a minimal graph connecting the points converges a.s. in n to the I-divergence after a suitable change of measure.**

I. Introduction

Let $\mathcal{X}_n = \{x_1, x_2, \ldots, x_n\}$ denote a sample of i.i.d. data points in R^d having unknown Lebesgue multivariate density $f(x)$ supported on $[0,1]^d$. Define the order ν Rényi I-divergence [1] with respect to a dominating reference density $f_o(x)$

$$I_\nu(f, f_o) = \frac{1}{\nu - 1} \ln \int \left(\frac{f(x)}{f_o(x)}\right)^\nu f_o(x) dx \qquad (1)$$

The I-divergence takes on its minimum value (equals zero) if and only if $f = f_o$ (a.e.). $I_\nu(f, f_o)$ reduces to the Rényi entropy $H_\nu(f)$ when f_o is equal to a uniform density over $[0,1]^d$. Special cases of interest are obtained for $\nu = \frac{1}{2}$ for which one obtains the log Hellinger distance squared and for $\nu \to 1$ for which one obtains the Kullback-Liebler divergence.

II. MST's and Entropy Estimation

A spanning tree $\mathcal{T}$ through the sample $\mathcal{X}_n$ is a connected acyclic graph which passes through all the n points $\{x_i\}_i$ in the sample. $\mathcal{T}$ is specified by an ordered list of edge (Euclidean) lengths e_{ij} connecting certain pairs (x_i, x_j), $i \neq j$, along with a list of edge adjacency relations. The power weighted length of the tree $\mathcal{T}$ is the sum of all edge lengths raised to a power $\gamma \in (0, d)$, denoted by: $\sum_{e \in \mathcal{T}} |e|^\gamma$. The minimal spanning tree (MST) is the tree which has the minimal length $L(\mathcal{X}_n) = \min_{\mathcal{T}} \sum_{e \in \mathcal{T}} |e|^\gamma$. For any subset $\mathcal{X}_{n,k}$ of k points in $\mathcal{X}_n$ define $\mathcal{T}_{\mathcal{X}_{n,k}}$ the k-point MST which spans $\mathcal{X}_{n,k}$. The k-MST is defined as that k-point MST which has minimum length. Thus the k-MST spans the densest k-dimensional subset $\mathcal{X}^*_{n,k}$ of $\mathcal{X}_n$. The k-MST computation is NP complete. In [2] we presented asymptotic results for a d-dimensional extension of the planar k-MST approximation of Ravi et al, called the greedy k-MST approximation, which runs in polynomial time.

Let $\nu \in (0,1)$ be defined by $\nu = (d-\gamma)/d$ and define the statistic

$$\hat{H}_\nu(\mathcal{X}^*_{n,k}) = \frac{1}{1-\nu} \ln \left(n^{-\nu} L(\mathcal{X}^*_{n,k})\right) + \beta(\nu, d) \qquad (2)$$

where β is a constant equal to the ν-th order Rényi entropy of the uniform density on $[0,1]^d$. Let $G(x)$ be the coordinate transformation on $[0,1]^d$ which maps the reference distribution f_o to a uniform distribution and define the transformed data sample $\mathcal{Y}_n = G(\mathcal{X}_n)$. Then using the results of [2] it can be shown that $\hat{H}_\nu(\mathcal{Y}^*_{n,n})$ is an a.s. consistent estimator of the I-divergence (1). Furthermore, with $\alpha = k/n$, $\hat{H}_\nu(\mathcal{Y}^*_{n,k})$ is an α-trimmed estimator of I-divergence in the sense that

$$\hat{H}_\nu(\mathcal{Y}^*_{n,k}) \to \min_{A: P(A) \geq \alpha} \frac{1}{1-\nu} \ln \int_A \left(\frac{f(x)}{f_o(x)}\right)^\nu f_o(x) dx \quad (a.s.) \quad (3)$$

where the minimization is performed over all d-dimensional Borel subsets of $[0,1]^d$ having probability $P(A) = \int_A f_o(x) dx \geq \alpha$.

Let f follow the mixture model

$$f = (1 - \epsilon) f_1 + \epsilon f_o, \qquad (4)$$

where f_o is a known outlier density and f_1, $\epsilon \in [0,1]$ are unknown. Then for small ϵ and α close to one it can easily be shown that the right hand side of (3), which is $I_\nu(f, f_o)$, is to a close approximation $I_\nu(f_1, f_o)$. Thus $\hat{H}_\nu(\mathcal{Y}^*_{n,k})$ is a robust estimator of $I_\nu(f_1, f_o)$.

Note the following: the estimator $\hat{H}_\nu(\mathcal{Y}^*_{n,k})$ does not require performing the difficult step of density estimation; estimates of various orders ν of I_ν can be obtained by varying the edge power exponent; the sequence of trees $\mathcal{Y}_{n,2}, \ldots \mathcal{Y}_{n,n} = \mathcal{Y}_n$ provides a natural extension of rank order statistics for multidimensional data. Here k plays the same role as the parameter α in the α-trimmed mean estimator for 1-dimensional data.

[1] This research was supported in part by AFOSR under MURI grant F49620-97-0028.

References

[1] M. Basseville, "Distance measures for signal processing and pattern recognition," *Signal Processing*, vol. 18, pp. 349–369, 1989.

[2] A. Hero and O. Michel, "Asymptotic theory of greedy approximations to minimal k-point random graphs," *IEEE Trans. on Inform. Theory*, vol. IT-45, no. 6, pp. 1921–1939, Sept. 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On the Interpretation of the APP Algorithm as an LLR Filter

Ingmar Land and Peter Hoeher
Information and Coding Theory Lab
University of Kiel
Kaiserstr. 2, D-24143 Kiel, Germany
e-mail: {il,ph}@techfak.uni-kiel.de

Ulrich Sorger
Institute for Communications Technology
Darmstadt University of Technology
Merckstr. 25, D-64283 Darmstadt, Germany
e-mail: uli@nesi.tu-darmstadt.de

Abstract — **A channel decoder employing the a posteriori probability (APP) algorithm can be formulated so that its inputs and its outputs are log-likelihood-ratios (LLR): channel LLRs of the code bits are accepted, and a posteriori LLRs of the info bits and/or the code bits are delivered. Since decoding improves the reliability, the APP algorithm can be interpreted as a non-linear filter for LLRs. The "LLR amplification" depends on the distance properties of the channel code; for high signal-to-noise ratios it is dominated by the minimum distance.**

Summary

The APP algorithm [1] accepts a priori probabilities and channel probabilities as inputs and delivers a posteriori probabilities as outputs. With additional computation of soft outputs for the code bits [2][3] and with usage of LLRs instead of probabilities [4], it can be extended to the logarithmic APP (LogAPP).

Consider a binary linear convolutional encoder of rate $R = k/n$. Let $\boldsymbol{e}$ denote the path through the trellis associated with the info word $\boldsymbol{u}(\boldsymbol{e})$ and the code word $\boldsymbol{x}(\boldsymbol{e})$, $u, x \in \{+1, -1\}$. The code bits are transmitted over a memoryless channel; the received value of a single bit is denoted by y, and the received word is denoted by $\boldsymbol{y}$.

The LogAPP algorithm takes the a priori LLRs of the info bits U and the channel LLRs of the code bits X,

$$L^-(U) \triangleq \ln \frac{P(U=+1)}{P(U=-1)}, \quad L^-(X) \triangleq \ln \frac{P(X=+1|y)}{P(X=-1|y)}, \qquad (1)$$

and computes the a posteriori LLRs of the info bits and of the code bits

$$L^+(U) \triangleq \ln \frac{P(U=+1|\boldsymbol{y})}{P(U=-1|\boldsymbol{y})}, \quad L^+(X) \triangleq \ln \frac{P(X=+1|\boldsymbol{y})}{P(X=-1|\boldsymbol{y})}. \qquad (2)$$

These inputs and outputs of the LogAPP algorithm are depicted in Fig. 1. In the following, the info bits are assumed to be equally distributed, i.e. $L^-(U) = 0$.



Fig. 1: The input and the output LLRs of the LogAPP algorithm.

The purpose of decoding is to improve the reliability of the bits. This motivates to interpret decoding as non-linear filtering, as mentioned in [2]. In this paper, the LogAPP is treated as a *non-linear LLR filter*. This point-of-view suggests to define an *info bit LLR amplification* (ILA) and a *code bit LLR amplification* (CLA):

$$\mathrm{ILA} \triangleq \left.\frac{\mathrm{E}_y\, L^+(U)}{\mathrm{E}_y\, L^-(X)}\right|_{L^-(U)}, \quad \mathrm{CLA} \triangleq \left.\frac{\mathrm{E}_y\, L^+(X)}{\mathrm{E}_y\, L^-(X)}\right|_{L^-(U)}, \qquad (3)$$

where E_y denotes the expected value with respect to y. The ILA can be regarded as the transfer function of a *soft-decoder*; since there are less output values than input values, the soft-decoder is similar to a decimator. The CLA can be regarded as the transfer function of a *soft-repeater*, i.e. a device which performs decoding and re-encoding using soft values.

For rate 1/2 convolutional codes with memories 2 to 8, binary transmission over an AWGN channel was simulated. In Fig. 2, the ILA and the CLA are depicted as a function of the mean channel LLR $\mathrm{E}_y\, L^-(X)$ of the code bits. The following characteristics can be justified analytically:

1. For low input LLRs, the ILA approaches 0 and the CLA approaches 1.
2. For high input LLRs, both the ILA and the CLA approach a constant value which can be identified with the free distance of the code.

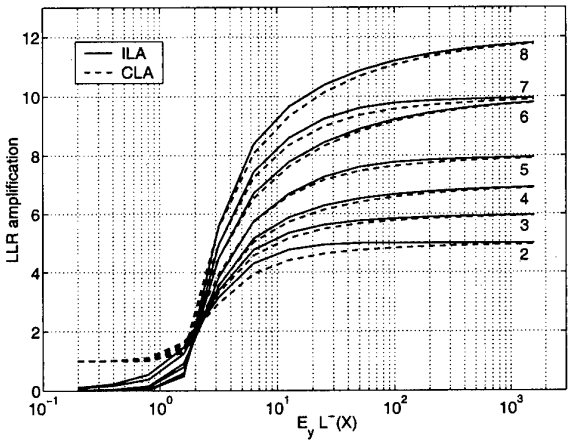


Fig. 2: The LLR amplifications of the convolutional codes with memories 2 to 8.

References

[1] L. R. Bahl, J. Cocke, F. Jelinek, and J. Raviv, "Optimal decoding of linear codes for minimizing symbol error rate," *IEEE Trans. Inform. Theory*, March 1974, pp. 284 – 287.

[2] J. Lodge, R. Young, P. Hoeher, and J. Hagenauer, "Separable MAP "filters" for the decoding of product and concatenated codes," in *IEEE Int. Conf. Commun.*, May 1993, pp. 1740 – 1745.

[3] S. Benedetto, D. Divsalar, G. Montorsi, and F. Pollara, "A soft-input soft-output APP module for iterative decoding of concatenated codes," *IEEE Commun. Letters*, vol. 1, no. 1, January 1997, pp. 22 – 24.

[4] P. Robertson, P. Hoeher, and E. Villebrun, "Optimal and sub-optimal maximum a posteriori algorithms suitable for turbo decoding," *Europ. Trans. Telecommun.*, vol. 8, no. 2, March – April 1997, pp. 119 – 125.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Minimum Bandwidth Basis Functions for the Fourth-Moment Bandwidth Measure [1]

Eric A. Fain
Lockheed Martin MDS
San Jose, CA 95134
Eric.Fain@lmco.com

Mahesh K. Varanasi
ECE Dept., University Of Colorado
Boulder, CO 80309-0425,
varanasi@schof.colorado.edu

Abstract — **We present a fourth-moment measure of the "bandwidth" of a strictly time-limited signal and obtain a minimum-bandwidth basis for $\mathcal{L}^2(a,b)$. Such a basis consists of orthonormal waveforms with the smallest obtainable bandwidths. The primary advantage of the fourth-moment bandwidth relative to the Root Mean Square (RMS) and Fractional Out-of-Band Energy (FOBE) measures is that its basis functions have a $O(1/f^3)$ frequency roll-off compared to the $O(1/f^2)$ and $O(1/f)$ decay of the RMS and FOBE basis functions, respectively.**

I. Main Result

Every strictly time-limited pulse has a spectrum which is non-zero for an infinite range of frequencies. Hence, non-strict measures of bandwidth are used to quantify the spectral concentration of such signals. Two such measures, namely the RMS and the FOBE bandwidths, have been studied in the past. In particular, it was shown that the minimum RMS and FOBE bandwidth orthonormal basis functions for $\mathcal{L}^2(0,T)$ are sinusoids $\sin(k\pi t/T)$ for integer k [1] and the set of time-truncated prolate-spheroidal wave functions [2], respectively. In this paper we consider the fourth-moment bandwidth and obtain the corresponding minimum bandwidth orthonormal basis.

Definition 1 (Fourth-Moment Bandwidth Measure) *For a baseband signal with energy spectrum $S_x(f)$, the fourth-moment bandwidth is defined as*

$$\mathrm{bw}(x) = \left[\frac{\int_{-\infty}^{\infty} f^4 S_x(f)\,df}{\int_{-\infty}^{\infty} S_x(f)\,df}\right]^{1/4} \tag{1}$$

Definition 2 (Minimum-Bandwidth Basis) *Let the collection of functions $\mathcal{B} = \{\psi_i\}_{i=1}^{\infty}$ be an orthonormal basis for $\mathcal{L}^2(-T/2,T/2)$ (the space of square-integrable functions with standard inner product), and let the bandwidth measure be defined through (1). If ψ_k has the minimum bandwidth of all $\mathcal{L}^2$ functions which are orthogonal to $\{\psi_i\}_{i=1}^{k-1}$, i.e.,*

$$\psi_k = \arg \min_{\substack{x\in\mathcal{L}^2(-\frac{T}{2},\frac{T}{2}) \\ x\perp\psi_1,\cdots,\psi_{k-1}}} \mathrm{bw}(x) \tag{2}$$

for all k, then $\mathcal{B}$ is a minimum-bandwidth basis *for $\mathcal{L}^2(-T/2,T/2)$.*

The main result of this paper is that the minimum bandwidth basis functions for the fourth-moment bandwidth measure are solutions of the eigenvalue/eigenfunction equation

$$\gamma\psi(t) = \frac{1}{16\pi^4}\left(\mathbf{T}^*\left(\frac{d^4}{dt^4}(\mathbf{T}\psi)\right)\right)(t) \tag{3}$$

where $\mathbf{T}$ denotes the time-limiting operator (to the interval $[-T/2,T/2]$). The boundary conditions are imposed by requiring the solutions to lie in $\mathcal{H}_0^2(-T/2,T/2)$ which are the time-limited elements of the Sobolev space $\mathcal{W}^2$ of functions on R defined as [3],

$$\mathcal{W}^2 = \left\{x : \left\|(1+f^2)\hat{x}(f)\right\|_2 < \infty\right\}. \tag{4}$$

It can be shown that the eigenvalues γ_k of (3), which are equal to the bandwidths of the respective basis functions, are given as $\gamma_k = (\phi_k/2\pi)^4$, where the ϕ_k's are the positive solutions to

$$\cos(\phi_k T/2)\sinh(\phi_k T/2) + \sin(\phi_k T/2)\cosh(\phi_k T/2) = 0 \tag{5}$$

and

$$\cos(\phi_k T/2)\sinh(\phi_k T/2) - \sin(\phi_k T/2)\cosh(\phi_k T/2) = 0 \tag{6}$$

The eigenfunctions are given for $t \in [-T/2,T/2]$ by

$$\psi_k(t) = \begin{cases} \sqrt{\frac{2}{T(1+\alpha_k^2)}}\left(\cos(\phi_k t) + \alpha_k\cosh(\phi_k t)\right) & k, \text{ odd} \\ \sqrt{\frac{2}{T(1+\alpha_k^2)}}\left(\sin(\phi_k t) + \alpha_k\sinh(\phi_k t)\right) & k, \text{ even} \end{cases}. \tag{7}$$

where $\alpha_k = -\cos(\phi_k T/2)/\cosh(\phi_k T/2)$.

A comparison of the frequency roll-off of the minimum FOBE, RMS and fourth-moment bandwidth functions can be seen in Figure 1. This figure reveals that while the minimum fourth-moment bandwidth basis function has a somewhat larger main lobe than the truncated prolate-spheroidal function and the half sinusoid, its rate of side-lobe decay is significantly better.

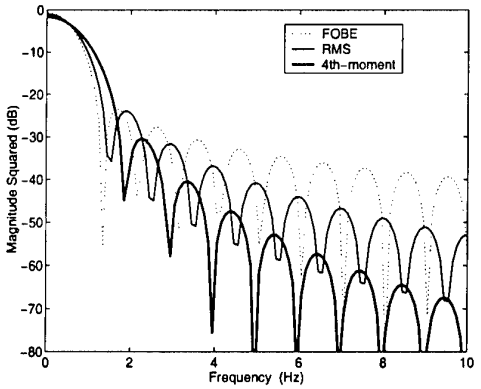


Figure 1: Magnitude spectra of $\psi_1(t)$ for the FOBE case (with $BT = 2\pi$), the RMS bandwidth and the fourth-moment measure, all for $T = 1$.

References

[1] A. H. Nuttall, "Minimum rms Bandwidth of M Time-Limited Signals with Specified Code or Correlation Matrix," *IEEE Trans. Inform. Th.* Vol. 14, pp. 699-707, Sept. 1968.

[2] D. Slepian and H. O. Pollak, "Prolate Spheroidal Wave Functions, Fourier analysis and uncertainty-I," *Bell Syst. Tech. J*, Vol. 40, pp. 43-63, 1961.

[3] G. B. Folland, *Real Analysis: Modern Techniques and Their Applications*, New York: Wiley-Interscience, 1984.

[1] This work was supported in part by NSF Grant NSF Grant CCR-9706591

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Neuro-Dynamic Programming and Rollout Algorithms. An Overview

Dimitri P. Bertsekas

ABSTRACT NOT AVAILABLE AT THE TIME OF PRINT

0-7803-5857-0/00/$10.00 ©2000 IEEE.

A system-theoretic derivation of the Welch-Berlekamp algorithm

Margreet Kuijper
Dept. of EE Engineering
University of Melbourne
VIC 3010 Australia
email: m.kuijper@ee.mu.oz.au

Abstract — **The similarity of the Berlekamp-Massey (B-M) algorithm and the Welch-Berlekamp (W-B) algoritm is demonstrated in showing that both algorithms are special instances of one iterative modeling procedure. In particular, from Reed & Solomon's original problem statement a W-B type algorithm is directly derived through a system-theoretic interpolation approach.**

Reed & Solomon's original curve fitting formulation for decoding a (n,k) Reed-Solomon code over a finite field $\mathbb{F}$ is readily reformulated as a minimal interpolation problem, see [1] and references therein. From this a system-theoretic formulation, involving trajectories of time $\boldsymbol{b}_i : \mathbb{Z}_+ \mapsto \mathbb{F}^2$, can be obtained as follows. Let the code locations be given by $x_1, \ldots, x_n$, define $G(s) := (s - x_{n-k+2}) \cdots (s - x_n)$ and let $(r_1, \ldots, r_n)$ be a received word. Without restrictions we may assume that $r_{n-k+1} = \cdots = r_n = 0$. Next let trajectories $\boldsymbol{b}_i$ be defined by

$$\boldsymbol{b}_i := \frac{1}{G(x_i)} \begin{bmatrix} 1 & 0 \\ 0 & G(\sigma) \end{bmatrix} \tilde{\boldsymbol{b}}_i \qquad \text{with}$$

$$\tilde{\boldsymbol{b}}_i := \left(\begin{bmatrix} r_i \\ 1 \end{bmatrix}, \begin{bmatrix} r_i x_i \\ x_i \end{bmatrix}, \begin{bmatrix} r_i {x_i}^2 \\ {x_i}^2 \end{bmatrix}, \ldots \right),$$

for $i = 1, \ldots, n-k+1$. Here σ denotes the backward shift. The decoding problem can now be formulated as: find a representation with minimal row degrees

$$\begin{bmatrix} D(\sigma) & -N(\sigma) \\ K(\sigma) & -Q(\sigma) \end{bmatrix} \boldsymbol{w} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \tag{1}$$

for the behavior $\mathcal{B}$ spanned by the trajectories $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{n-k+1}$. Thus we adopt a so-called behavioral system-theoretic approach, see [8] for more details.

The above corresponds to a slight variation of the W-B key equation in which polynomials D and N are sought with deg D minimal such that for $y_i := r_i / G(x_i)$

$$D(x_i) y_i = N(x_i) \tag{2}$$

as well as deg $N \leq$ deg D (rather than deg $N <$ deg D).

In earlier research [3] it was shown how the B-M algorithm can be interpreted as a special instance of the general iterative modeling procedure of [8, p. 289]. Below we outline an iterative algorithm along the same lines for constructing a representation (1), thereby solving the W-B type key equation (2). Our algorithm below is thus another instance of the modeling procedure of [8]. In particular, like the B-M algorithm, it makes use of the solution's degree L at each step to determine which type of update matrix is used. In this respect it differs from the W-B algorithm which uses a different integer parameter.

Algorithm

For $j = 0, \ldots, n-k$ *denote* $R_j := \begin{bmatrix} D_j & -N_j \\ K_j & -Q_j \end{bmatrix}$. *Initially define*

$$R_0 := \begin{bmatrix} 1 & 0 \\ 0 & s - x_{n-k+1} \end{bmatrix}, \text{ and } L_0 := 0.$$

Proceed iteratively as follows for $j = 1, \ldots, n-k$. *Compute, after processing* (x_i, y_i) *for* $i = 0, \ldots, j$, *the numbers* Δ_j *and* Γ_j *as follows:*

$$\begin{aligned} \Delta_j &:= D_{j-1}(x_j) y_j - N_{j-1}(x_j) \\ \Gamma_j &:= K_{j-1}(x_j) y_j - Q_{j-1}(x_j). \end{aligned}$$

Compute the matrix R_j *and the integer* L_j *as follows:*

$$R_j := V_j R_{j-1},$$

where, if $\Delta_j \neq 0$ *and* $(L_{j-1} < j/2 \quad or \ \Gamma_j = 0)$,

$$V_j(s) := \begin{bmatrix} s - x_j & 0 \\ -\frac{\Gamma_j}{\Delta_j} & 1 \end{bmatrix}; \quad L_j := L_{j-1} + 1,$$

and, if otherwise,

$$V_j(s) := \begin{bmatrix} 1 & -\frac{\Delta_j}{\Gamma_j} \\ 0 & s - x_j \end{bmatrix}; \quad L_j := L_{j-1}.$$

Topics of further research consist of the derivation of insightful and efficient algorithms (see also [2, 5]) for list decoding based on a behavioral modeling view.

References

[1] V. Guruswami and M. Sudan, "Improved decoding of Reed-Solomon and algebraic-geometric codes", *IEEE Trans. Info. Theory*, vol. 45, no. 6, pp. 1757–1768, 1999.

[2] G-L. Feng, "A generalization of the Welch-Berlekamp algorithm for weighted curve fitting with application to the Sudan decoding procedure", *Proceedings of the 13th Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes (AAECC)*, Hawaii, USA pp. 88–89, 1999.

[3] M. Kuijper and J.C. Willems, "On constructing a shortest linear recurrence relation", IEEE Trans. Aut. Control, vol. 42, pp. 1554–1558, 1997.

[4] M. Kuijper, "An algorithm for constructing a minimal partial realization in the multivariable case", *Systems & Control Letters*, vol. 31, pp. 225–233, 1997.

[5] R.R. Nielsen and T. Hoeholdt, "Decoding Reed-Solomon codes beyond half the minimum distance", Draft manuscript, 1999.

[6] J.C. Willems, "Paradigms and puzzles in the theory of dynamical systems", *IEEE Trans. Aut. Control*, vol. 36, pp. 259–294, 1991.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Very High-Speed Reed-Solomon Decoders

Dilip V. Sarwate and Naresh R. Shanbhag
Coordinated Science Laboratory
and the Department of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign
1308 West Main Street
Urbana, Illinois 61801-2307 USA
e-mail: {sarwate, shanbhag}@uiuc.edu

Abstract — **A pipelined finite-field multiplier structure in conjunction with a single systolic array implementation of the Berlekamp-Massey algorithm leads to a highly parallel decoder architecture in which the critical path delay is an order of magnitude smaller than the path delays of conventional architectures.**

Introduction

The Berlekamp-Massey algorithm [1] is an efficient iterative method for solving the key equation in BCH decoding that relates the (unknown) error locator polynomial $\lambda(z)$ and error evaluator polynomial $\omega(z)$ to the (known) syndrome polynomial $S(z)$. In the r-th iteration, the algorithm computes the r-th *discrepancy* Δ_r, and then updates its estimate of $\lambda(z)$ and a "scratch" polynomial $B(z)$. Even in highly parallel implementations, the speed bottleneck is this iterative loop which requires a multiplication (while computing Δ_r) followed by a division (while updating $B(z)$): the latter is more time-consuming than the former. Fortunately, the division can be replaced by a multiplication as described in [3]. Similarly, the two serial multiplications can be carried out in parallel if Δ_{r+1} (which is to be used in the *next* iteration) is computed at the same time as the polynomials are being updated in the *current* iteration. This gives the following algorithm, implementable with a single systolic array, for a t-error-correcting BCH code:

Initialization: $\Delta^{(0)}(z) = \Theta^{(0)}(z) = S(z) + z^{3t}$; $\gamma^{(0)} = 1$.

for $r = 0$ **until** $2t - 1$ **do**

$$\Delta^{(r+1)}(z) = \left\lfloor \frac{\gamma^{(r)}\lambda^{(r)}(z)}{z} \right\rfloor - \Delta_0^{(r)}\Theta^{(r)}(z)$$

$$(\Theta^{(r+1)}(z), \gamma^{(r+1)}) = \begin{cases} (\Theta^{(r)}(z), \gamma^{(r)}) \\ \left(\left\lfloor \frac{\Delta^{(r)}(z)}{z} \right\rfloor, \Delta_0^{(r)} \right) \end{cases}$$

Output: $\lambda(z) = \left\lfloor \frac{\Delta^{(2t)}(z)}{z^t} \right\rfloor$. $\omega(z) = \Delta^{(2t)}(z) \bmod z^t$.

Here, $\lfloor a(z)/z^s \rfloor$ denotes the quotient when $a(z)$ is divided by z^s. This is readily implemented by shifting when $s = 1$, whereas the output polynomials are merely different parts of the Δ register. Note that $\Delta_0^{(r)} = \Delta^{(r)}(0)$ is the r-th discrepancy and it is always the low-order symbol in the Δ register.[1]

High-Speed Implementations

VLSI implementations of the algorithm described above can be expected to operate roughly twice as fast as the the implementation in [3]. Even faster implementations are possible for block-interleaved codes, provided that decoding is completed *prior* to de-interleaving. For a code interleaved to depth M, the decoder structure is the same systolic array except that each storage cell now consists of a serial M-stage register. The critical path delay is no different from that in the original circuit. However, the results of a polynomial update are not required during the next $M - 1$ cycles while other (interleaved) codewords are being processed. This allows the use of a pipelined multiplier that computes the product of two elements of GF(2^m) in m clock cycles (assuming that $M \geq m$.)

Let $Y = y_0 + y_1\alpha + y_2\alpha^2 + \cdots y_{m-1}\alpha^{m-1}$ be an element of GF(2^m). The pipelined multiplier architecture is based on writing the product of X and Y as

$$X(y_0 + y_1\alpha + y_2\alpha^2 + \cdots y_{m-1}\alpha^{m-1}) =$$
$$Xy_0 + (X\alpha)y_1 + ((X\alpha)\alpha)y_2 + \cdots(\cdots((X\alpha)\alpha)\cdots\alpha)y_{m-1}$$

which can be computed by adding X into an empty accumulator (or not) according as y_0 is 1 (or 0). Simultaneously, X is multiplied by α to produce $X\alpha$. Then, $X\alpha$ is either added (or not) to the accumulator according as y_1 is 1 (or 0), while simultaneously, $X\alpha$ is multiplied by α to produce $X\alpha^2$; and so on ... for m stages. Multiplication by α is easy to implement, and thus the critical path for this new decoder architecture passes through only one Exclusive OR (XOR) gate and one 2-to-1 multiplexer. This is an order of magnitude smaller than the delay in a conventional multiplier.

Ignoring wiring delays and other non-idealities, an 0.18 μm CMOS technology Reed-Solomon decoder over GF(2^8) has critical path delays of 6.8 ns, 3.0 ns, and 0.36 ns respectively for the implementations described in [3], [4] and this paper. Decoding at rates exceeding a gig*abyte* per second appears to be feasible with the decoder implementation described above. Details of the proposed architecture can be found in [5].

Acknowledgments

This research was supported in part by the National Science Foundation under Grants MIP-9707742 and MIP-9710235.

References

[1] R. E. Blahut, *Theory and Practice of Error-Control Codes,* Addison-Wesley, Reading MA, 1983.

[2] R. E. Blahut, *Algebraic Codes for Data Transmission,* Cambridge University Press, (second edition of [1], to appear.)

[3] I. S. Reed, M. T. Shih, and T. K. Truong, "VLSI design of inverse-free Berlekamp-Massey algorithm," *Proc. IEE, Part E,* vol. 138, pp. 295-298, September 1991.

[4] S. Sakata and M. Kurihara, "A fast parallel implementation of the Berlekamp-Massey algorithm with a 1D systolic array architecture," in *Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes,* (G. Cohen, M. Giusti, and T. Mora, (eds.): Proc. AAECC-11, Paris, July 1995), *Lecture Notes on Computer Science,* vol. 948, pp. 415-426, Springer-Verlag, 1996.

[5] D. V. Sarwate and N. R. Shanbhag, "High-speed architectures for Reed-Solomon decoders," *IEEE Trans. VLSI Systems,* (to appear).

[1] After discovering this result, we found that it had been published already in [4]. It also appears in [2].

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Euclid's Algorithm and LFSR synthesis

P. Udaya [1]
Department of Computer Science
and Software Engineering,
University of Melbourne,
Parkville, Vic., 3052, Melbourne,
AUSTRALIA.
e-mail: udaya@cs.mu.oz.au

Abstract — **We consider two methods of Euclid's algorithm to solve the Linear Feedback Shift Register (LFSR) synthesis problem. One of the methods is identically equivalent to the celebrated Berlekamp-Massey(B-M) algorithm. The other method is distinctly Euclidean. The formulation of the problem from Euclid's algorithm leads to the characterization of the LFSR synthesis for the reverse sequence given the LFSR synthesis for the forward sequence.**

I. LFSR Synthesis problem

All polynomials and sequences considered in this paper are over a finite field $\mathbf{F}$. Let $deg(P)$ denote the degree of the polynomial P and $Coeff(P,l)$ denote the coefficient of x^l in P. Let $S^N = \{s_0, s_1, \cdots, s_{N-1}\}$ denote a sequence of length N over $\mathbf{F}$. The LFSR synthesis problem is, given S^N find a shortest length LFSR (L) satisfying the recursion:

$$s_j = -\sum_{i=0}^{L-1} c_i s_{j-L+i}, N < j \leq L, c_i \in \mathbf{F}. \quad (1)$$

A Algorithm A

Here we represent the sequence S^N as $S_{N-1} + s_{N-2}x + \cdots + s_1 x^{N-2} + s_0 x^{N-1}$ and compute recursively using the GCD algorithm the minimal connection polynomial $C(x) = c_0 + c_1 x + \cdots + c_{L-1}x^{L-1} + x^L$, where $c_i's$ are as in (1). We denote the LFSR of length L by a polynomial pair $(C(x), B(x))$, where $B(x) = S(x)C(x) \ (mod\ x^N)$. This is the version of Euclid's algorithm used by Dornstetter in [1] to prove the equivalence with the B-M algorithm.

B Algorithm-B

Let a sequence $S^{(N)}$ be represented by the polynomial $S(x) = s_0 + s_1 x + \cdots + s_{N-1}x^{N-1}$, and the corresponding connection polynomial $D(x)$ is given by $D(x) = 1 + c_{L-1}x + \cdots + c_0 x^L$, where $c_i's$ are as in (1). Note that the the polynomials $S(x)$ and $D(x)$ given above happen to be the reciprocal polynomials of the corresponding polynomials defined in Algorithm-A. The following theorem supports the LFSR synthesis.

Theorem 1 *An LFSR of lengthg L with a connection polynomial $D(x)$ of degree L generates S^N if and only if there exists a polynomial $B(x)$ such that*

$$B(x) = S(x)D(x) \ (mod\ x^N), deg(B(x)) < L, Coeff(D,0) = 1. \quad (2)$$

We denote the LFSR of length L by a polynomial pair $[D(x), B(x)]$ in this representation. The above theorem in conjunction with the Euclid's GCD evaluation of the polynomials $S(x)$ and x^N, results in Algorithm B. At each iteration the algorithm provides a valid LFSR representation of (2) with the length $max\{deg(D(x)), 1 + deg(B(x))\}$. A minimal solution is chosen when length of the LFSR is minimal.

Remark: In Algorithm-B, the length of the LFSR at each step monotonically decreases to the minimum value ($L^0 = N$). On the other hand, in Algorithm-A which resembles the B-M algorithm, the length of the LFSR at each iteration gradually increases to the minimal value of L from 0.

Next theorem characterizes the length of the LFSR design for the reverse sequence.

Theorem 2 *Let us consider the shortest LFSR $(C^{(2m)}, B^{(2m)})$ of length $L^{(2m)}$ that generates the sequence $S^{(2m)} = \{s_1, s_2, \cdots s_{2m}\}$, Let $(\hat{C}^{(2m)}, \hat{B}^{(2m)})$ be the shortest LFSR for reverse sequence $\hat{S}^{(2m)} = (s_{2m}, s_{2m-1}, \cdots s_1)$ of length $\hat{L}^{(2m)}$. If $L^{(2m)} < m$, then*
$\hat{L}^{(2m)} = L^{(2m)}$ if $Coeff(C^{2m}, 0) \neq 0$;
$\hat{L}^{(2m)} = 2m - L^{(2m)} + 1$ otherwise.
If $L^{(2m)} > m$, then
$\hat{L}^{(2m)} = L^{(2m)}$ if $Coeff(\hat{C}^{2m}, 0) \neq 0$;
$\hat{L}^{(2m)} = 2m - L^{(2m)} + 1$ otherwise.

The above Theorem characterizes completely the length of the LFSR for the reverse sequence given the design of the forward sequence. This generalizes a result in [2] which considers the length of the reverse sequence only for a particular case of sequences whose complexity is exactly half of the sequence length ($L^{(2m)} = m$). Also observe that, in our approach, the designs for the reverse sequence can be obtained by Euclid's algorithm.

Even though the similarities between the B-M and other algorithms are studied extensively, this view point of the paper concerning the LFSR synthesis procedures using Euclid's algorithm seems to be new.

[1] This work was supported by Australian Research Council Large Grant #A49701206

References

[1] J. L. Dornstetter. On the Equivalence Between Berlekamp's and Euclid's Algorithms. *IEEE Trans. Inform. Theory*, 33:428–431, 1987.

[2] K. Imamura and W. Yashida. A Simple Derivation of the Berlekamp Massey Algorithm. *IEEE Trans. Inform. Theory*, 33:146–150, 1987.

[3] P. Udaya. *Linear Feedback Shift Regiter Synthesis for Sequences over Finite Fields and Rings.* PhD thesis, Indian Institute of Technology, Kanpur, India, 1987.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On Syndrome Generation and Error Location Search in the Decoding of Hermitian Codes

Chung-Chin Lu[1] Heng-Shun Wang Jia-Pyn Chen

Abstract — **When a Hermitian curve is put in a special position with respect to its infinite rational point, the (x, y)-coordinates of all finite rational points of the Hermitian curve have regular algebraic properties. Based on these properties, the use of Horner's rule and the mechanism of Chien search in the decoding of Reed-Solomon codes can be extended to render up efficient architectures for syndrome generation and error location search in the decoding of codes constructed from the Hermitian curve.[1, 2, 3]**

I. Introduction

It is well known that syndrome generation in the decoding of Reed-Solomon codes is usually executed by Horner's rule which has regular hardware structure and is suitable for VLSI implementation. The first goal of this paper is to extend the use of Horner's rule to the decoding of Hermitian codes. The intuitive idea of error-locator searching is to evaluate the value of the error-locator polynomial at each finite rational point of the Hermitian curve. If the value is zero, then an error location is found. It will be welcome to have an architecture like the mechanism of Chien search, which generates all finite rational points of the Hermitian curve and evaluates the error-locator polynomial at these points very efficiently, which is the second goal of this paper.

II. Rational Points in a Hermitian Curve

Let $E_r = \{\infty, 0, 1, \cdots, r-2\}$ be a linearly ordered set with $\infty < 0 < 1 < \cdots < r-2$. Assume that α is a primitive element of $GF(q^2)$ and $\beta = \alpha^{q+1}$. For convenience, we define $\alpha^\infty = 0$. The set Ω of (x, y)-coordinates of all finite rational points of the Hermitian curve $\mathcal{H}_q$ over $GF(q^2)$, defined by $x^{q+1} = y^q + y$, can be shown to be $\Omega = \bigcup_{m \in E_q}(X_m \times Y_m)$, where

$$X_m = \begin{cases} \{0\}, & \text{if } m = \infty, \\ \{\alpha^{m+k(q-1)} | k = 0, 1, \cdots, q\}, & \text{if } m \in [0, q-2], \end{cases} \quad (1)$$

and Y_m is the solution set of the equation $y^q + y = \beta^m, \forall m \in E_q$. Define $\Omega_i^{(y)}$ to be the intersection of the Hermitian curve with the line $y = \alpha^i$ on the affine plane over $GF(q^2)$ and λ_i be m if α^i is in Y_m for each $i \in E_{q^2}$. Now, we are able to identify a point $(\alpha^{\lambda_i + k(q-1)}, \alpha^i)$ in the y-slice $\Omega_i^{(y)}$ by the pair (k, i), denote this point as $P_{(k,i)}$ for each i in E_{q^2}, and order the points $P_{(k,i)}$ in Ω according to a lexicographical ordering on the index pairs (k, i) : $(k', i') <_l (k, i)$ if $i' < i$ or if $i' = i$ and $k' < k$, where $\infty < 0 < 1 < \cdots < q^2 - 2$.

III. Syndrome Generation

For our purposes, let $S(a, b)$ be the syndrome of the Hermitian code H_m associated with the monomial $x^a y^b$ for $a, b \geq 0$ and $aq + b(q+1) \leq m$. It can be shown that $S(a, b) = \sum_{P \in \Omega} r_P x(P)^a y(P)^b = \sum_{i=0}^{q^2-2} c_{a,i} (\alpha^b)^i$, where $\{r_p\}_{P \in \Omega}$ is the received symbol sequence and $c_{a,i} = \sum_{P \in \Omega_i^{(y)}} r_P x(P)^a$ for each $i \in E_{q^2}$. If $\lambda_i = \infty$, we have $c_{a,i} = 0$ and if $\lambda_i \neq \infty$, $c_{a,i} = \alpha^{a\lambda_i} \sum_{k=0}^{q} r_{k,i} (\alpha^{a(q-1)})^k$, where we denote r_P as $r_{k,i}$ when the two-dimensional index of P is (k, i). Thus the generation of the syndrome $S(a, b)$ can be implemented by a Horner's double-loop with feedback gains $\alpha^{a(q-1)}$ and α^b respectively.

IV. Error Location Search

Here we re-index the q^3 finite rational points through a unique order-preserving transformation T from the two-dimensional index set onto $(E_{q^3}, <)$. Let $\sigma(x, y) = \sum_{l=1}^{n} \sigma_l x^{a_l} y^{b_l}$ be an error-locator polynomial with $a_1 = b_1 = 0$. Since the first point P_∞ has coordinates $(0, 0)$, we have $\sigma(P_\infty) = \sigma_1$ and then P_∞ is an error location if and only if $\sigma_1 = 0$. At all other finite rational points $P_j, 0 \leq j \leq q^3 - 2$, we have $\sigma(P_j) = \sum_{l=1}^{n} F_l(P_j) = \sum_{l=1}^{n} Loop_l(j) \cdot Select_l(j)$. The sequence $\{Select_l(j)\}_{0 \leq j \leq q^3-2}$ can be implemented by a multiplier-selection unit with a control signal and the sequence $\{Loop_l(j)\}_{0 \leq j \leq q^3-2}$ can be generated sequentially like in the mechanism of Chien search by a closed-loop with initial value σ_l and with three feedback gains $\alpha^{a_l(q-1)}$, $\alpha^{a_l(q-1)+b_l}$ and α^{b_l}, selected by a multiplexer with a control signal.

V. Conclusion

In this paper, we exploit a specific ordering of all finite rational points of a Hermitian curve and extend the use of Horner's rule and the mechanism of Chien search in the decoding of Reed-Solomon codes to the decoding of Hermitian codes. The basic building blocks in the proposed architectures are loops and multiplier-selection units. Since the multipliers used are all special-purposed, the hardware complexity is very acceptable. Moreover, the number of clock times needed to complete a cycle of syndrome generation or a cycle of error-location search is just the length of a received codeword. In conclusion, the two goals of this paper, stated in the introduction section, are achieved.

References

[1] J. Little, K. Saints and C. Heegard, "On the structure of Hermitian codes," *J. Pure and Applied Algebra,* 121 (1997), pp. 293–314.

[2] B.-Z Shen, "On the encoding and decoding of the codes from Hermitian curves," in *Cryptography and Coding III, IMA Conf. Proc. Ser.*, vol. 45, M. Fanley, Ed. Oxford, UK: Oxford Univ. Press, 1993, pp. 337–356.

[3] H. Stichtenoth, "A note on Hermitian codes over $GF(q^2)$, "*IEEE Trans. Inform. Theory,* vol. 34, pp. 1345–1348, Sept. 1988.

[1]This work was supported by the National Science Council, Taiwan, under contract no. NSC86-2221-E-007-022. The authors are with the Department of Electrical Engineering, National Tsing Hua University, Hsinchu 30055, Taiwan, email: cclu@ee.nthu.edu.tw.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

An All–Analog Ring Network for Turbo–Detection of Convolutionally Encoded DPSK Signals

Joachim Hagenauer
Inst. for Communications Eng.
Munich University of Technology
D-80290 Munich, Germany
e-mail: hag@lnt.ei.tum.de

Andrew Schaefer
Inst. for Communications Eng.
Munich University of Technology
D-80290 Munich, Germany
e-mail: abschaef@eikon.tum.de

Christian Weiß
Inst. for Communications Eng.
Munich University of Technology
D-80290 Munich, Germany
e-mail: weiss@lnt.ei.tum.de

I. Description and performance results

The turbo–principle [Hag97] is far more reaching than the original turbo code concept. Encoded DPSK transmission, e.g., can be viewed as a serial concatenation of a channel code with a rate–one code representing the DPSK modulation. Iterative decoding of this concatenated scheme shows surprisingly good performance (see [PSH97, Hoe99]). We describe the serial concatenation of interleaved tail–biting convolutional codes (TBCC) with this DPSK rate–one code transmitted over AWGN and flat Rayleigh fading channels. The receiver performs time–continuous "turbo" iterations between the inner and outer codes and is realized by two analog ring networks connected via an interleaver ring which exchanges extrinsic information by means of analog signals being continuous in time and value. Employing analog circuits is advantageous, since they are much faster and consume significantly less power. The feasibility of analog circuits replacing the Viterbi or BCJR algorithm was shown in [Hag98], [HOM99] and [Loel98]. In the meantime the first VLSI chips for simple decoders have been produced at Lucent/TU Munich [MGY00] and Endora/ETH Zurich.

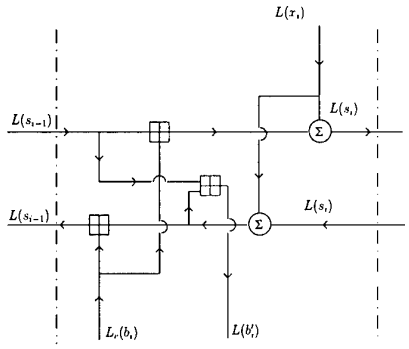


Figure 1: Structure of the analog DECPSK receiver corresponding to one trellis section.

The key element of the analog networks is the representation of the log–likelihood ratio (LLR) of a binary random variable $L(x) = \log(P(x=+1)/P(x=-1))$ by voltages. The 'box–plus' element $\boxplus$ defined by

$$\begin{aligned} L(x_1) \boxplus L(x_2) &\triangleq L(x_1 \oplus x_2) \\ &= 2\,\mathrm{atanh}(\tanh(L(x_1)/2) \cdot \tanh(L(x_2)/2)) \end{aligned}$$

can then be realized by a simple circuit consisting of 9 transistors [MGY00]. Using these elements plus summations we design an analog turbo receiver for the concatenation of DECPSK modulation and a memory–2 TBCC. One section of the DECPSK receiver (processing one trellis section) is shown in Fig. 1. Note that this results in a delay–less nonlinear bidirectional circuit connected to the receiver values, the neighboring circuits and the interleaver ring. The channel provides us with the weighted matched filter outputs $L(x_i)$ and the interleaver ring with the extrinsic LLRs $L(b_i)$ from the decoder circuit of the TBCC. Simulation results are obtained by solving nonlinear differential equations. Fig. 2 shows that the analog network performs similar to a digital turbo decoder applying 20 iterations. In addition, we discuss implementation issues of analog VLSI showing their advantages in terms of power consumption and speed.

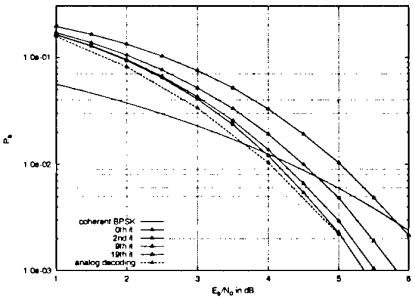


Figure 2: Bit error rate versus signal–to–noise ratio for decoding of DECPSK serially concatenated with tail–biting convolutional codes applying a digital iterative decoder and an analog decoder.

References

[Hag97] J. Hagenauer, "The turbo principle — Tutorial introduction and state of the art," in *Proc. Int. Symposium on Turbo Codes & Related Topics*, Brest, France, pp. 1–11, Sept. 1997.

[Hoe99] P. Hoeher and J. Lodge, "'Turbo DPSK": Iterative differential PSK demodulation and channel decoding", *IEEE Trans. on Communications*, vol. Com–47, Jun. 1999.

[PSH97] M. Peleg and S. Shamai, "Iterative decoding of coded and interleaved noncoherent multiple symbol detected DPSK", *Electronic Letters*, vol. 33, no.12, pp 1018–1020, Jun. 1997.

[Hag98] J. Hagenauer,"Decoding of binary codes with analog networks," In: *Proc. of the Information Theory Workshop 1998*, San Diego, CA, USA, pp. 13–14, Feb. 1998

[Loel98] H.-A. Loeliger, M. Helfenstein, F. Lustenberger, and F. Tarkoey, "Iterative sum–product decoding with analog VLSI," in *ISIT'98, Cambridge, MA, USA*, p. 146, 1998.

[HOM99] J. Hagenauer, E. Offer, C. Measson, and M. Moerz, "Decoding and equalization with analog non–linear networks" *European Transactions on Telecommunications ETT*, vol. 10, no. 6, Nov. 1999.

[MGY00] M. Moerz, Th. Gabara, R. Yan, and J. Hagenauer, "An analog 0.25 μm BICMOS tailbiting MAP decoder" in *Proc. of the ISSCC*, San Francisco, USA, pp. 356–357, Febr. 2000.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On the Efficiency of Some Suboptimal Algorithms for Bit Decoding of Binary Codes[1]

Elke Offer
Institute for Commun. Engineering
Munich University of Technology
Arcisstr. 21
D-82290 Munich, Germany
elke@lnt.e-technik.tu-muenchen.de

Emina Soljanin
Mathematical Sciences
Research Center,
Bell Labs, Lucent Technologies,
Murray Hill, NJ 07974,USA
emina@lucent.com

Abstract — **Several popular, suboptimal algorithms for bit decoding of binary block codes such as turbo decoding, threshold decoding, and message passing for LDPC, were developed almost as a *common sense* approach to decoding of some specially designed codes. We explain exactly how they approximate the optimal decoding algorithm, and show how good this approximation is in some special cases.**

We propose an entirely new approach to the problem of iterative decoding, which is algebraic in nature and *derives* the well known suboptimal algorithms from the bit-optimal as a starting point. This approach gives new insights into the issues of iterative decoding.

We are concerned with a binary block code $\mathcal{C}$ defined by its parity-check matrix $H = \{h_{ij}\}_{(n-k)\times n}$, *i.e.*, by the group generators $\boldsymbol{h}_i = \{h_{ij}\}_{1\times n}$, $i \in \mathcal{I}$, of its dual code $\mathcal{C}'$, where $\mathcal{I}$ is used to denote the index set $\mathcal{I} = \{0, 1, \ldots, n-k-1\}$. We consider suboptimal decoding algorithms for a binary code $\mathcal{C}$, *e.g.*, a turbo decoding scheme (as introduced in [1], [2]) with two component codes $\mathcal{C}_1$ and $\mathcal{C}_2$ defined by their dual codes' sets of generators $\mathcal{I}_1$ and $\mathcal{I}_2$ such that $\mathcal{I}_1 \cap \mathcal{I}_2 = \emptyset$ and $\mathcal{I}_1 \cap \mathcal{I}_2 = \mathcal{I}$.

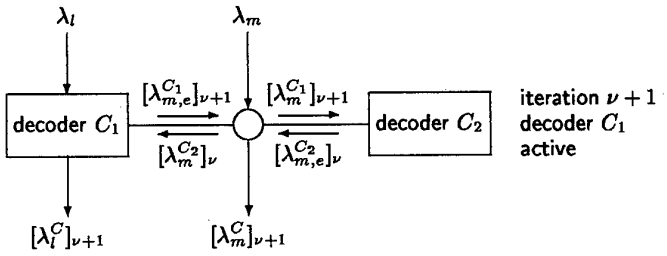
The channel is assumed to be memoryless and codewords equiprobable. We derive an expression for optimal decoding of the whole code $\mathcal{C}$ based on the dual code (as in [3]), and then rewrite it so that it explicitly involves only $\boldsymbol{h}_i$. Thus, for the log-likelihood of bit m over code $\mathcal{C}$, $L_m^{\mathcal{C}} = \log[P(c_m = 0|\boldsymbol{r})/P(c_m = 1|\boldsymbol{r})]$, we obtain the following:

$$L_m^{\mathcal{C}} = \log\frac{1+\lambda_m}{1-\lambda_m} + \log\frac{\prod\limits_{i\in\mathcal{I}}{}^{\otimes}\left[1+\prod\limits_{\substack{j=0\\ j\neq m}}^{n-1}\lambda_j^{h_{ij}}\right]}{\prod\limits_{i\in\mathcal{I}}{}^{\otimes}\left[1+(-1)^{h_{im}}\prod\limits_{\substack{j=0\\ j\neq m}}^{n-1}\lambda_j^{h_{ij}}\right]}, \quad (1)$$

where $\lambda_j = [p(r_j|0) - p(r_j|1)]/[p(r_j|0) + p(r_j|1)]$ and

$$\lambda_i \otimes \lambda_j = (\lambda_i \cdot \lambda_j)^{1-\delta_{i,j}} = \begin{cases} \lambda_i \cdot \lambda_j, & i \neq j, \\ 1, & i = j. \end{cases}$$

We then show that the turbo decoding algorithm can be represented as shown in the figure below:



$$[\lambda_m^{\mathcal{C}_1}]_{\nu+1} = \frac{\lambda_m \otimes \prod\limits_{i\in\mathcal{I}_1}{}^{\otimes}\left[1+\lambda_m^{h_{im}}\prod\limits_{\substack{j=1\\ j\neq m}}^{n-1}[\lambda_j^{\mathcal{C}_2}]_\nu^{h_{ij}}\right]}{\prod\limits_{i\in\mathcal{I}_1}{}^{\otimes}\left[1+\lambda_m^{h_{im}}\prod\limits_{\substack{j=1\\ j\neq m}}^{n-1}[\lambda_j^{\mathcal{C}_2}]_\nu^{h_{ij}}\right]}$$

$$[\lambda_m^{\mathcal{C}}]_{\nu+1} = \frac{[\lambda_m^{\mathcal{C}_2}]_\nu \otimes \prod\limits_{i\in\mathcal{I}_1}{}^{\otimes}\left[1+\prod\limits_{j=0}^{n-1}[\lambda_j^{\mathcal{C}_2}]_\nu^{h_{ij}}\right]}{\prod\limits_{i\in\mathcal{I}_1}{}^{\otimes}\left[1+\prod\limits_{j=0}^{n-1}[\lambda_j^{\mathcal{C}_2}]_\nu^{h_{ij}}\right]}$$

The corresponding expression for the log-likelihood of bit m of the turbo decoding algorithm at iteration $(\nu+1)$ given by

$$[L_m^{\mathcal{C}}]_{\nu+1} = \log\frac{1+[\lambda_m^{\mathcal{C}_2}]_\nu}{1-[\lambda_m^{\mathcal{C}_2}]_\nu} + \log\frac{\prod\limits_{i\in\mathcal{I}_1}{}^{\otimes}\left[1+\prod\limits_{\substack{j=0\\ j\neq m}}^{n-1}[\lambda_j^{\mathcal{C}_2}]_\nu^{h_{ij}}\right]}{\prod\limits_{i\in\mathcal{I}_1}{}^{\otimes}\left[1+(-1)^{h_{im}}\prod\limits_{\substack{j=0\\ j\neq m}}^{n-1}[\lambda_j^{\mathcal{C}_2}]_\nu^{h_{ij}}\right]}$$

is then compared to the optimal solution (1).

A similar analysis can be done for Gallager's message passing algorithms for his LDPC codes as well as for threshold decoding.

[1]This work was supported by the 1999 German-American Networking Research Grant given by the the national academies of engineering of Germany and the USA.

References

[1] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error correcting coding and decoding: Turbo-codes(1)," *Proc. 1993 IEEE Int. Conf. Commun. (ICC'93)*, Geneva, Switzerland, May 1993, pp. 1064–1070.

[2] J. Hagenauer, E. Offer, and L. Papke, "Iterative decoding of binary block and convolutional codes," *IEEE Trans. Inform. Theory*, Vol. IT-42, pp. 429–445, March 1996.

[3] C. R. P. Hartmann and L. D. Rudolph, "An optimum symbol by symbol decoding rule for linear codes," *IEEE Trans. Inform. Theory*, Vol. IT-22, pp. 514–517, Sept. 1976.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

An Efficient MAP Decoding Algorithm Using a Section Trellis Diagram

Ryujiro Shibuya† Yuichi Kaji† Tadao Kasami‡
†Nara Institute of Science and Technology, ‡Hiroshima City University
e-mail: {ryuji-s,kaji}@is.aist-nara.ac.jp, kasami@cs.hiroshima-cu.ac.jp

Abstract — **An efficient algorithm for the MAP decoding is presented. The proposed algorithm is a hybrid of the conventional BCJR algorithm and the recursive-MAP (r-MAP) algorithm which has been proposed by the authors. The r-MAP algorithm uses structural properties of linear codes to reduce the decoding complexity, but does not work well for high-rate codes. The proposed algorithm overcomes this defect, and achieves smaller decoding complexity than BCJR and r-MAP algorithms for any code.**

I. Background

The *maximum a posteriori (MAP)* decoding plays an essential role in the decoding of *turbo codes* and the complexity of a MAP decoding algorithm is significant for realization of efficient turbo decoders. The *BCJR algorithm*[1] is known as the conventional algorithm for the MAP decoding, but the complexity of the BCJR algorithm is too much for constructing the entire *trellis diagram* of the code. The authors have proposed the *recursive-MAP (r-MAP) algorithm* in [3]. The r-MAP algorithm uses structural properties of linear codes, and succeeds in reducing (time and space) complexity for the MAP decoding for relatively low-rate codes. However, the r-MAP algorithm is inefficient for high-rate codes. Liu et al. consider to apply the BCJR algorithm on a *section trellis diagram*, and show that the decoding complexity is reduced[2].

II. Proposed Algorithm

Let C be an (n,k) binary linear code, and let C_{xy} be the set of codewords of C such that the first x and the last $n-y$ symbols are all zero. Also let $p_{xy}(C)$ be a set of vectors which are obtained by deleting the first x and the last $n-y$ symbols of each codeword of C. Let L_{xy} be the set of cosets of $p_{xy}(C_{xy})$ in $p_{xy}(C)$, and define $D_{xy}^{i/b}$ with $D_{xy} \in L_{xy}$, $x < i \leq y$ and $b \in \{0,1\}$ as the set of vectors in D_{xy} such that the $(i-x)$-th symbol of the vector is b. Define

$$\mathrm{MAP}(D_{xy}, i, b) \triangleq \sum_{v \in D_{xy}^{i/b}} \prod_{x<j\leq y} \Pr_j(v_j) \cdot \Pr(r_j|v_j)$$

for $x < i \leq y$ and $b \in \{0,1\}$ where $\Pr_j(v_j)$ is the *a priori probability* that the symbol v_j is chosen at the j-th bit position. If the j-th bit position is a parity symbol, then $\Pr_j(v_j) \triangleq 1$. The MAP table for $D_{xy} \in L_{xy}$ is a table which contains $\mathrm{MAP}(D_{xy}, i, b)$ for $x < i \leq y$ and $b \in \{0,1\}$. In the r-MAP algorithm, the MAP tables are constructed in a divide-and-conquer manner: For short sections (i.e. $y-x$ is small), the MAP tables are constructed in a rather straight-forward way. Otherwise, the MAP tables are computed recursively, by decomposing the coset D_{xy} into cosets in L_{xz} and L_{zy}, where $x < z < y$, computing the (smaller) MAP tables for the decomposed cosets, and combining the computed (smaller) MAP tables. By this approach, the decoding complexity is reduced significantly for low-rate codes. However, for high-rate codes, the complexity of the r-MAP algorithm is larger than the BCJR algorithm. Careful analysis of the complexity of the r-MAP algorithm shows that the complexity necessary at the recursion levels two or three is considerably large.

We consider a hybrid algorithm of the r-MAP and the BCJR algorithms. In the proposed hybrid algorithm, MAP tables are constructed in the bottom-up manner, as in the r-MAP algorithm. When MAP tables for reasonable section length are built up, we switch to the BCJR algorithm. A section trellis diagram with appropriate section boundaries are considered, and MAP tables are associated with the composite branches of the section trellis. Then, a BCJR-like algorithm is executed to obtain the MAP table for the code C.

III. Evaluation

The decoding complexity of the proposed algorithm depends on the section boundaries at which algorithms are switched. The BCJR and the (pure) r-MAP algorithms can be regarded as special cases of the proposed algorithm. Therefore, the decoding complexity of the proposed algorithm cannot be wronger than the complexity of the BCJR and r-MAP algorithms. Table 1 is to compare the decoding complexity of the BCJR, r-MAP and the proposed algorithms with the *known best* sectionalization. The table shows the number of multiplications of probabilities necessary for one decoding. The proposed algorithm is more efficient than the other algorithms.

As a future work, a systematic way for finding the optimum sectionalization must be investigated.

Table 1: The decoding complexity.

code*	BCJR	r-MAP	proposed
RM(64,22)	1,500,132	174,464	116,096
RM(64,42)	2,197,476	4,492,672	529,792
$\mathrm{eBCH}(64,16)_b$	2,860,004	120,192	120,192
$\mathrm{eBCH}(64,36)_c$	56,098,788	105,056,640	20,670,592
$\mathrm{eBCH}(64,45)_c$	3,000,292	15,525,680	1,762,528

*$\mathrm{RM}(n,k)$ and $\mathrm{eBCH}(n,k)_p$ stand for Reed-Muller code and extended BCH code with p-type permutation, respectively.

References

[1] L.R. Bahl, J. Cocke, F. Jelinek and J. Raviv: "Optimal Decoding of Linear Codes for Minimizing Symbol Error Rate," IEEE Trans. on IT., **20**, 2, pp.284-287 (1974).

[2] Y. Liu, M. Fossorier and S. Lin: "MAP Algorithms for Decoding Linear Block Codes Based on Sectionalized Trellis Diagram," Globecom '98, Sydney, Australia, pp.562-566 (Nov. 1998).

[3] R. Shibuya, Y. Kaji, T. Fujiwara, T. Kasami and S. Lin: "Recursive Algorithm for Efficient MAP Decoding of Binary Linear Block Codes," the 1998 Intl. Symp. on IT. and its App., Mexico City, Mexico, pp.639-642 (Oct. 1998).

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On the Analog Implementation of the APP (BCJR) Algorithm

M. Moerz[1], J. Hagenauer, and E. Offer
Institute for Communications Engineering
Munich University of Technology
Arcisstr. 21, 80290 München, Germany
e-mail: Matthias.Moerz@ei.tum.de

Abstract — **Fundamental building blocks for analog decoders are introduced which transform log-likelihood ratios into probabilities and vice versa. By interconnecting these blocks general trellis modules can be designed for an analog VLSI implementation of the APP (BCJR) decoding algorithm.**

I. Introduction

Analog Viterbi decoders are already employed in magnetic recording. Recently, analog VLSI implementations of APP decoders were reported in [1], [2]. For more background information see references therein. Such decoders are needed for complex and time-consuming 'turbo'-decoding and 'turbo'-equalization. The main advantages of an analog implementation include higher speed, smaller size and lower power consumption when compared to a digital implementation.

II. Log-Likelihood Ratios and Probabilities

Consider a discrete random variable X with values $x \in \{0,\ldots,J-1\}$. The log-likelihood of the probability $P_X(x=j)$ is defined as $l_j(X) = \ln(P_X(x=j))$ by using the natural logarithm. A log-likelihood ratio of the discrete random variable X can be expressed by using two outcomes $x=i$ and $x=j$

$$L_{i,j}(X) = l_i(X) - l_j(X) = \ln \frac{P_X(x=i)}{P_X(x=j)}. \qquad (1)$$

The probability of a possible outcome $x=j$ is determined by

$$P_X(x=j) = \frac{e^{-L_{i,j}(X)}}{\sum_{\nu=0}^{J} e^{-L_{i,\nu}(X)}}. \qquad (2)$$

III. Analog Decoder Implementation

Elementary devices of an analog decoder are bipolar transistors and diodes, which realize the exponential and logarithmic functions, respectively. The collector current I_C of a bipolar transistor is a function of the base emitter voltage V_{BE} with $I_C = I_S\, e^{V_{BE}/V_T}$, where I_S denotes the transport saturation current and V_T is a temperature dependent quantity ($\approx$ 26 mV at 300° K). The configuration of the emitter coupled transistors shown in Fig. 1 forms a Type II block. This block is an exact circuit implementation of (2), where the input voltages $V_j = V_T\, l_j(X) + C$ are transformed into output currents $I_j = I\, P_X(x=j)$. Here I is the bias current of the circuit and C is a voltage constant to be chosen according to the required input voltage range of the circuit. Log-likelihood ratios are represented by differential input voltages $V_{i,j} = V_i - V_j = V_T\, L_{i,j}(X)$. The probability

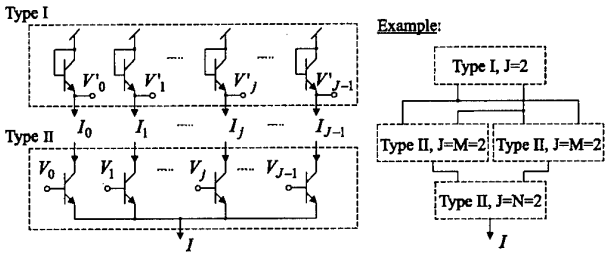


Fig. 1: Type I block: Diode connected transistors transforming probabilities into log-likelihood ratios, Type II block: Emitter coupled devices transforming log-likelihood ratios into probabilities, Example: Trellis module for a binary trellis section (XOR operation of three bits).

multiplication of the APP decoding algorithm can be implemented by using a stacked configuration of Type II blocks, where output currents of one lower block ($J = N$) are used as bias currents for N upper blocks ($J = M$). Assuming the lower Type II block for a variable X_1 and each upper Type II block for a variable X_2 the output currents of the upper Type II blocks represent NM probability products $P_{X_1} P_{X_2}$. The probability summation of the APP decoding algorithm is simply obtained by connecting the current outputs of the blocks together. This technique is used in [1] to design trellis modules with current inputs and in [2] for modules with voltage inputs. The inversion of the exponential characteristic can be obtained by using diode connected transistors which form the Type I block in Fig. 1. Such devices act as simple diodes and generate voltage drops proportional to the logarithm of the input currents. When the input currents represent (scaled) probabilities this circuit exactly implements (1) with $-V'_{i,j} = V'_{j,i} = V_T\, L_{i,j}(X)$. The negative sign is due to all V'_j which are voltages to ground rather than voltage drops at the diodes. Note that any scaling of probabilities cancels out in (1). The trellis modules in [2] use such Type I blocks on top of all Type II blocks to transform the (scaled) probabilities back into the log-likelihood domain while in [1] CMOS current mirrors are used to generate output currents carrying the probability information. For the binary case with $N, M = 2$ and a single binary trellis section (see Example in Fig. 1) the circuit implementation results in a Gilbert cell with diode loads [2], where the overall function can be described by $V'_{1,0} = 2\, V_T\, \tanh^{-1}\left[\tanh\left(\frac{V_{0,N-1}}{2V_T}\right)\tanh\left(\frac{V_{0,M-1}}{2V_T}\right)\right]$.

[1] This work was supported by the Wireless Circuits and Systems Research Department, Bell Labs, Lucent Technologies, 600 Mountain Avenue, Murray Hill, NJ 07974.

References

[1] F. Lustenberger, M. Helfenstein, H.-A. Loeliger, F. Tarköy, and G. S. Moschytz, "All-Analog decoder for a binary (18,9,5) tailbiting trellis code," *Proc. European Solid-State Circuits Conference*, pp. 362–365, Duisburg, September 1999.

[2] M. Moerz, T. Gabara, R. Yan, and J. Hagenauer, "An analog 0.25μm BiCMOS tailbiting MAP decoder," *IEEE Proc. International Solid-State Circuits Conference*, pp. 356–357, San Francisco, February 2000.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On Fix-Free Codes

Chunxuan Ye
Dept. of Information Engineering
The Chinese Univ. of Hong Kong
Shatin, New Territories
Hong Kong, China
e-mail: cxye7@ie.cuhk.edu.hk

Raymond W. Yeung
Dept. of Information Engineering
The Chinese Univ. of Hong Kong
Shatin, New Territories
Hong Kong, China
e-mail: whyeung@ie.cuhk.edu.hk

Abstract — **We prove a sufficient and a necessary condition on the existence of fix-free codes, and give a few new upper bounds on the redundancy of optimal fix-free codes.**

I. Introduction

In fix-free codes, no codeword is a prefix or a suffix of any other codeword. This kind of codes has several applications [1]. For example, a file compressed by fix-free codes can be decoded in the forward direction and the reverse direction simultaneously, thus reducing the decoding time to half compared with decoding in one direction only.

II. Main results

Consider a code with n codewords. The lengths of these codewords form a vector $(l_1, \cdots, l_k, \cdots, l_n)$, where l_k is the length of the kth codeword. We assume without loss of generality that $l_1 \le l_2 \le \cdots \le l_n$, and use $\overrightarrow{l_n}$ to denote this ordered set of codeword lengths. Let $h(i)$ be the smallest h^* such that $l_{h^*} = l_{i+1}$. Define $(x)^+$ as the positive part of a real number x, i.e.,

$$(x)^+ = \begin{cases} x, & \text{if } x \ge 0, \\ 0, & \text{if } x < 0. \end{cases}$$

Our main results in [2] are summarized below.

Theorem 1 *(Sufficient Condition) For a set of codeword lengths $\overrightarrow{l_n}$, define*

$$s_l(\overrightarrow{l_n}) = \prod_{i=1}^{n-1}(1 - 2\sum_{1\le j\le i} 2^{-l_j} + [i+1-h(i)]\cdot 2^{-l_{i+1}} + \sum_{\substack{1\le j,k\le h(i)-1 \\ s.t.\ l_j+l_k\le l_{i+1}}} 2^{-l_j-l_k})^+.$$

If $s_l(\overrightarrow{l_n}) > 0$, there exists a fix-free code with lengths $\overrightarrow{l_n}$.

Corollary 1 *Let $\overrightarrow{l_n}$ be a set of codeword lengths. If*

$$\sum_{1\le j\le n} 2^{-l_j} < \frac{1}{2} + \frac{n+2-h(n-1)}{2}\cdot 2^{-l_n},$$

then there exists a fix-free code with lengths $\overrightarrow{l_n}$.

Corollary 2 *Let $\overrightarrow{l_n}$ be a set of codeword lengths. If*

$$\sum_{1\le j\le n} 2^{-l_j} \le \frac{1}{2},$$

then there exists a fix-free code with lengths $\overrightarrow{l_n}$.

Corollary 3 *Let $\overrightarrow{l_n}$ be a set of codeword lengths. If $l_1 = 1$, then*

$$\sum_{1\le j\le n} 2^{-l_j} \le \frac{5}{8}$$

implies the existence of a fix-free code with lengths $\overrightarrow{l_n}$.

Theorem 2 *(Necessary Condition) For a set of codeword lengths $\overrightarrow{l_n}$, define*

$$s_u(\overrightarrow{l_n}) = \prod_{i=1}^{n-1}(1 - 2\sum_{1\le j\le i} 2^{-l_j} + [i+1-h(i)]\cdot 2^{-l_{i+1}} + \sum_{1\le j,k\le h(i)-1} 2^{(l_{i+1}-l_j-l_k)^+ - l_{i+1}})^+.$$

If $s_u(\overrightarrow{l_n}) = 0$, no fix-free code with lengths $\overrightarrow{l_n}$ exists.

Theorem 3 *For a set of codeword lengths $\overrightarrow{l_n}$, if for $1 \le i \le n-1$, either $l_i = l_{i+1}$ or $2l_i \le l_{i+1}$, then there exists a fix-free code with lengths $\overrightarrow{l_n}$ if and only if*

$$\prod_{i=1}^{n-1}(1 - 2\sum_{1\le j\le i} 2^{-l_j} + [i+1-h(i)]\cdot 2^{-l_{i+1}} + \sum_{1\le j,k\le h(i)-1} 2^{-l_j-l_k})^+ > 0.$$

Let q, p_1 and p_n be the probability of any given source symbol, the probability of the most likely source symbol and the probability of the least likely source symbol, respectively. Denote R as the redundancy of an optimal fix-free code.

Theorem 4

$$R < \begin{cases} 2 - H_b(q) - (1-q)\log(1 - 2^{-\lceil -\log q\rceil}) \\ \quad -q(1 - \lceil -\log q\rceil), & \text{if } q < 0.5, \\ 4 - 3q - H_b(q), & \text{if } q \ge 0.5. \end{cases}$$

Corollary 4 *For any fixed n, where n is the size of the source alphabet, it is impossible to construct a sequence of source distributions for which R tends to 2.*

Theorem 5

$$R < min[4 - 3p_1 - H_b(p_1), 2 - H_b(p_1) - (1-p_1)\log(1 - 2^{-\lceil -\log p_1\rceil}) - p_1(1 - \lceil -\log p_1\rceil)].$$

Theorem 6

$$R \le 2 - H_b(p_n) - (1-p_n)\log(1 - p_n + 2^{-\lceil -\log p_n\rceil}) - p_n(1 - \lceil -\log p_n\rceil).$$

References

[1] J. L. Peterson, "Computer programs for detecting and correcting spelling errors," *Comm. ACM*, 23, pp. 676-687, 1980.

[2] C. Ye and R. W. Yeung, "Some basic properties of fix-free codes," Accepted by IEEE Trans. Infoem. Theory,.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Variable-rate Codes for Synchronization with Timing*

Navin Kashyap and David L. Neuhoff
EECS Dept., University of Michigan
Ann Arbor, MI 48109-2122, USA
{nkashyap,neuhoff}@eecs.umich.edu

Abstract — **This paper proposes and analyzes variable-rate sync-timing codes that resynchronize after the encoded bits are corrupted by insertions, deletions or substitution errors, and also produce estimates of the time indices of the decoded data.**

I. Introduction

Information theory, which has traditionally focused on encoding data values, has apparently overlooked the problem of encoding data time indices. The latter is necessary in most situations where conventional data synchronization is needed, *i.e.*, when the encoded bit stream is corrupted by insertions, deletions or substitution errors. For example, suppose an infinite sequence of temperatures, $43, 64, 27, 54, 36, 42, 73, 45, \ldots$, corresponding to cities Det, LA, Chi, Bos, NY, StL, Mia, Bal,..., is encoded into an infinite sequence of bits, which a decoder must begin decoding midstream, at some arbitrary point. Since the decoder does not initially know how to parse the arriving bits into codewords, it will ordinarily produce erroneous outputs, until at some point, it acquires synchronization and produces correct outputs from then on. For example, if it produces $73, 40, 54, 36, 42, 73, 45, \ldots$, then it has acquired sync when producing "54". However, the decoded data is of limited value because the correspondence between temperatures and cities has been lost. What is needed is a system that encodes data time indices, as well as data values, so that the decoder produces estimates of both, *i.e.*, a sequence of temperature and time index pairs, like $(73, 12), (40, 7), (54, 4), (36, 5), (42, 6), (73, 7), (45, 8), \ldots$. We refer to codes that encode and decode data time indices, as well as data values, as *sync-timing codes*. They are essential in video coding, where they ensure frame-sync, as well as audio-video sync.

While conventional sync codes have been much studied (*cf.* [1]), only *ad hoc* techniques have been developed for sync-timing, *e.g.* the marker systems in JPEG and MPEG. Indeed, the sync-timing problem has only recently been identified as such, and only recently has a theory begun to emerge [2]. However, the theory in [2] applies only to fixed-rate schemes, whereas source codes are often variable-rate, and such codes are the most sensitive to errors. In this paper, we initiate a theory of variable-rate sync-timing codes by introducing a family of such codes and analyzing them on the basis of the performance measures used in [2]: coding rate, resynchronization delay and timing span (which measures the code's ability to reproduce time indices). We find that the asymptotic performance of the variable-rate sync-timing codes studied here is the same as that of the best known fixed-rate codes.

II. A variable-rate sync-timing code

Here, we describe a variable-rate sync-timing encoder that is designed to follow a binary source encoder that maps blocks of k source symbols into codewords with average length $k\overline{L}$. The output of the sync-timing encoder, in response to a source codeword, is a *sync-timing codeword* that consists of one of p distinct *markers*, followed by the source codeword after it has undergone *bitstuffing*, followed by a zero. The marker prefixed to the jth "bitstuffed" codeword comprises a *flag* of m_1 consecutive ones (denoted by 1^{m_1}), followed by a zero, followed by a *block index codeword* for $j-1 \bmod p$, followed by another zero. The block index codewords are p distinct binary sequences of length m_2, each of which does not contain the flag. Bitstuffing prevents the appearance of a flag in each source codeword by "stuffing" a zero immediately after each occurrence of 1^{m_1-1} in the codeword, the idea being that the flag can then be used for synchronization purposes. The structure of this variable-rate sync-timing code is similar to that of the cascaded code described in [2]. Note that the source encoder could be lossless or lossy, and it need not process blocks independently.

The decoder locates the flags in the stream of received bits, and for each flag found, it reverses (if possible) the encoding procedure on the sequence up to the next flag. Thus, every successful reversal of the encoding yields the integer j encoded by the block index codeword, and the reproductions of the k source symbols encoded by the source codeword. The ith source symbol decoded receives the time index $jk+i$. Since $j \leq p-1$, the time indices produced by the decoder are modulo-kp reductions of the actual time indices of the data.

We measure the performance of this code in terms of delay, rate and timing span, as defined in [2], after modifying their definitions slightly to account for the variable-rate nature of this code. Thus, we define resynchronization *delay* to be the average length of a sync-timing codeword, so that $D = m_1 + m_2 + k(\overline{L}+\overline{S})+3$, where $k\overline{S}$ is the average number of stuffed bits added per codeword. *Rate*, $R = k\overline{L}/D$, is a measure of the redundancy introduced by the sync-timing encoder. Finally, the *timing span* of the code, $T = kp$, is a measure of the code's ability to reproduce time indices. We want D to be small, R to be close to 1, and T to be large. Let $T(r,d)$ denote the maximum timing span achievable by such a code with rate at least r and delay at most d. The following theorem shows that the rate of growth of $T(r,d)$ with d has the same asymptotic form as that for fixed-rate codes (*cf.* [2]).

Theorem: For $r \in (0,1)$, (i) for any $d > 0$, $T(r,d) \leq (d/\overline{L})\, 2^{d(1-r)}$, (ii) for any $\epsilon > 0$, there exists $d(r,\epsilon) > 0$ such that for all $d > d(r,\epsilon)$, $T(r,d) \geq rd/(\overline{L}(1+\epsilon))\, 2^{d(1-r)/(1+\epsilon)}$, and (iii) $\lim_{d\to\infty}(\log_2 T(r,d))/d = 1-r$.

*This work was supported by NSF Grant NCR-9415754.

References

[1] R.A. Scholtz, "Frame synchronization techniques," *IEEE Trans. Commun.*, vol. 28, no. 8, pp. 1204–1212, Aug. 1980.

[2] N. Kashyap and D.L. Neuhoff, "Data Synchronization with Timing," submitted to *IEEE Trans. Inform. Theory*. Available via anonymous FTP at `ftp.eecs.umich.edu/people/neuhoff/sync_timing.submit.ps`.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Error Containment in Compressed Data Using Sync Markers

Aaron Kiely*, Sam Dolinar*, Matthew Klimesh*, and Adina Matache*
Jet Propulsion Laboratory, California Institute of Technology
4800 Oak Grove Drive, Mail Stop 238-420, Pasadena, CA 91109
e-mail: {aaron, sam, klimesh, matache}@shannon.jpl.nasa.gov

Abstract — **We examine a specific strategy of using sync markers for error containment in compressed data, using a model that separates the data compression and error containment stages.**

I. A Simple Error Containment Scheme

Consider a data compressor that maps blocks of source symbols to variable length binary sequences. At the output of the compressor, we assume that zeros and ones are equally likely and that an error at this point would be undetectable to the decompressor. To limit the effect of channel errors we use a special sequence called a sync marker. The length m sync marker s is inserted between compressed blocks so that block boundaries can be identified following a channel error. To prevent the chance occurrence of the sync marker within the compressed data sequence, we insert a bit whenever we observe the first $m-1$ bits of the sync marker.

Our aim is to determine how to choose sync markers and analyze the impact on overall performance of this strategy. A complete version of these results is available in [2]. Related work includes [1, 3].

II. Error Containment Performance

The bit insertion procedure can be described using a state diagram that is essentially the same as that in [1]. The expected total number of bits $I_n(s)$ inserted in a block of n compressed bits can be computed from the transition matrix for the state diagram [2].

Two length m sync markers s and t are said to be *equivalent* if they give identical performance in the error containment scheme, i.e., when $I_n(s) = I_n(t)$ for all $n > 0$. Two equivalent sync markers can have very different state diagrams.

We define the overlap set of the bit string $s = s_1 s_2 \ldots s_m$ as $V(s) = \{1 \le i < m : s_1 \ldots s_i = s_{m-i+1} \ldots s_m\}$. In other words, $i \in V(s)$ if s can be written twice with i identical bits overlapping. Let $V'(s)$ denote the overlap set of s with the last bit inverted.

Theorem 1 *If s and t are length m sync markers for which $V(s) = V(t)$ and $V'(s) = V'(t)$, then s and t are equivalent.*

The asymptotic growth rate of the average number of inserted bits $I_n(s)$ can be neatly evaluated for any sync marker s:

Theorem 2 *If s is a length m sync marker, then*

$$\lim_{n\to\infty} \frac{1}{n} I_n(s) = \left(2^{m-1} - 1 + \sum_{i\in V(s)} 2^{i-1} - \sum_{i\in V'(s)} 2^{i-1}\right)^{-1}.$$

*The work described was funded by the TMOD Technology Program and performed at the Jet Propulsion Laboratory, California Institute of Technology under contract with the National Aeronautics and Space Administration.

Given a blocklength n, for any fixed sync marker length $m \le 8$, we have verified empirically (and we conjecture that it is true for all m) that the optimal sync marker must belong to one of three classes. These classes are those containing 10^{m-1}, $10^{m-2}1$, and 1^m, which we refer to as class-1, class-2, and class-3, respectively.

Theorem 3 *For class-1, class-2, and class-3 sync markers, the average number of inserted bits $I_n(s)$ takes the following form wherever it is nonzero:*

$$I_n(s) = \frac{n}{a(s)} + b(s) + c_n(s)2^{-n},$$

where $a(s)$, $b(s)$ are independent of n, and $c_n(s)$ is periodic in n with a short period on the order of the length of s. Expressions for $a(s)$, $b(s)$, and $c_n(s)$ are given in [2] for each of the three special classes.

To compare the performance of sync markers of different lengths, we compute the average *data expansion*, i.e., the average number of extra bits that are added to each data block for synchronization purposes. The average data expansion is $X_n(s) = |s| + I_n(s)$ where $|s|$ denotes the length of sync marker s. In Figure 1 we plot the difference between the globally optimum average data expansion $\min_s X_n(s)$ and $\log_2 n$.

For large n, class-1 and class-2 markers take approximately equal turns at being optimum, and the globally optimum average data expansion is confined to a tight range of values between $\log_2 n + 1.9$ and $\log_2 n + 2$. Class-3 markers, while asymptotically optimum for any *fixed* marker length m, are never globally optimum.

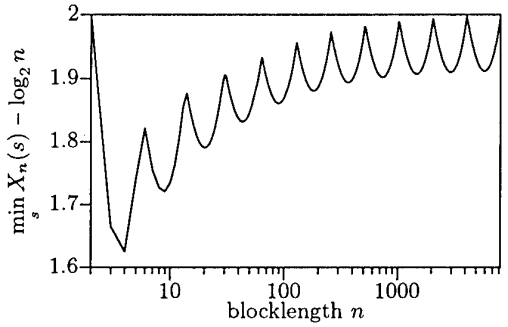


Figure 1: Globally minimum average data expansion, $\min_s X_n(s)$, plotted as a difference relative to $\log_2 n$.

References

[1] E. N. Gilbert, "Synchronization of Binary Messages," *IRE Trans. Inform. Theory*, vol. IT-6, pp. 470–477, 1960.

[2] A. Kiely, S. Dolinar, M. Klimesh, A. Matache, "Synchronization Markers for Error Containment in Compressed Data," *TMO Progress Report 42-136*, Oct.-Dec. 1998, pp. 1-40, Feb. 15, 1999. http://tmo.jpl.nasa.gov/tmo/progress_report/42-136/136H.pdf

[3] J. J. Stiffler, *Theory of Synchronous Communications*, Prentice-Hall, Englewood Cliffs, New Jersey, 1971.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Error Recovery for Ziv-Lempel Coding by Using UEP Schemes

Eiji FUJIWARA, Hongyuan CHEN and Masato KITAKAMI
Graduate School of Information Science and Engineering, Tokyo Institute of Technology
2-12-1 O-okayama, Meguro-ku, Tokyo, 152-8552 JAPAN
Email: fujiwara@cs.titech.ac.jp

I. Introduction

Lossless data compression, such as arithmetic coding and Ziv-Lempel coding, is widely used for text compression[1]. Since errors in compressed data give serious influence to the decompression, error control for compressed data is necessary. From this point, the authors proposed burst error recovery in arithmetic coding[2]. This paper proposes error recovery schemes for LZW coding and LZ77 coding[1] by using Unequal Error Protection (UEP) schemes, which protect the important parts of the compressed data more strongly.

II. Error Recovery for LZW Coding

Let the input alphabet[1] contain q characters. Initially, the dictionary contains q distinct phrases each of which corresponds to one character in the input alphabet. A phrase is a word, part of a word, or several words[1]. The compressor searches the dictionary for a phrase which matches the input and dispenses the pointer of the phrase. At the same time, a new phrase is parsed and added into the dictionary until the number of phrases reaches its limit. Let the size of the dictionary be M phrases. Then the length of the pointer is $\lceil \log_2 M \rceil$ bits, where $\lceil x \rceil$ is the smallest integer greater than or equal to x, and the first $(M-q)$ pointers are used to rebuild the dictionary in decompression. Thus the former part is more important than the latter part and should be more strongly protected.

The algorithm of the proposed scheme is as follows.

(1) Divide the compressed data into two parts, where the former part consists of the first $(M-q) \times \lceil \log_2 M \rceil$ bits and the latter part consists of the remaining compressed data.

(2) Apply t_1 bytes error correcting code to the former part and t_2 bytes error correcting code to the remaining latter part, where $t_1 > t_2$.

Fig. 1 shows the relation between error location in the compressed data and relative amount of errors occurred in the decompressed data in the proposed scheme with $M = 8192$, $q = 256, t_1 = 5$ and $t_2 = 1$. The source file is "paper1"[1]. The check bit length is 116 bits and 48-bit burst errors are injected. The relative amount of errors is given by calculating the percentage of erroneous lines to total number of lines. Here, a line shows a group of phrases separated with each other by "return mark". For comparison, the cases of applying the conventional four bytes error correcting code with the same number of check bits as that of the proposed UEP scheme, denoted as "4bEC", to the whole compressed data as well as of no error correcting code, denoted as "Without ECC", are also shown. Fig. 1 says that the proposed scheme is more efficient to control errors than the conventional error control coding. Simulation results for other source files are similar to this.

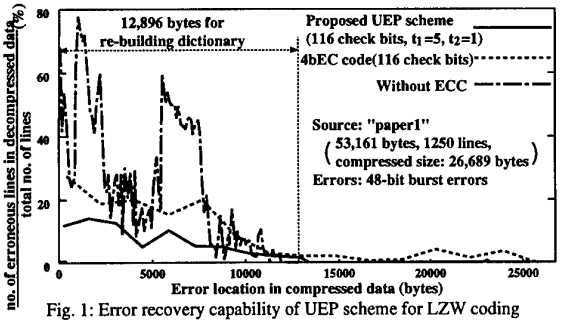


Fig. 1: Error recovery capability of UEP scheme for LZW coding

III. Error Recovery for LZ77 Coding

Compressor of LZ77 coding searches a fixed-size sliding window for the longest phrases which matches the current input. In the i-th match, compressor dispenses a fixed-length pointer (o_i, f_i, u_i), where o_i is the offset of the match, f_i the matched length and u_i the first character which does not match. In decompression of the i-th pointer, the decompressor copies a f_i-symbol phrase from the position indicated by o_i and shifts the copied phrase as well as the character u_i into the sliding window and the output buffer.

The influence of errors occurring in f_i's is quite different from those in o_i's or u_i's. If error is in f_i's, the length of copied phrase is changed. It affects the window shift, i.e., o_i's of the following pointers will indicate the phrases different from the correct ones. Hence, all the following decoded phrases are corrupted. Simulation shows that an error in f_i's averagely gives over 40 times larger damage than that in o_i's or u_i's. In addition, errors in f_i's located in the former part of the compressed data give more serious influence than those in the latter part. Thus, algorithm of the proposed scheme is as follows.

(1) Group the compressed output (o_1, f_1, u_1), (o_2, f_2, u_2), ..., (o_n, f_n, u_n) into two sequences $\{o_1, u_1, o_2, u_2, ..., o_n, u_n\}$ and $\{f_1, f_2, ..., f_n\}$.

(2) Apply l_1-bit burst error correcting code to $\{o_1, u_1, o_2, u_2, ..., o_n, u_n\}$.

(3) Apply l_2-bit burst error correcting code to $\{f_1, f_2, ..., f_{\lfloor n/2 \rfloor}\}$ and l_3-bit burst error correcting code to $\{f_{\lfloor n/2 \rfloor+1}, f_{\lfloor n/2 \rfloor+2}, ..., f_n\}$. Here, $l_2 > l_3$.

(4) Append the check bits obtained in Steps (2) and (3) at the end of the compressed data.

Fig. 2 shows the relation between error location in the compressed data and relative amount of errors occurred in the decompressed data in the the proposed scheme with $l_1 = 16$, $l_2 = 12$ and $l_3 = 8$. The source file is "paper1"[1]. The check bit length is 105 bits and 48-bit burst errors are injected. The results of Fig. 2 are obtained in the same way as that in Fig. 1. For comparison, the cases of applying the 40-bit burst error correcting Fire code with 119 check bits as well as of no error correcting code, denoted as "Without ECC", are also shown. Fig. 2 says that the proposed scheme is more powerful to control errors than applying the 40-bit burst error correcting Fire codes. Simulation results for other source files also lead to the similar conclusion.

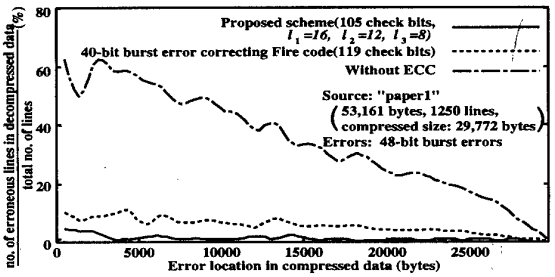


Fig. 2: Error recovery capability of UEP scheme for LZ77 coding

References

[1] T.C. Bell et al. *Text Compression* Prentice-Hall, Inc., 1990.

[2] H. Chen, M. Kitakami and E. Fujiwara, "Burst Error Recovery Method for VF Arithmetic Codes", *Proceedings of 1999 IEEE ITW*, South Africa, pp.124, June 20-25 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Optimal Encoding Over Uncertain Channels with Decoding Delay Constraints

Philip A. Whiting
Bell Laboratories
Lucent Technologies
600 Mountain Ave. Rm. 2C-317
Murray Hill, NJ 07974
e-mail: pawhiting@lucent.com

Edmund M. Yeh
Dept. of Electrical Engineering
Mass. Institute of Technology
77 Mass. Ave. Rm 35-303
Cambridge, MA 02139
email: emyeh@mit.edu

Abstract — **We examine communication over block fading additive Gaussian channels with delayed channel state information feedback and finite decoding delay constraints. Following an approach due to Cover [1], we apply the broadcast strategy and find the maximum achievable expected rate in cases where the underlying parallel Gaussian broadcast channels are not degraded in the same direction.**

I. Introduction

Consider a single user communicating over a discrete time additive Gaussian noise channel where the noise variance stays constant over a block of N symbols but may vary from block to block. The channel model over the kth block ($k \in \mathbb{Z}$) is

$$\boldsymbol{Y}_k = \boldsymbol{X}_k + \boldsymbol{Z}_k \tag{1}$$

where $\boldsymbol{X}_k = (X_{k1}, \ldots, X_{kN})$ and $\boldsymbol{Y}_k = (Y_{k1}, \ldots, Y_{kN})$ are vectors in $\mathbb{R}^N$ representing the inputs and outputs of the channel over the kth block. $\boldsymbol{Z}_k$ is a Gaussian random vector with mean zero and covariance matrix $S_k I$. Assume that the noise variance process $\{S_k\}$ is stationary ergodic and that $\mathcal{S}$, the state space of $\{S_k\}$, is a finite subset of $\mathbb{R}$. The $\boldsymbol{Z}_k$'s are assumed to be independent. This is an equivalent model for a version of the *block fading channel.* For convenience, we refer to (1) as the *block Gaussian channel* (BGC).

Assume that during the kth block, the receiver has perfect knowledge of the noise variances $S_{-\infty}^{k} \triangleq (\ldots, S_{k-1}, S_k)$, while the transmitter has perfect knowledge only of $S_{-\infty}^{k-d}$, where $d \geq 1$, via delayed noiseless feedback. Next, suppose the system has a maximum allowable decoding delay of KN symbols ($K \in \mathbb{N}$). The goal is to maximize the *expected rate* (expectation is over the fading process $\{S_k\}$) over the BGC subject to the decoding delay constraint and an average power constraint $\frac{1}{KN}\sum_{k=1}^{K}\sum_{n=1}^{N}\mathbb{E}\left[X_{kn}^2\right] \leq P$.

II. Decoding Delay of One Block ($K = 1$)

For the one block case, we show that the maximum expected rate per block is attained by a broadcast strategy which associates noise variance levels in the BGC with corresponding receivers in a degraded broadcast channel. The optimal power splitting parameters are chosen according to the conditional probabilities of the current channel state given all previous channel states.

Theorem 1 *Consider a BGC with an average transmit power constraint P and noise power varying according to a stationary ergodic process $\{S_k, k \in \mathbb{Z}\}$ with state space $\mathcal{S} = \{\eta_1, \ldots, \eta_L\}$, $\eta_1 > \eta_2 > \ldots > \eta_L$. Suppose the decoding delay constraint is N symbols and noiseless channel state feedback to the transmitter is delayed by d blocks. If arbitrarily small error probability is required, the expected rate per block satisfies*

$$\mathbb{E}_{S_{-\infty}^{k}}[R] \leq \mathbb{E}_{S_{-\infty}^{k-d}}\left[\sum_{l=1}^{L} Q_l\left(S_{-\infty}^{k-d}\right) C\left(\frac{\alpha_l^*(S_{-\infty}^{k-d})P}{\sum_{j>l}\alpha_j^*(S_{-\infty}^{k-d})P + \eta_l}\right)\right]$$

where $Q_l\left(S_{-\infty}^{k-d}\right) \triangleq \sum_{j=l}^{L} P\left(S_k = \eta_j | S_{-\infty}^{k-d}\right)$, and $\boldsymbol{\alpha}^*(s_{-\infty}^{k-d}) = \left(\alpha_1^*\left(s_{-\infty}^{k-d}\right), \ldots, \alpha_L^*\left(s_{-\infty}^{k-d}\right)\right)$ maximizes

$$\sum_{l=1}^{L}\left[\sum_{j=l}^{L} P\left(S_k = \eta_j | S_{-\infty}^{k-d} = s_{-\infty}^{k-d}\right)\right] C\left(\frac{\alpha_l P}{\sum_{j>l}\alpha_j P + \eta_l}\right)$$

subject to $\alpha_l \geq 0, \sum_{l=1}^{L}\alpha_l = 1$.

III. Decoding Delay of Two Blocks ($K = 2$)

The main challenge in extending Theorem 1 to the case of $K > 1$ is that unlike the one-block case, the underlying parallel Gaussian broadcast channels for $K > 1$ are in general not degraded in the same direction. Nevertheless, we extend El Gamal's work [2] on the capacity region for the two-receiver two-parallel Gaussian broadcast channel with common information to conclude that the broadcast strategy remains optimal for the the case of a two state i.i.d. BGC with $K = 2$.

Theorem 2 *Consider a two-state i.i.d. BGC with noise variance $S = \eta_1$ with probabilty q and $S = \eta_2$ w.p. $1 - q$. Let the average transmit power constraint be P and the decoding delay constraint be two N-blocks. If arbitrarily small error probability is required, the expected rate per block satisfies*

$$\begin{aligned}\mathbb{E}[R] \quad \leq \quad & \frac{1}{2}(1-q^2)\left[C\left(\frac{\alpha_2^* P}{\eta_1 + \alpha_3^* P}\right) + C\left(\frac{\alpha_2^* P}{\eta_2 + \alpha_3^* P}\right)\right] \\ & + C\left(\frac{\alpha_1^* P}{\eta_1 + \overline{\alpha_1^*} P}\right) + (1-q)^2 C\left(\frac{\alpha_3^* P}{\eta_2}\right)\end{aligned} \tag{2}$$

where $\overline{\alpha} \triangleq 1 - \alpha$, and $\boldsymbol{\alpha}^* = (\alpha_1^*, \alpha_2^*, \alpha_3^*)$ maximizes the RHS in (2) in $\boldsymbol{\alpha}$ subject to $\alpha_i \geq 0, i = 1, 2, 3$ and $\sum \alpha_i = 1$.

References

[1] T. Cover. "Broadcast Channels." *IEEE Trans. Information Theory*, Vol. 18, No. 1, pp. 1-14, January 1972.

[2] A. El Gamal. "Capacity of the Product and Sum of Two Unmatched Broadcast Channels." *Problems of Information Transmission*, Vol. 16, No. 1, January-March 1980, pp. 1-16.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Competitive Equilibrium in the Gaussian Interference Channel

Wei Yu[1] and John M. Cioffi
Electrical Engineering Department
Stanford University, Stanford, CA 94305, U.S.A.
e-mail: weiyu@stanford.edu

Abstract — **A game theory formulation for the Gaussian interference channel is given under the assumption that no interference subtraction is performed. The existence, uniqueness and stability of a pure strategy Nash equilibrium is established under a mild-interference condition,**

I. Introduction

In a Gaussian interference channel, two independent sender-receiver pairs attempt to communicate in the presence of interference from each other. The capacity region for the interference channel is still an open problem. The largest rate region presently known is achieved with superposition coding and interference subtraction [1], but its optimality is not yet known. However, the traditional view of the interference channel allows the two senders, while remaining independent, to be cooperative in their respective coding strategies. If such cooperation cannot be assumed, the interference channel becomes a non-cooperative game. This paper studies the interference channel from this game theory perspective. We focus on Gaussian interference channels with memory, but make the simplifying assumption that no interference subtraction is performed regardless of interference strength. We ask the following questions: if each sender's sole objective is to maximize its *own* data rate, can an equilibrium be achieved in a competitive environment? If so, is such an equilibrium unique?

II. Competitive Equilibrium

The two senders in a Gaussian interference channel,

$$\mathbf{y}_1 = \mathbf{x}_1 + A_2\mathbf{x}_2 + \mathbf{n}_1 \quad (1)$$

$$\mathbf{y}_2 = \mathbf{x}_2 + \mathcal{A}_1\mathbf{x}_1 + \mathbf{n}_2, \quad (2)$$

are considered as two players in a game. The channel transfer functions are normalized to unity. The square magnitude of the interference transfer functions $\mathcal{A}_1$ and $\mathcal{A}_2$ are denoted as $\alpha_1(f)$ and $\alpha_2(f)$. Let $N_1(f)$ and $N_2(f)$ denote noise power spectrum densities. The structure of the game, i.e., the interference coupling functions and noise power, are common knowledge to both players. A strategy[2] for each player is its transmit power spectrum, $P_1(f)$ and $P_2(f)$, subject to the power constraints $\int_0^F P_1(f)df \le \mathbf{P}_1$, and $\int_0^F P_2(f)df \le \mathbf{P}_2$, respectively. The payoffs are data rates :

$$R_1 = \int_0^F \log\left(1 + \frac{P_1(f)}{N_1(f) + \alpha_2(f)P_2(f)}\right) df, \quad (3)$$

$$R_2 = \int_0^F \log\left(1 + \frac{P_2(f)}{N_2(f) + \alpha_1(f)P_1(f)}\right) df, \quad (4)$$

where bandwidth up to F is used. The game is not zero-sum. We are interested in characterizing its pure strategy Nash equilibrium.

[1]This work was supported by a Stanford Graduate Fellowship.
[2]Only pure (or deterministic) strategy is considered here.

A Nash equilibrium is a strategy profile in which each player's strategy is an optimal response to the other player's strategy [2]. For the interference channel, the optimal response for a player is the waterfilling of its power with respect to the combined noise and interference. If the power distributions are such that waterfilling is achieved simultaneously for both players, a Nash equilibrium is reached. At a Nash equilibrium, neither player has an incentive to move away from its present power distribution.

Theorem: Suppose that $\sup_f \alpha_1(f) \cdot \sup_f \alpha_2(f) < 1$, then a pure strategy Nash equilibrium in the Gaussian interference game exists, is unique, and is stable.

Proof: The first idea is to recognize that if $\alpha_1(f)\cdot\alpha_2(f) < 1$ $\forall f$, there is a Nash equilibrium corresponding to every water level (K_1, K_2). For fixed (K_1, K_2), the Nash equilibrium $(P_1(f), P_2(f))$ is found by solving the waterfilling condition:

$$P_1(f) + \alpha_2(f)P_2(f) + N_1(f) = K_1 \quad (5)$$

$$P_2(f) + \alpha_1(f)P_1(f) + N_2(f) = K_2, \quad (6)$$

unless $\alpha_1(f) > \frac{K_2 - N_2(f)}{K_1 - N_1(f)}$, in which case $P_1(f) = \max\{0, (K_1 - N_1(f))\}$ and $P_2(f) = 0$, or $\alpha_2(f) > \frac{K_1 - N_1(f)}{K_2 - N_2(f)}$, in which case $P_2(f) = \max\{0, (K_2 - N_2(f))\}$ and $P_1(f) = 0$.

Next, we establish that for a given power constraint $(\mathbf{P}_1, \mathbf{P}_2)$, there exists (K_1, K_2) whose Nash equilibrium has exactly this power. For each (K_1, K_2), denote the power level at the corresponding Nash equilibrium as $(\mathbf{P}_{K_1}, \mathbf{P}_{K_2})$. Observe that when $\alpha_1(f) \cdot \alpha_2(f) < 1$, if $K_1 < K_1'$ and $K_2 = K_2'$, then $\mathbf{P}_{K_1} \le \mathbf{P}_{K_1'}$ and $\mathbf{P}_{K_2} \ge \mathbf{P}_{K_2'}$. Now, start with $K_1 = K_2 = 0$. Increase K_1 until $\mathbf{P}_{K_1} = \mathbf{P}_1$, then increase K_2 until $\mathbf{P}_{K_2} = \mathbf{P}_2$. But then, we have $\mathbf{P}_{K_1} \le \mathbf{P}_1$ by observation. So, we can increase K_1 again, until $\mathbf{P}_{K_1} = \mathbf{P}_1$, then increase K_2, etc. The increasing sequences of K_1's and K_2's converge because they cannot go to infinity with finite power constraints. The limit point is a Nash equilibrium corresponding to $(\mathbf{P}_1, \mathbf{P}_2)$.

To prove uniqueness, let $(P_1^N(f), P_2^N(f))$ be the power distribution at a Nash equilibrium. Start with any power distribution $P_1^{(0)}(f)$ that satisfies the power constraint. Waterfill for $P_2^{(0)}(f)$, assuming $P_1^{(0)}(f)$ as interference. Then, waterfill for $P_1^{(1)}(f)$, assuming $P_2^{(0)}(f)$ as interference, etc. This iterative waterfiling process coverges in $\mathbf{L}_1$-norm $\int_0^F |P_1^{(k)} - P_1^N|df$ because $\max(||(P_1^{(k+1)} - P_1^N)_+||_1, ||(P_1^{(k+1)} - P_1^N)_-||_1) \le \sup\alpha_2(f) \cdot \max(||(P_2^{(k)} - P_2^N)_+||_1, ||(P_2^{(k)} - P_2^N)_-||_1) \le \sup\alpha_2(f)\sup\alpha_1(f)\cdot\max(||(P_1^{(k)} - P_1^N)_+||_1, ||(P_1^{(k)} - P_1^N)_-||_1)$, which is a contraction by the assumption that $\sup\alpha_1(f) \cdot \sup\alpha_2(f) < 1$. So, $P_1^{(k)} \to P_1^N$ in $\mathbf{L}_1$-norm as $k \to \infty$. □

References

[1] T.S. Han, K. Kobayashi, "A New Achievable Rate Region for the Interference Channel," *IEEE Trans. Info. Theory*, vol. 27, pp. 49–60, January 1981.

[2] D. Fudenberg and J. Tirole, *Game Theory*, MIT Press, 1991.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Capacity-Achieving Distributions for Non-Gaussian Additive Noise Channels

Arnab Das
Bell Laboratories
Lucent Technologies
Holmdel, NJ 07733
e-mail: arnab@lucent.com

Abstract —

We characterize the capacity-achieving distribution for a class of non-Gaussian additive noise channels, when the transmitter is subject to an "average" power constraint. Specifically, we show that if the probability density function of the noise, in addition to satisfying some mild technical conditions, has a tail which decays at a rate slower (resp. faster) than the Gaussian, then the capacity-achieving distribution has bounded (resp. unbounded) support.

I. Preliminaries

Consider a (discrete-time) additive noise channel where the $\mathbb{R}$-valued output corresponding to an $\mathbb{R}$-valued input x_t is given by

$$Y_t = x_t + Z_t, \quad t \geq 1, \tag{I.1}$$

where $\{Z_t\}_{t=1}^{\infty}$ is the $\mathbb{R}$-valued i.i.d. noise with $\mathbb{E}[Z_t] = 0$, and $\mathbb{E}[(Z_t - \mathbb{E}[Z_t])^2] = \sigma_z^2$.

Assume that the distribution of the rv Z_t admits a probability density function (pdf) p_Z with respect to the Lebesgue measure. Then, for any $\mathbb{R}$-valued channel input rv X_t with distribution Q, let p_Y^Q denote the resulting pdf of the output rv Y_t. The capacity of the channel in (I.1), subject to an average power constraint $\mathcal{P}_0 < \infty$, denoted $C(\mathcal{P}_0)$, is given as

$$C(\mathcal{P}_0) = \max_{Q\,:\,\mathbf{E}_Q[X_t^2] \leq \mathcal{P}_0} I(Q), \tag{I.2}$$

where $I(Q) \triangleq I(X_t \wedge Y_t)$.

Let the marginal entropy density (cf. e.g., Smith (1969)) be given by

$$\mathbb{h}(x;Q) = -\int_{-\infty}^{\infty} p_Z(y-x)\log p(y;Q)dy, \quad x \in \mathbb{R},\ Q \in \mathcal{A} \tag{I.3}$$

where $\mathcal{A}$ denotes the set of all distributions of the $\mathbb{R}$-valued rv X_t.

Next, we consider three kinds of noise rv with pdf p_Z in (I.1): heavy-tailed, light-tailed and bounded.

A noise rv Z_t will be called *heavy-tailed* if its pdf p_Z satisfies the following conditions:

(A1) it is uniformly continuous;

(A2) for $Q_1, Q_2 \in \mathcal{A}$, it holds that if $p_Y^{Q_1}(y) = p_Y^{Q_2}(y)$, $y \in \mathbb{R}$, then $Q_1 = Q_2$;

(H1) there exist (finite) positive constants k_1, k_2 and ρ_h, $0 < \rho_h < 2$, such that

$$p_Z(z) \geq k_1 e^{-k_2|z|^{\rho_h}}, \quad z \in \mathbb{R}; \tag{I.4}$$

(H2) there exist (finite) positive constants k_3 and k_4, such that

$$p_Z(z) \leq \frac{k_3}{k_4 + z^2}, \quad z \in \mathbb{R}. \tag{I.5}$$

On the other hand, a noise rv Z_t will be called *light-tailed* if its pdf p_Z, in addition to satisfying (A1) and (A2), is such that

(L1) there exist (finite) positive constants c_1, c_2, and $\rho_l > 2$, such that

$$p_Z(z) \leq c_1 e^{-c_2|z|^{\rho_l}}, \quad z \in \mathbb{R}; \tag{I.6}$$

(L2) there exists a (measurable) convex, increasing mapping $\phi : \mathbb{R}^+ \to \mathbb{R}^+$, such that

$$\begin{aligned} \phi(z) &< \infty, \quad z \in \mathbb{R}^+ \\ p_Z(z) &\geq e^{-\phi(|z|)}, \quad z \in \mathbb{R}, \\ \mathbb{E}[\phi(4|Z_t|)] &< \infty. \end{aligned} \tag{I.7}$$

Finally, a noise rv Z_t will be called *bounded* if its pdf p_Z is a bounded function and has bounded support.

II. Result

Theorem II.1 *If the noise rv Z_t in (I.1) is heavy-tailed, then the capacity-achieving distribution Q_0 in (I.2) has a bounded support. If the noise pdf has the additional property that for every $\mathcal{P}_0 > 0$ and $Q \in \mathcal{Q}_{\mathcal{P}_0}$, there exists an analytic extension of the marginal entropy density $\mathbb{h}(x;Q)$, $x \in \mathbb{R}$, then Q_0 has a finite support. On the other hand, if the noise rv Z_t is light-tailed or has a bounded support, then Q_0 has unbounded support.*

Earlier related results can be found in the work of Abou-Faycal, Trott and Shamai (ISIT 1997).

The heuristics behind the assertions in Theorem II.1 can be understood as follows. denoting by g a Gaussian pdf with mean zero and variance $\mathcal{P}_0 + \sigma_z^2$, and by $\mathcal{Q}^*_{\mathcal{P}_0}$ the set $\{Q \in \mathcal{Q}_{\mathcal{P}_0} : \mathbb{E}_Q[X_t^2] = \mathcal{P}_0\}$, under the conditions (H1, H2) or (L1. L2) and (A1), it holds that

$$\begin{aligned} C(\mathcal{P}_0) &= \max_{Q \in \mathcal{Q}^*_{\mathcal{P}_0}} I(Q) \\ &= \frac{1}{2}[1 + \log 2\pi(\mathcal{P}_0 + \sigma_z^2)] - \mathbb{h}(Z_t) - \min_{Q \in \mathcal{Q}^*_{\mathcal{P}_0}} D(p_Y^Q || g). \end{aligned} \tag{II.1}$$

Hence, the maximization in (I.2) is equivalent to minimizing the (Kullback-Leibler) divergence between the pdf of the output rv Y_t and the Gaussian pdf g. The assertion in Theorem II.1 is then, in effect, a reflection of the fact that for a given noise pdf, an input distribution with a bounded support results in an output pdf which decays more rapidly than when the input distribution has unbounded support.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

The Binary Jitter Channel: A New Model for Magnetic Recording

D. Arnold	A. Kavčić[1]	R. Kötter[2]	H.-A. Loeliger	P.O. Vontobel[3]
IBM Research	Harvard University	University of Illinois	Endora Tech AG	ETH Zurich
Säumerstr. 4	29 Oxford Street	1308 W. Main St.	Hirschgässlein 40	Sternwartstr. 7
CH-8803 Rüschlikon	MA 02138, USA	Urbana, IL 61801, USA	CH-4051 Basel	CH-8092 Zurich
arn@zurich.ibm.com	kavcic@hrl.harvard.edu	koetter@uiuc.edu	haloeliger@endora.ch	vontobel@isi.ee.ethz.ch

Abstract — **The capacity of future high-density magnetic recording systems is expected to be limited primarily by "jitter". For such systems, a new simple channel model is proposed. A factor graph representation as well as upper and lower bounds on the capacity of this channel model are given.**

As mechanical and electronic components of magnetic recording systems are being improved, the "noise" of the magnetic medium itself will begin to dominate other noise sources [1]. This "medium noise" is highly signal-dependent [2] and comes in two different forms. First, *isolated transitions* (i.e., changes of magnetic polarization) are affected by *jitter* [3]: the transition is read at a different position than where it was written. Second, very short polarization regions tend to be *unstable*: the two transitions move towards, and may actually cancel, each other.

The present paper addresses the problem of modeling these effects in a way that is suitable for signal processing. To this end, the magnetic recording channel is first decomposed into three parts: a "binary jitter channel" (BJC) that captures the mentioned medium noise, a linear intersymbol interference channel that is defined by the impulse response of the read head, and additive white Gaussian noise due to the amplifier. The BJC is then further decomposed as follows.

Let $X_k \in \{0,1\}$ and $Y_k \in \{0,1\}$ be the time-k input and output, respectively, of the BJC, where $X_k = 1$ ($Y_k = 1$) means that a transition is written into (read from) the time-k slot. The BJC $X_k \to Y_k$ is decomposed into a memoryless probabilistic channel $X_k \to J_k$ and a deterministic channel $J_k \to Y_k$ with memory. The auxiliary variable J_k takes values in the set $\{0\} \cup \{D^i : i = -m, -m+1, \ldots, m\}$ for some positive integer m; $J_k = D^j$ means that a transition was written into the time-k slot and moved into slot $k+j$. We mainly consider the simplest case with $m = 1$, $p_{J|X}(D^{\pm 1}|1) = p$, and $p_{J|X}(1|1) = 1 - 2p$. We always have $p_{J|X}(0|0) = 1$.

The deterministic channel $J_k \to Y_k$ —which takes into account the cancellation of transitions that fall into the same slot or cross—can be described by a trellis. For $m = 1$, this trellis has 4 states and 16 branches.

The factor graph [4] that corresponds to this BJC model is shown in Fig. 1. This factor graph can be plugged into a block factor graph (as in Fig. 2) of the whole system. The sum-product algorithm ("probability propagation") [4] can then be applied to "turbo" decoding of such a system.

The mentioned cancellation of crossing transitions makes it difficult to compute the capacity of the BJC. However, methods similar to those of [5] (where cancellations were not considered) can be used to obtain tight upper and lower bounds by optimization of $\overline{C}_L^M \triangleq \max_{P_X} \left[H(Y_L|\mathbf{Y}_{-L}^{L-1}) - H(Y_L|\mathbf{X}_{-L+1}^{+L+1}\mathbf{Y}_{-L}^{L-1}S'_{-L})\right]$ and $\underline{C}_L^M \triangleq \max_{P_X} \left[H(Y_L|\mathbf{Y}_{-L}^{L-1}S'_{-L}) - H(Y_L|\mathbf{X}_{-L-1}^{+L+1}\mathbf{Y}_{-L}^{L-1})\right]$ respectively, where S'_{-L} is the state of the BJC composed of the time-$(-L)$ state and M prior inputs. The input is assumed to be stationary and generated by a Markov-Chain of order M. Then $\underline{C}_L^M \le C^M \le \overline{C}_L^M$, and C^M approaches capacity for $M \to \infty$. Fig. 3 shows upper and lower bounds on the capacity of the BJC for $(1,\infty)$-constrained input sequences, i.e., there is at least one zero between two ones.

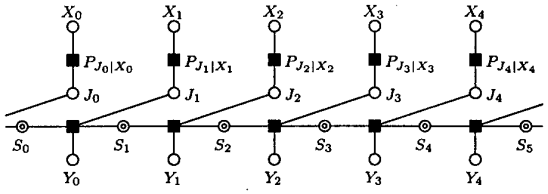


Fig. 1: Factor graph representation of the BJC.

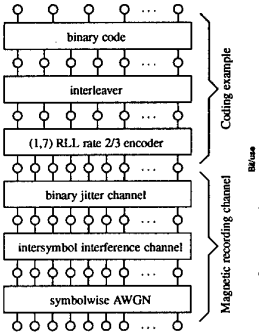


Fig. 2: Block factor graph.

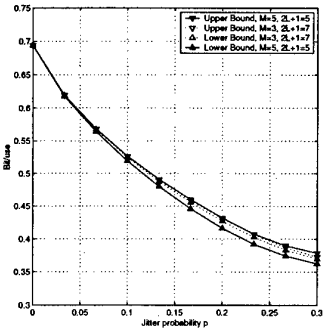


Fig. 3: Bounds of the BJC for $(1,\infty)$-constrained inputs.

References

[1] A. Kavčić and A. Patapoutian, "A signal-dependent autoregressive channel model," in *Proc. IEEE INTERMAG Conference,* Kyongju, Korea, May 1999.

[2] S. M. Yuan, H. N. Bertram, "Statistical data analysis of magnetic recording noise mechanisms," *IEEE Trans. Magnetics,* vol. MAG-28, pp. 84–92, Jan. 1992.

[3] C. P. M. J. Baggen, *An Information Theoretic Approach to Timing Jitter*, Ph.D. thesis, UCSD, 1991.

[4] F. R. Kschischang, B. J. Frey, and H.-A. Loeliger, "Factor graphs and the sum-product algorithm," submitted to *IEEE Trans. Inform. Theory,* available at http://www.comm.utoronto.ca/frank/factor/.

[5] Sh. Shamai, E. Zehavi, "Bounds on the capacity of the bit shift magnetic recording channel," *IEEE Trans. Inform. Theory*, vol. IT-37, no. 3, pp. 863–872, May 1991.

[1]Partial support from NSF Grant CCR-9904458.
[2]This work was supported by NSF Grant CCR-9984515.
[3]This work was supported by Grant TH-16./99-3.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

The Traffic Carrying Capacity Of Wireless Networks

Piyush Gupta and P. R. Kumar
CSL, University of Illinois
1308 W. Main St, Urbana, IL 61801
{piyush,prkumar}@decision.csl.uiuc.edu

Abstract — **How much traffic can wireless networks carry? Consider n nodes located in a disk of area A sq. meters, each capable of transmitting at a data rate of W bits/sec. Under a protocol based model for successful receptions, the total network can carry only $\Theta\left(W\sqrt{An}\right)$ bit-meters/sec, where 1 bit carried a distance of 1 meter is counted as 1 bit-meter. This is the best possible even assuming the nodes locations, traffic patterns, and the range/power of each transmission, are all optimally chosen. If the node locations and their destinations are randomly chosen, and all transmissions employ the same power/range, then each node only obtains a throughput of $\Theta\left(W/\sqrt{n\log n}\right)$ bits/sec, if the network is optimally operated. Similar results hold for a physical SIR based model.**

I. Introduction

Consider a network with n nodes located in an area of A sq. m. Every node can transmit at a data rate of W bits/sec over a common channel. Due to interference between transmissions, we need to specify when transmissions are successfully received. We allow for two models.

The Protocol Model: For a node to receive a transmission at a range r, there can be no other simultaneous transmissions within a range $(1+\Delta)r$ from it. (Or one can assume that interference rules out any other receptions in a disk of radius $(1+\Delta)r$ around a transmitter of range r).

The Physical Model: Assume that path-loss can be modeled as $r^{-\alpha}$ where $\alpha > 2$, and that there is ambient noise of power level N. Then a transmission by node X_i at a power level P_i is successfully received by node X_j if and only if the signal-to-interference ratio (SIR) is at least β, i.e.,

$$\frac{P_i\,|X_i - X_j|^{-\alpha}}{N + \sum_{k\in\mathcal{T}} P_k\,|X_k - X_j|^{-\alpha}} \;\geq\; \beta.$$

Above $\mathcal{T}$ is the set of all other nodes which are transmitting at the very same time, and P_k is the power level of node X_k.

II. The Best Case Scenario

The destinations of nodes are allowed to be arbitrary, as are the traffic levels for OD-pairs. Each transmission may be of an arbitrary range/power.

We say that the network has transported 1 bit-meter when 1 bit has been transmitted over a distance of 1 meter.

[1]This material is based upon work partially supported by the Air Force of Scientific Research under Contract No. AF-DC-5-36128, the Office of Naval Research under Contract No. N00014-99-0696, and EPRI and DOD-ARO under subcontract Nos. W08333-04 and 35352-6086. Any opinions, findings, and conclusions are those of the authors and do not necessarily reflect the views of the above agencies.

[2]Please address all correspondence to the second author.

III. The Random Scenario

We assume that the n nodes are randomly located (uniform iid) in a disk of area A sq. m. Each node has a random destination, chosen as the node nearest to a uniform and iid chosen point to which it wishes to send traffic at a rate $\lambda(n)$ bits/sec. We suppose that in this homogeneous environment all transmissions employ the same range or power.

We say that the **throughput capacity** is $\Theta(f(n))$ bits/sec if for some constants $0 < c < c' < +\infty$,

$$\begin{aligned}\lim_{n\to\infty} \text{Prob } (\lambda(n) = cf(n) \text{ is feasible for each node}) &= 1\\ \liminf_{n\to\infty} \text{Prob } (\lambda(n) = c'f(n) \text{ is feasible for each node}) &= 0.\end{aligned}$$

IV. The Main Results

Theorem 1. Best Case for Protocol Model: The transport capacity is $\Theta\left(W\sqrt{An}\right)$ bit-meters/sec. More specifically,

$$\frac{W\sqrt{A}}{1+2\Delta}\,\frac{n}{\sqrt{n}+\sqrt{8\pi}} \;\leq\; \begin{matrix}\text{Transport}\\ \text{capacity}\end{matrix} \;\leq\; \sqrt{\frac{8}{\pi}}\,\frac{W\sqrt{A}}{\Delta}\,\sqrt{n}.$$

Theorem 2. Best Case for Physical model: A transport capacity of $cW\sqrt{An}$ bit-meters/sec is feasible, while $c'W\sqrt{A}n^{\frac{\alpha-1}{\alpha}}$ bit-meters/sec is not. More specifically,

$$\left[16\beta\left(2^{\frac{\alpha}{2}} + \frac{6^{\alpha-2}}{\alpha-2}\right)\right]^{-\frac{1}{\alpha}} \frac{W\sqrt{A}\,n}{\sqrt{n}+\sqrt{8\pi}} \;\leq\; \begin{matrix}\text{Transport}\\ \text{capacity}\end{matrix} \;\leq\; \pi^{-\frac{1}{2}}\,[2+2/\beta]^{\frac{1}{\alpha}}\,W\sqrt{A}\,n^{\frac{\alpha-1}{\alpha}}.$$

Theorem 3. Random Case for Protocol Model: The throughput capacity is $\Theta\left(W/\sqrt{n\log n}\right)$ bits/sec.

Theorem 4. Random Case for Physical Model: A throughput $\lambda(n) = cW/\sqrt{n\log n}$ bits/sec is feasible, while $\lambda(n) = c'W/\sqrt{n}$ is not, for appropriate values of c and c', both with probability approaching one as $n \to +\infty$.

V. Concluding Remarks

Under a protocol model, the best per-node throughput for a wireless network with n nodes, with each node having a destination non-vanishingly far away, is $\Theta\left(1/\sqrt{n}\right)$ bits/sec. If the nodes are randomly located, the per-node throughput is $\Theta\left(1/\sqrt{n\log n}\right)$ bits/sec. The random case is nearly best.

Thus, in wireless networks, compromises should be made either with respect to the number of nodes involved, or basically only nearest neighbor communication should be envisaged. Other conclusions following from the constructive proof of capacity in the random case are: A cellular operation is feasible, the range of nodes is about $O(\sqrt{A\log n/\pi n})$, and the fraction of time a node is busy is only $\Theta(1/\log n)$.

References

[1] P. Gupta and P. R. Kumar, "The capacity of wireless networks," to appear in *IEEE Trans. Inform. Theory*, March 2000.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Sequential Signal Encoding and Estimation for Wireless Sensor Networks

Haralabos C. Papadopoulos
ECE Department and Institute for Systems Research
University of Maryland
College Park, MD, 20742, U.S.A
e-mail: babis@eng.umd.edu

Abstract — **We develop extensions to our techniques in [1] for signal estimation from sequential encodings in the form of quantized measurements communicated over binary symmetric channels. We show that the channel quality affects not only the quality of the encoding but also its optimality. We also construct encodings from optimized pseudo-noise and feedback-based control inputs, and efficient signal estimators from channel corrupted versions of the encodings.**

I. Introduction

We consider sequential signal encoding strategies in the form of quantizer bias control for wireless sensor networks where the sensor encodings are communicated to the host over a binary symmetric channel (BSC).

In [1] we focused on the case where the encodings are communicated error-free to the host and showed that a properly designed control input added to the noisy signal prior to quantization can improve the effective digital encoding. For this scenario, we developed optimized control input selection strategies and associated estimators for several different scenarios. These methods can be viewed as lossy encoding techniques of a noisy source [2, 3, 4] that are sequential.

We develop extensions of these approaches for the case that each communication link is a BSC. The block diagram involving a single sensor and the host is shown in Fig. 1, where $w[n]$ is a control input, $v[n]$ is zero-mean IID Gaussian sensor noise, $y[n]$ denotes the binary quantized signal sent to the host, and $z[n]$ denotes the encoding sequence received by the host.

II. Main Results and Discussion

We focus on two special cases. First, we consider pseudo-noise control inputs whose statistical characterization alone is exploited at the host for estimation. Second, we examine the effects of BSC errors when knowledge of the control input can be exploited for estimation at the host and where, in addition, feedback information from the host to the sensor is available and can be exploited in the selection of the control input.

For pseudo-noise control inputs that are accurately modeled as sample paths of a zero-mean IID Gaussian process, we show the optimal pseudo-noise level is an increasing function of the BSC error probability p_e; in particular, as p_e is varied from 0 to 0.5, the optimal aggregate (sensor plus pseudo-noise) level σ^{opt} changes monotonically from $\approx 2\Delta/\pi$ to Δ, where Δ denotes the signal dynamic range. Hence, in order to accurately optimize the quality of the pseudo-noise encoding at the sensor it is important to take into account the quality of the BSC. We also show that, if the encoder does not know the fidelity of the BSC, choosing $\sigma^{\text{opt}}(p_e \to 0.5)$ achieves the best performance across the p_e spectrum.

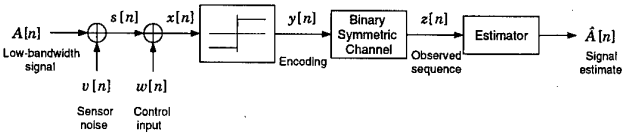


Fig. 1: Signal estimation from channel-corrupted encodings.

In the second case the host knows the control input and can also broadcast feedback information (based on past received encodings) which can be used by each sensor in the selection of future control input values. For any given p_e we derive a bound on the MSE performance of any feedback-based control input strategy and develop control selection methods and computationally efficient estimation algorithms that achieve this bound. Again, both the optimized encoding and estimation algorithms depend on the BSC quality.

We also develop extensions of these bounds and algorithms that achieve them for the more practical case where the sensor receives noise-corrupted feedback information from the host, and, in particular, the case where the (additive) feedback noise is well modeled as a zero-mean IID Gaussian random process. Although the estimators we develop effectively achieve the associated bound provided the number of observations is large enough, the larger the p_e level the larger the number of observations required to effectively achieve the bound.

Finally, as in the case $p_e = 0$ that was considered in detail in [1], for any given p_e the asymptotic performance of these systems can be completely characterized by means of the signal-to-noise ratio (SNR). In particular, for any given p_e level, the MSE performance loss with pseudo-noise control inputs can be made to grow quadratically with SNR by judicious selection of the pseudo-noise power level, while a fixed loss independent of SNR can be achieved in the feedback cases. For comparison, the MSE performance loss due to the encoding in the absence of control input can be shown to grow exponentially with SNR for any given p_e value.

References

[1] H. Papadopoulos, G. Wornell, and A. Oppenheim, "Sequential signal encoding from noisy measurements using quantizers with dynamic bias control," submitted to *IEEE Trans. IT.*

[2] R. Gray, S. Boyd, and T. Lookabaugh, "Low rate distributed quantization of noisy observations," in *Allerton Conf. Commun. Contr. Comp.*, pp. 354–358, 1985.

[3] Y. Ephraim and R. Gray, "A unified approach for encoding clean and noisy sources by means of waveform and autoregressive model vector quantization," *IEEE Trans. IT*, pp. 826–834, July 1988.

[4] R. Zamir and T. Berger, "Multiterminal source coding with high resolution," *IEEE Trans. IT*, pp. 106–117, Jan. 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Information Theory of Wireless Sensor Networks: The *n*-helper Gaussian Case

Mohiuddin Ahmed and Gregory Pottie
Electrical Engineering Department
University of California, Los Angeles
Los Angeles, CA 90095-1594
e-mail: mohin@ucla.edu, pottie@icsl.ucla.edu

***Abstract*: In this paper, wireless sensor networks are considered from an information theory point of view and the rate distortion region for the special case of correlated Gaussian sources where *n* sources provides partial side information to one main source is discussed.**

I. Introduction

It is well known from the theory of distributed detection that higher reliability and lower probability of detection error can be achieved when observation data from multiple, distributed sources is intelligently fused in a decision making algorithm, rather than using a single observation data set [1, 3]. This, coupled with the fact that fabrication technological advances have made low-cost sensors incorporating wireless transceivers, signal processing and sensing in one integrated package a desirable low-cost option, it is inevitable that such devices will be widely used in detection applications such as security, monitoring, diagnostic, remote exploration etc. This has given rise to the development of wireless integrated networked sensors (WINS) [2].

However, the effective deployment of such distributed processing systems introduces some significant design issues, most notably: networking and communication protocols, transmission channel and power constraints, and scalability, among others [1]. These are not the subject of this summary. However, it is evident that some fundamental limits are required to assess the optimality of any system design with regard to the "best design". Thus, an information theoretic analysis of the system is required. We consider a special case of this problem.

II. The *n*-Helper System

Consider the multisensor system as shown below.

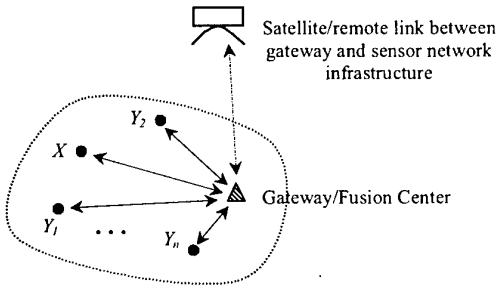


Figure 1: A multi-node networked sensor system.

A portion of a distributed cluster of sensor nodes (perhaps mobile) is observing a phenomenon and generating source data. Algorithms exist which can determine which nodes in the proximity of the phenomenon need to be activated and which can remain dormant [1]. Once this boot-up process is completed, the node observation data is assumed to be Gaussian (for analytical simplicity), with one data node acting as the main data source (e.g. that which is closest to the phenomenon), and the remaining nodes generating correlated data. The coding challenge is then to determine appropriate codes and data rates such that the gateway/data-fusion center can reproduce the data from the main node using the remaining nodes as sources of partial side information, subject to some distortion criteria.

III. A Rate-Distortion Bound

Thus for a main source, X, and n correlated sources, Y_n with $\{X_t, Y_{1t}, \cdots Y_{nt}\}_{t=1}^{\infty}$ being stationary Gaussian memoryless sources, for each observation time, t=1, 2, 3, ..., we let the random $(n+1)$-tuplet $(X_t, Y_{1t}, \cdots Y_{nt})$ take values in $X \times Y_1 \times \cdots Y_n$. The covariance matrix is denoted as:

$$\begin{bmatrix} \sigma_X^2 & \rho_{XY_1}\sigma_X\sigma_{Y_1} & \cdots & \rho_{XY_n}\sigma_X\sigma_{Y_n} \\ \rho_{XY_1}\sigma_X\sigma_{Y_1} & \sigma_{Y_1}^2 & \cdots & \rho_{Y_1Y_n}\sigma_{Y_1}\sigma_{Y_n} \\ \vdots & \vdots & \ddots & \vdots \\ \rho_{XY_n}\sigma_X\sigma_{Y_n} & \rho_{Y_1Y_n}\sigma_X\sigma_{Y_1} & \cdots & \sigma_{Y_n}^2 \end{bmatrix}$$

Then for an encoding system using the Y_n's as n-helpers, the rate-distortion region, given by:

$$\Re(D_X, D_1, \cdots D_{Y_n}) = \{(R_X, R_1, \cdots R_n) : (R_X, R_1, \cdots R_n) \text{ is admissible}\}$$

for a given set of rates and distortion measures is desired. The encoding functions: $\varphi_X : X^m \to \aleph_1 = \{1, \cdots, C_1\} \cdots \varphi_i : Y_i^m \to \aleph_i = \{1, \cdots, C_i\}$ are such that the rate constraints being satisfied are: $\frac{1}{m}\log C_i \le R_i + \delta$, i=$X, 1, 2, \ldots n$. Extending previous results [4 -6], we show that for an admissible rate $(R_X, R_1, R_2, \cdots R_n)$, and for some D_i's > 0, the n-helper system data rates can be fused to yield an effective date rate (with respect to source X) satisfying the following lower bound:

$$R_X \ge \frac{1}{2}\log\left\{\frac{\sigma_X^2}{D_X}\cdot\left[\prod_{k=1}^{n}\left(1-\rho_{XY_k}^2+\rho_{XY_k}^2\cdot 2^{-2R_k}\right)\right]^{\frac{1}{n}}\right\}$$

Future work will attempt to extend these results for non-Gaussian, non-stationary sources.

IV. References

[1]. G. J. Pottie, "Multi-node Processing Problems in Distributed Sensor Networks", *IEEE International Symposium on Information Theory,* Cambridge, MA Aug 16-21, 1998.

[2]. G. J. Pottie, et. al., "Wireless Sensor Networks", *Information Theory Workshop Proceedings,* 1998, Killarney, Ireland, June 22-26, 1998.

[3]. P.K. Varshney, *Distributed Detection and Data Fusion,* New York: Springer-Verlag, 1997

[4]. A. D. Wyner and J. Ziv, "The rate-distortion function for source coding with side information at the decoder", *IEEE Transactions on Information Theory*, vol. IT-22, pp. 1-10, Jan. 1976.

[5]. Y. Oohama, "Gaussian multi-terminal source coding", *IEEE Transactions on Information Theory,* vol. 43, no. 6, Nov. 1997.

[6]. T. S. Han and K. Kobayashi, "A unified achievable rate region for a general class of multi-terminal source coding systems", *IEEE Transactions on Information Theory,* vol. IT-26, pp. 277-288, May 1980.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Optimal Binary Distributed Detection

Wei Shi[1]
University of California
Los Angeles, CA 90095-1594
U.S.A.
e-mail: wshi@ee.ucla.edu

Thomas W. Sun
University of California
Los Angeles, CA 90095-1594
U.S.A.
e-mail: wsun@ee.ucla.edu

Richard D. Wesel
University of California
Los Angeles, CA 90095-1594
U.S.A.
e-mail: wesel@ee.ucla.edu

Abstract — **This paper considers a distributed binary detection system with n binary independent identical sensors. We show that the system-wise probability of error is a quasi-convex function of local threshold τ for generalized Gaussian noise and some non-Gaussian noise distributions. This yields a globally optimal and computationally feasible solution technique.**

Consider distributed detection of $s \in \{-m, m\}$, where the ith of n local sensors observes $x_i = s + z_i$ with i.i.d. noise z_i. The ith sensor compares x_i to a threshold τ to compute a binary decision u_i to be 0 when $x_i < \tau$ and 1 otherwise.

Each binary decision u_i is transmitted to a fusion center, which applies a fusion rule F to $k = \sum_{i=1}^{n} u_i$ to produce the final decision $F(k)$.

The identical threshold τ in local sensors generally does not result in an optimum system. However results in [1] showed that identical local detectors are asymptotically optimum when the number of sensors n tends to infinity. Even with identical local thresholds, the problem is still complicated by the discontinuity of Bayesian error probability and the existence of multiple local minima. [2] provided continuous bounds on the Bayesian error probability, but the minimization problem still has local minima.

In this paper we show that for any admissible fusion rule F (i.e. any F that is optimal for at least one τ), the probability of error is a quasi-convex function of τ. The admissible functions F are simply threshold tests of the form

$$s = F_i(k) = \begin{cases} -m & \text{if } k < i \\ m & \text{if } k \geq i. \end{cases} \quad (1)$$

Hence, the problem decomposes into a series of n quasi-convex optimization problems. We have used this technique to identify the optimal (τ, F) pairs for a variety of cases, and our results suggest that the optimal F is always essentially majority vote for equal *a-priori* probability case. According to this conjecture, the optimal F is identified without computation and only one quasi-convex problem needs to be solved.

For brevity, we prove the quasi-convexity for the Gaussian noise case, i.e. $z_i \sim \mathcal{N}(0,1)$. See [3] for a more extended presentation showing the quasi-convexity for generalized Gaussian noise and some well known non-Gaussian noises.

First define

$$A_k(\tau) = p_0 \binom{n}{k} Q^k(\tau + m) Q^{n-k}(-\tau - m),$$

$$B_k(\tau) = p_1 \binom{n}{k} Q^k(\tau - m) Q^{n-k}(-\tau + m),$$

where p_0 is the *a-priori* probability of $s = -m$ and $p_1 = 1 - p_0$. $Q(\tau) = \int_\tau^\infty f(x)dx$, where $f(x)$ is the pdf of normal distribution with zero mean and unit variance.

Theorem 1 *Only fusion rules of the form F_i in (1) are admissible, i.e. are MAP for some choice of τ.*

Proof: For every τ the MAP F has the form F_i in (1).

Theorem 1 states the same admissible fusion rule as observed in [4].

Theorem 2 *For a fixed admissible fusion rule F_i, probability of error is a quasi-convex function of τ.*

Proof: Define $P_e(\tau, i)$ as the probability of error for (τ, F_i). $P_e(\tau, i)$ can be expressed as

$$P_e(\tau, i) = p_0 + \sum_{k=0}^{i-1} (B_k(\tau) - A_k(\tau)). \quad (2)$$

The derivative of $P_e(\tau, i)$ is a telescoping sum (i.e. has the form $\sum_{k=0}^{i-1}(f_k(\tau) - f_{k-1}(\tau))$ for a specific $f_k(\tau)$) and can be simplified to $P'_e(\tau, i) = \alpha(\tau)(\beta(\tau) - \gamma(\tau))$, where $\alpha(\tau)$ is always positive, $\beta(\tau)$ is a positive and monotonically increasing function and $\gamma(\tau)$ is a positive and monotonically decreasing function. $\beta(-\infty) < \gamma(-\infty)$ and $\beta(\infty) > \gamma(\infty)$. So $P'_e(\tau, i) = 0$ for only one τ^*, for which $\beta(\tau^*) = \gamma(\tau^*)$. For $\tau < \tau^*$, $P'_e(\tau, i) < 0$ and $\tau > \tau^*$, $P'_e(\tau, i) > 0$. So $P_e(\tau, i)$ is quasi-convex. □

[5] gencralizes these results by showing quasiconvexity in the likelihood ratio function for any distribution on the i.i.d. observations x_i. The quasiconvexity can also be extended to Bayesian cost function $\Re(\tau, i)$.

Using quasiconvexity we examined the SNR required for $P_e = 10^{-5}$ as a function of the number of sensors [3]. For Gaussian noise, we found that the number of binary sensors needed for every SNR is fewer than twice the number of infinite-precision sensors. This can make the binary sensor a better choice from a practical or economic point of view.

References

[1] J.N.Tsitsiklis, "Decentralized detection by a large number of sensors," *Mathematics of Control, Signals, and Systems*,vol. 1, pp. 167–182, 1988.

[2] W.A.Hashlamoun and P.K.Varshney,"Near-optimum quantization for signal detection," *IEEE Trans. on Comm.* , vol. 44, no. 3, pp. 294–297, March 1996

[3] W.Shi, T.W.Sun and R.D.Wesel, "Optimal binary distributed detection ," *33rd Asilomar Conference on Signals, Systems & Computers* , Pacific Grove, California, Oct., 1999.

[4] Z. Chair and P.K.Varshney, "Optimal data fusion in multiple sensor detection systems," *IEEE Trans. on Aerospace and Electronic Systems* , vol. AES-23, no. 1, pp. 98–101, Jan. 1986.

[5] Q.Zhang, P.K.Varshney and R.D.Wesel, "Optimal distributed binary hypothesis testing with independent identical sensors," *CISS*, Princeton University, March 2000

0-7803-5857-0/00/$10.00 ©2000 IEEE.

CDMA with fading: Effective bandwidth and spreading-coding tradeoff

E. Biglieri, G. Taricco, E. Viterbo
Dipartimento di Elettronica
Politecnico di Torino, Italy
e-mail: name@polito.it

G. Caire
Institut Eurécom
Sophia-Antipolis, France
e-mail: caire@eurecom.fr

Abstract — **We find the capacity regions of large CDMA systems with linear receivers and random spreading subject to slow fading (nonergodic channel) and fast fading (ergodic channel).**

We consider the *uplink* of a single-cell, synchronous DS-CDMA system with K users and random spreading sequences of L *chips*. The received signal L-chip column vector corresponding to one symbol interval is given by

$$\mathbf{y} = \sum_{k=1}^{K} \sqrt{z_k} x_k \mathbf{s}_k + \mathbf{n} \tag{1}$$

where $\mathbf{n} \sim \mathcal{N}_C(\mathbf{0}, N_0\mathbf{I})$, x_k is the complex modulation symbol of user k, $\mathbf{s}_k$ is the spreading sequence of user k, made of binary antipodal chips $\pm 1/\sqrt{L}$ generated at random with uniform probability and where z_k is the flat fading power gain. We assume that the base station receiver has perfect knowledge of all fading gains and phases, and without loss of generality, we include the phase rotation of the k-th channel into the modulation symbol x_k. User k is received with signal-to-noise ratio (SNR) $\gamma_k = z_k\Gamma_k$, where Γ_k is the *transmit* SNR. As in [3, 4], we consider an asymptotically large system with $K \to \infty$ and $K/L \to \alpha$. The receiver for user 1 (our reference user) is defined by $y_1 = \mathbf{h}_1^H\mathbf{y}$ followed by a single-user decoder operating on the sequence of filter outputs y_1. The filter $\mathbf{h}_1$ can be either a single-user matched filter (SUMF) or a linear MMSE filter [1]. Under the above assumptions, the output SINR β_1 of receiver 1 satisfies [3]:

$$\beta_1 = \begin{cases} \dfrac{\gamma_1}{1+\alpha\int_0^\infty x\, dF_\gamma(x)} & \text{SUMF} \\ \dfrac{\gamma_1}{1+\alpha\int_0^\infty \frac{x\gamma_1}{\gamma_1+x\beta_1} dF_\gamma(x)} & \text{MMSE} \end{cases} \tag{2}$$

Where $F_\gamma(x)$ is the limiting cdf of the received user SNRs. In the following, we assume that users are partitioned into J classes. Each class j is characterized by a transmit SNR Γ_j. Each class has p_jK users, where $\sum_{j=1}^J p_j = 1$, and the z_k are i.i.d. and normalized, so that $\int_0^\infty x dF_z(x) = 1$. Then, $F_\gamma(x) = \sum_{j=1}^J p_j F_z(x/\Gamma_j)$ where $F_z(x)$ is the fading cdf. Let user 1 belong to class i. Because of the uncompensated fading, user 1 SINR is a random variable $\beta_{i,1}$. However, the ratio $\xi = \beta_{i,1}/(\Gamma_i z_1)$ is non-random and independent of i, and can be calculated from (2).

Non-ergodic fading. In this case, we assume that the fading time-variations are very slow so that the output SINR is random but constant over one code word. Outage probability for users of class i is given by $P_{\text{out},i} = P(\beta_{i,k} \le \bar{\beta}_i) = F_z\left(\frac{\bar{\beta}_i}{\xi\Gamma_i}\right)$ where $\bar{\beta}_i$ is a SINR threshold that depends on the coding scheme of class i. Assuming Gaussian codes and minimum distance decoding at the output of the receiving filter, we let $\bar{\beta}_i = 2^{R_i} - 1$.

Let $\bar{\mathbf{\Gamma}} = (\bar{\Gamma}_1, \ldots, \bar{\Gamma}_J)$ be a vector of input SNR constraints, $\boldsymbol{\epsilon} = (\epsilon_1, \ldots, \epsilon_J)$ be a vector of target outage probabilities, and $\mathbf{R} = (R_1, \ldots, R_J)$ be a vector of coding rates. We find the outage capacity, i.e., the set $\mathcal{R} \subseteq \mathbb{R}_+^J$ of rate vectors $\mathbf{R}$ that can be assigned to the J classes such that, for all $i = 1, \ldots, J$, $P_{\text{out},i} \le \epsilon_i$ and $\Gamma_i \le \bar{\Gamma}_i$. By letting

$$\mu_i = \frac{2^{R_i} - 1}{\sup\{x \in \mathbb{R}_+ : F_z(x) = \epsilon_i\}} \tag{3}$$

we rewrite the outage constraint as $\Gamma_i\xi \ge \mu_i$. For maximum R_i this must hold with equality, which implies that $\Gamma_i/\mu_i = \kappa$ is a constant independent of i. Solving for κ and imposing the input constraints, we obtain the capacity inequality

$$\alpha\sum_{j=1}^{J} p_j B_j \le \min_{1\le i\le J}\left\{1 - \frac{\mu_i}{\bar{\Gamma}_i}\right\} \tag{4}$$

where the *effective bandwidth* B_j is given by

$$B_j = \begin{cases} \mu_j & \text{SUMF} \\ \int_0^\infty \frac{x\mu_j}{1+x\mu_j} dF_z(x) & \text{MMSE} \end{cases} \tag{5}$$

Ergodic fading. In this section we assume that the fading is sufficiently fast the channel can be considered *information stable* [2]. Assuming that all users generate their code book according to a complex circularly-symmetric Gaussian pdf, users in class i can communicate reliably at rate

$$R_i = \int_0^\infty \log_2(1 + x\xi\Gamma_i) dF_z(x)$$

We find the set of rates $\mathbf{R} = (R_1, \ldots, R_J)$ achievable with input constraints $\mathbf{\Gamma} \le \bar{\mathbf{\Gamma}}$. Since the function $f(y) = \int_0^\infty \log_2(1 + xy) dF_z(x)$ is monotonically increasing, we define $\nu_i = f^{-1}(R_i)$, then, $\Gamma_i\xi \ge \nu_i$ and from an argument similar to above we obtain a capacity inequality of the same form of (4), with the substitution $\nu_j \to \mu_j$. It follows that the effective bandwidth B_j in the ergodic case has the same form of (5), with $\nu_j \to \mu_j$.

References

[1] S. Verdú, *Multiuser Detection*. New York: Cambridge University Press, 1998.

[2] E. Biglieri, J. Proakis, and S. Shamai (Shitz), "Fading channels: Information-theoretic and communications aspects," *IEEE Trans. Inform. Theory*, Vol. 44, No. 6, pp. 2619-2692, October 1998.

[3] D. Tse and S. Hanly, "Linear multiuser receivers: Effective interference, effective bandwidth and capacity," *IEEE Trans. on Inform. Theory*, Vol. 45, No. 2, pp. 641-657, March 1999.

[4] S. Verdú and S. Shamai (Shitz), "Spectral efficiency of CDMA with random spreading," *IEEE Trans. on Inform. Theory*, Vol. 45, No. 2, pp. 622-640, March 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Spectral Efficiency of Low–Complexity Multiuser Detectors

Ralf R. Müller[1] and Sergio Verdú
Dept. EE, Princeton University, Princeton, NJ 08544, {rmueller,verdu}@ee.princeton.edu

Abstract — **A family of multiuser detectors is analyzed which require neither matrix inversions nor other operations with significant complexity. The time complexity per bit of most of them is independent of the number of users. Nevertheless, their spectral efficiency for random spreading sequences is shown to be not far behind that of linear MMSE detection.**

I. Introduction

Recently, the performances of well–known linear and nonlinear multiuser detectors in random environments were analyzed in [1, 2, 3] revealing important gains over the spectral efficiency of the single–user matched filter. The price for those improvements is receiver complexity.

An important class of multiuser receivers with lower complexity is based on the idea of approximate decorrelation (AD) [4] (a generalization to approx. MMSE detectors is straightforward): Matrix inversion in approximated via L^{th} order polynomial expansion $\boldsymbol{M}^{-1} \approx \sum_{\ell=0}^{L} w_\ell \boldsymbol{M}^\ell$, see e.g. [5], with properly chosen weights w_ℓ.

II. Main Results

Let $\boldsymbol{y} = \boldsymbol{S}^{\text{H}}(\boldsymbol{S}\boldsymbol{x} + \boldsymbol{n})$ denote the vector notation of a synchronous K user Gaussian CDMA channel with $\boldsymbol{x}, \boldsymbol{y}$ denoting the transmitted and received symbols, respectively, $\boldsymbol{n}$ the complex additive white Gaussian noise of variance σ^2 and $\boldsymbol{S}$ the $L \times K$ matrix of complex signature sequences. In this summary, we restrict attention to equal received powers and we assume that the diagonal elements of the matrix $\boldsymbol{R} = \boldsymbol{S}^{\text{H}}\boldsymbol{S}$ equal unity.

Theorem 1 *Let $K, N \to \infty$, but $0 < \beta = \frac{K}{N} < \infty$ and the random components of $\boldsymbol{S}$ be independent with finite variance. Then, the signal–to–interference–and–noise ratio at the output $\boldsymbol{d} = \boldsymbol{T}\boldsymbol{y}$ of any linear equalizer described by a matrix $\boldsymbol{T} = \sum_{\ell=0}^{L} w_\ell(\beta, \sigma)\boldsymbol{R}^\ell$ converges almost surely to a deterministic scalar for arbitrary weight functions $w_\ell(\beta, \sigma), 0 \le \ell \le L$, and arbitrary order L.*

Theorem 1 allows to give explicit expressions for the SIR of L^{th} order approximation to the MMSE multiuser detector. The results for $L = 1, 2, 3$ are the following:

$$\max_{w_i} SIR_1 \to \frac{1+\beta+\sigma^2}{\beta^2+\sigma^2(1+2\beta)+\sigma^4} > \frac{1-2\beta+\beta^2}{\beta^2+\beta^3+\sigma^2(1-\beta+\beta^2)} \leftarrow SIR_{\text{AD}}$$

$$\max_{w_i} SIR_2 \to \frac{1+\beta+\beta^2+\sigma^2(2+2\beta)+\sigma^4}{\beta^3+\sigma^2(1+2\beta+3\beta^2)+\sigma^4(2+3\beta)+\sigma^6}$$

$$\max_{w_i} SIR_3 \to \frac{1+\beta+\beta^2+\beta^3+\sigma^2(3+4\beta+3\beta^2)+\sigma^4(3+3\beta)+\sigma^6}{\beta^4+\sigma^2(1+2\beta+3\beta^2+4\beta^3)+\sigma^4(3+6\beta+6\beta^2)+\sigma^6(3+4\beta)+\sigma^8}$$

The 0^{th} order approx. is equivalent to the conventional matched filter. The first order approximation (cf. [4, Prob. 5.28.d] is better than the approximate decorrelator analyzed in [4, p. 281], where the weights were based on a Taylor expansion and not optimized with respect to the maximum achievable SIR. The optimum weights can be expressed as L^{th} order polynomials in β and σ^2 and calculated, recursively. Thus, their computation is very simple in real–time applications.

For a fair comparison to the performances of the decorrelator, the MMSE detector, and the matched filter, the spectral efficiency $\Gamma = \beta C = \beta \log_2(1 + SIR)$ and power efficiency $\frac{N_0}{E_{\text{b}}} = \sigma^2 C$ are calculated as in [1, 2]. Averaging capacity results over the load, our results are extended to re–encoded successive cancellation (SC) receivers [1, 2] via $\Gamma_{\text{SC}}(\beta) = \int_0^\beta \log_2(1 + SIR(\beta'))\mathrm{d}\beta'$. Fig. 1 shows the spectral efficiency for fixed E_{b}/N_0 as a function of the load $\beta = K/N$. At low β simple linear receivers noticeably outperform the single-user matched filter. At high β simple nonlinear receivers noticeably outperform the exact MMSE receiver.

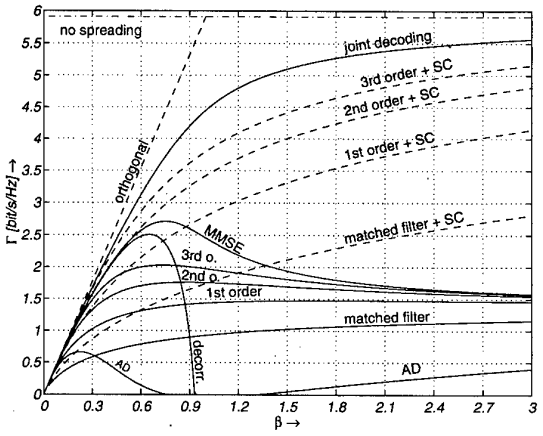


Fig. 1: Spectral efficiency vs. system load for several multiuser detectors and fixed $10\log_{10}(E_{\text{b}}/N_0) = 10$ dB.

III. Conclusion

Increasing spectral efficiency by multiuser detection need not involve significant increase in receiver complexity even with long spreading sequences.

References

[1] R. R. Müller. *Power and Bandwidth Efficiency of Multiuser Systems with Random Spreading.* Shaker, Aachen, 1999.

[2] S. Verdú and S. Shamai (Shitz). Spectral efficiency of CDMA with random spreading. *IEEE Trans. Inf. Th.*, 45(2):622–640, Mar. 1999.

[3] D. Tse and S. Hanly. Linear multiuser receivers: Effective interference, effective bandwidth and user capacity. *IEEE Trans. Inf. Th.*, 45(2):641–657, Mar. 1999.

[4] S. Verdú. *Multiuser Detection.* Cambridge University Press, New York, 1998.

[5] S. Moshavi, E. G. Kanterakis, and D. L. Schilling. Multistage linear receivers for DS–CDMA systems. *Int. J. Wireless Inf. Networks*, 3(1):1–17, Jan. 1996.

[1]This work was supported by the German Academic Exchange Service (DAAD) under grant 332 4 00 510 and by the U. S. Army Research Office under Grant ARO DAAH04-96-1-0379.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Evaluation of the Spectral Efficiency of Spread-Spectrum Multiple-Access Systems

M. Bystrom
ECE Department
Drexel University
Philadelphia, PA 19104
bystrom@ece.drexel.edu

J.W. Modestino
ECSE Department
Rensselaer Polytechnic Institute
Troy, NY 12181
modestin@ecse.rpi.edu

Abstract — **In this work we present an approach for evaluating the spectral efficiency of a direct-sequence spread-spectrum system based on the channel cutoff rate. The spectral efficiency is evaluated independently of specific forward error control codes, and thus can provide general insight into system performance and parameter tradeoffs.**

I. Introduction

For equal-power users with known power the effective noise spectral density in a direct-sequence (DS) spread-spectrum system is given by [1, 2]

$$I_0 = N_0 + (N-1)R_b E_b / W_T \ . \qquad (1)$$

where the first term, N_0, represents the thermal noise while the second term represents the multiple-access interference in terms of the bit rate per user, R_b. We consider the single-user detection case, with a large number of users. To incorporate the effects of fading, we assume the energy is unknown and that the amplitude of the received signal from each user is subject to Rician-distributed fading, $|\tilde{z}|$, and further impose a conservation-of-energy constraint so that $E\{|\tilde{z}(t)|^2\} = 1$.

It follows that the signal-to-interference ratio can be written as

$$E_b/I_0 = \frac{E_b/N_0}{1 + (N-1)(R_b/W_T)(E_b/N_0)} \ . \qquad (2)$$

Defining the spectral efficiency as $\eta_N = \frac{NR_b}{W_T}$; $bits/sec/Hz$ and the total carrier power as $C_T = NR_bE_b$ as in [3], combining the three equations and normalizing by the total thermal noise yields the spectral efficiency in terms of the carrier-to-noise power ratio,

$$\eta_N = \frac{C_T/(N_0W_T)}{(E_b/I_0)[1 + (\frac{N-1}{N})(C_T/(N_0W_T))]} \ ; \ bits/sec/Hz \ . \qquad (3)$$

We are particularly interested in the limiting spectral efficiency in terms of increasing numbers of users, i.e., $N \to \infty$. A general method for evaluating the spectral efficiency is presented in the following section.

II. Cutoff Rate Evaluation of Spectral Efficiency

The cutoff rate for both MPSK and QAM can be written in the form

$$R_0 = \log_2 \frac{M}{1 + \frac{1}{M} f_M(RE_b/N_0, \zeta^2)} \ ; \ bits/c.u. \ , \qquad (4)$$

where M is the constellation size and R is the coding rate. Setting $R = R_0$ in (4) leads to the requirement that the value of E_b/N_0 required to operate at this rate be the solution of $f_M(RE_b/N_0, \zeta^2) = (M2^{-R} - 1)M$. Given E_b/N_0 for a specific channel and modulation scheme, the value of E_b/I_0 in (3) is then taken as E_b/N_0.

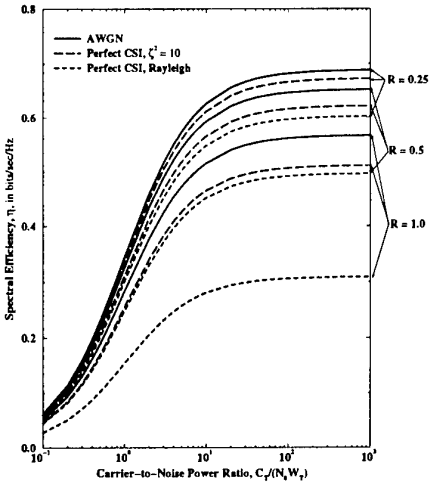


Fig. 1: The limiting spectral efficiency for $M = 4$ and selected rates.

In Fig. 1 the limiting spectral efficiency as $N \to \infty$ for DS/MPSK is shown as a function of the carrier-to-noise power ratio, $C_T/(N_0W_T)$, for selected channel coding rates. Observe that for all rates there exists a value of the carrier-to-noise power ratio, $C_T/(N_0W_T) \approx 10$, above which increasing the ratio does not result in a significant gain in the spectral efficiency. It is also readily observable that the spectral efficiency is monotonically increasing with increase in error control coding, i.e., decreasing R. However, the spectral efficiency gains reach a point of diminishing returns at approximately $R = 0.25$. Similar results are shown for DS/QAM.

III. Summary

It is shown that in general use of some FEC coding increases the spectral efficiency of the system. However, regardless of code rate, performance is optimized for $M = 4$; no significant performance gains are realized for larger signaling alphabet sizes.

References

[1] A.J. Viterbi, "When Not to Spread Spectrum - a Sequel", *IEEE Communications Magazine*, vol. 23, April 1985.

[2] A.J. Viterbi, *CDMA Principles of Spread Spectrum Communications*, Reading, MA: Addison-Wesley Publishing Co., 1995.

[3] J.W. Modestino, "The Spectral Efficiency of Frequency-Hopped MFSK Modulation Schemes," Unpublished GE/CRD Report, March 1994.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Asymptotic Analysis of Data-Aided Channel Estimation Algorithms for Synchronous CDMA Systems

Jamie S. Evans
School of EIE
University of Sydney
NSW 2006, Australia
jevans@ee.usyd.edu.au

Abstract — **The performance of data-aided channel estimation algorithms for CDMA systems is analysed. We compare frame-synchronous and frame-asynchronous LMMSE channel estimators in large systems with random spreading.**

I. Signal Model

Our starting point is the equation for the chip-matched filter output vector at time m

$$y(m) = \sum_{k=1}^{K} a_k(m) b_k(m) s_k(m) + n(m)$$

where $k \in \{1, \ldots, K\}$ indexes the multiple users, $a_k(m)$ is the channel gain for user k over symbol period m, $b_k(m)$ is the M-ary PSK data symbol of user k over period m, $s_k(m)$ is the signature sequence of user k over symbol period m and $n(m)$ is a circularly symmetric complex white Gaussian noise with $\mathbf{E}[n(m)] = 0$ and $\mathbf{E}[n(m)n^H(m)] = \sigma^2 I$.

The channel gain process for each user is a circularly symmetric complex Gaussian random process and the processes for each user are independent with $\mathbf{E}[a_k(m)] = 0$ and $\mathbf{E}[a_k(m)a_k^*(m)] = \bar{p}$. We assume that the channel is constant over time spans corresponding to the frame or block duration so that within a particular frame of data we can drop the time dependence. We also assume the channel estimation starts from scratch at the beginning of every frame which means that our a priori information is simply $\mathbf{E}[a_k(m)] = 0$ and $\mathbf{E}[a_k(m)a_k^*(m)] = \bar{p}$.

The signature sequence $s_k(m)$ is assumed to be an N dimensional column vector with independent and identically distributed elements each being a circularly symmetric complex Gaussian random variable with zero mean and variance $1/N$. The random sequences are independent across users and across symbols.

II. Channel Estimation

Suppose throughout that we are interested in estimating the channel of user one. If we refer to *the* channel we are referring to the channel of user one. We assume we have τ pilot symbols in every frame for channel estimation and let $\bar{p}_\tau = \bar{p}/\tau$, $\sigma_\tau = \sigma/\sqrt{\tau}$ and $\alpha_\tau = \alpha/\tau$. The proofs of the results are omitted however Result 2 can be found in [1] and Result 1 follows using the same techniques (first applied in [2] for the data estimation problem).

Frame-Asynchronous LMMSE

For this estimator we perform LMMSE estimation of the channel based on the received signal over the estimation window, along with the training data of user one. We do not assume that the data of the interfering users is known to the channel estimator so that this algorithm is applicable in frame-asynchronous scenario where the training data of the users does not line up.

Result 1 *The MSE for any user converges almost surely as $N \to \infty$ to the nonrandom $\xi^2 = \bar{p}/(1 + \bar{p}\beta_c)$, where*

$$\beta_c = \frac{1-\alpha}{2\sigma_\tau^2} - \frac{1}{2\bar{p}_\tau} + \left[\frac{(1-\alpha)^2}{4\sigma_\tau^4} + \frac{1+\alpha}{2\bar{p}_\tau\sigma_\tau^2} + \frac{1}{4\bar{p}_\tau^2}\right]^{1/2}$$

The effect of the estimation window length is that the background noise power and the interference power are reduced by τ relative to the $\tau = 1$ case.

Frame-Synchronous LMMSE

In this case we assume we know the data of all users over the estimation window and perform LMMSE estimation conditioned on this information. We thus require that the training interval or estimation window of all users is aligned. In this case the resulting channel estimate is the MMSE estimate since the problem is one of Gaussian estimation.

Result 2 *The MSE for any user converges almost surely as $N \to \infty$ to the nonrandom $\xi^2 = \bar{p}/(1 + \bar{p}\beta_c)$ where*

$$\beta_c = \frac{1-\alpha_\tau}{2\sigma_\tau^2} - \frac{1}{2\bar{p}} + \left[\frac{(1-\alpha_\tau)^2}{4\sigma_\tau^4} + \frac{1+\alpha_\tau}{2\bar{p}\sigma_\tau^2} + \frac{1}{4\bar{p}^2}\right]^{1/2}$$

For this receiver we see that, along with the background noise being reduced by τ, the effective spreading gain is increased by τ. The alignment of the pilot symbols of all users means that we can form effective spreading sequences of interferers by piecing together the (modulated) spreading sequences from all the pilot symbols. This property can lead to very large performance improvements over the frame-asynchronous LMMSE estimator.

III. Conclusions

In this work, we analyse the performance of *multiuser* channel estimation algorithms for CDMA systems. One point that is evident, is that there are significant gains from knowing the data of all users over the estimation window. The results we have presented can be extended to frequency-selective fading and to handle non-equal average powers.

References

[1] J. S. Evans and D. N. C. Tse, "Large system performance of linear multiuser receivers in multipath fading channels," *To appear in IEEE Trans. Information Theory.* (Available from http://www.ee.usyd.edu.au/~jevans.)

[2] D. N. C. Tse and S. Hanly, "Linear multiuser receivers: Effective interference, effective bandwidth and user capacity," *IEEE Trans. Inform. Theory*, vol. 45, pp. 641–657, Mar. 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On Minimal α–Mean Error Parameter Transmission Over Poisson Channel

Marat V. Burnashev [1]
Institute for Problems of Information Transmission
Russian Academy of Sciences
19 B. Karetni, 101447 Moscow, Russia
email: burn@iitp.ru

Yury A. Kutoyants
Laboratoire de Statistique et Processus
Université du Maine
72085 Le Mans, Cédex France
email: kutoyants@univ-lemans.fr

Abstract — **We consider the problem of one–dimensional parameter transmission over the Poisson channel when input signal (intensity) obeys peak energy constraint. We show that it is possible to choose input signals and estimator in such a way that the mean–square error (or, more generally, α–mean error for loss function $|x|^\alpha$) of parameter transmission will decrease exponentially with transmission time $T \to \infty$, and we find the best possible exponent, if $\alpha \geq \alpha_0 = (1+\sqrt{5})/2 \approx 1.618$.**

I. Statement of the problem

Let $\Theta = [0,1]$ be the parameter (to be transmitted) set. We assume that an input signal (intensity function) $S(\theta,t)$ of Poisson channel satisfyes only the peak energy constraint:

$$0 \leq S(\theta,t) \leq A \quad \text{for any} \quad \theta \in [0,1],\ 0 \leq t \leq T, \qquad (1)$$

where $A > 0$ is some given constant.

Thus, if θ_0 is the true value of parameter θ then the observation process at the channel output $X(t)$, $0 \leq t \leq T$, is a random process with independent increments such that $X(0) = 0$ and for any $0 \leq t_1 \leq t_2 \leq T$

$$\Pr\{X(t_2) - X(t_1) = j\} = \frac{e^{-\Lambda}\Lambda^j}{j!}, \quad j = 0,1,\dots,$$

where

$$\Lambda = \int_{t_1}^{t_2} S(\theta_0,t)\,dt.$$

Introduce function $d(\alpha,T)$, giving the minimal possible α–mean error for the best estimator $\bar{\theta}_T$ and the best chosen signals $S(\theta,t)$ when parameter θ takes values from the set $\Theta = [0,1]$:

$$d(\alpha,T) = \inf_{S(.,.)} \inf_{\bar{\theta}_T} \sup_{\theta\in\Theta} \mathbf{E}_\theta \left|\bar{\theta}_T - \theta\right|^\alpha, \quad \alpha > 0,$$

where $\inf_{S(.,.)}$ is taken over all signals $S(.,.)$ satisfying constraint (1).

We are interested in asymptotic behavior of function $d(\alpha,T)$ for large T. Since it decreases exponentially when $T \to \infty$, we introduce also function $e(\alpha)$, giving the best possible exponent for the α–mean error

$$e(\alpha) = \lim_{T\to\infty} \left\{-\frac{1}{AT} \ln d(\alpha,T)\right\}, \quad \alpha > 0. \qquad (2)$$

[1]This work was supported by Grant N 98-01-04108 from the Russian Fund for Fundamental Research.

II. Main result

The following theorem presents the main result of the paper.

Theorem . *If* $\alpha \geq \alpha_0 = (1+\sqrt{5})/2 \approx 1.618$ *then*

$$e(\alpha) = \frac{\alpha}{4(1+\alpha)}. \qquad (3)$$

In other words, if $\alpha \geq \alpha_0$ *then for* $T \to \infty$

$$\inf_{S(.,.)} \inf_{\bar{\theta}_T} \sup_{\theta\in[0,1]} \mathbf{E}_\theta \left|\bar{\theta}_T - \theta\right|^\alpha = \exp\left\{-\frac{\alpha A T(1+o(1))}{4(1+\alpha)}\right\},$$

where $\inf_{S(.,.)}$ *is taken over all signals* $S(.,.)$ *satisfying constraint (1).*

Clearly, $e(2) = 1/6$ determines the best exponential rate for the mean–square error.

Remarks. 1) Function $e(\alpha)$ is very similar to the reliability function $E(R)$ of Poisson channel [5], [3]. Using function $E(R)$ we get the lower bound for function $e(\alpha)$. On the other hand, knowning function $e(\alpha)$ we can get the exact upper bound for function $E(R)$ that is the most difficult part in finding the function $E(R)$.

2) In the case of White Gaussian noise channel a similar problem was solved in [1, 2]. Moreover, a number of optimal results known for White Gaussian noise channel has been obtained recently for Poisson channel as well [5, 3]. In that respect, the paper also extends results of [1, 2] to the Poisson channel. A common feature of all papers [5, 3] and this one is that the Poisson channel turns out to be a simpler than the Gaussian one.

References

[1] M. V. Burnashev, "A new lower bound for the α– mean error of parameter transmission over the white Gaussian channel," *IEEE Trans. Inform. Theory*, vol. IT-30, no. 1, 23–34, 1984.

[2] M. V. Burnashev, "On a minimum attainable mean–square error for parameter transmission over the white Gaussian channel," *Probl. Inform. Transm.*, vol. 21, no. 4, 3–16, 1985.

[3] M. V. Burnashev and Yu. A. Kutoyants, "On sphere-packing bound, capacity and related results for Poisson channel," *Probl. Inform. Transm.*, vol. 35, no. 2, 3–22, 1999.

[4] Yu. A. Kutoyants, *Statistical Inference for Spatial Poisson Processes*. Lecture Notes in Statistics, 134. Springer, 1998.

[5] A. D. Wyner, "Capacity and error exponent for the direct detection photon channel," *IEEE Trans. Inform. Theory*, vol. IT-34, pt. I, pp. 1449–1461; pt. II, pp. 1462–1471, 1988.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Real-time ARMA identification in the case of missing observations

Élisabeth Lahalle[1]
École Supérieure d'Électricité
Service des Mesures
Plateau de Moulon
3, rue Joliot-Curie
91192 Gif sur Yvette, France
e-mail:
elisabeth.lahalle@supelec.fr

Gilles Fleury
e-mail:
gilles.fleury@supelec.fr

Jacques Oksman
e-mail:
jacques.Oksman@supelec.fr

Abstract — **In this paper, a new recursive algorithm for ARMA modeling of uniformly sampled signals with missing observations is proposed. This algorithm enables real-time processing and may be used for time and frequency domain reconstruction.**

This paper addresses the problem of statistical inference concerning time series from missing data. Several restoration methods, including parametric estimation methods in the presence of incomplete data, can be found in [1] [2] [3]. All those methods deal only with stationary signals while the proposed method is also suited to non-stationary ones.

An ARMA adaptive predictor is used. It has been adapted to the non-uniform sampling context by the way of replacing each missing value by its estimate. So, due to missing observations a non-linear optimization criterion is required in order to estimate the model parameters. The optimum is reached by means of an LMS-like algorithm adapted to this sampling context.

A low-pass ARMA (2,2) signal is generated as the output of an elliptic filter in order to test the performances of the proposed algorithm for both AR and MA parts. Figure 1 shows the reconstructed signal for only one realization of the sampling process in the case where 20% of the samples are lost.

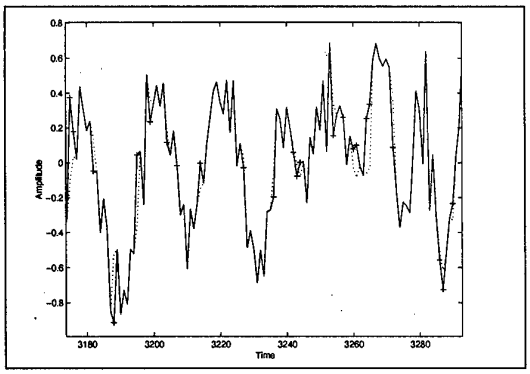


Fig. 1: Original (—) and reconstructed (...) signal, missing samples (++)

Figure 2 shows a good agreement between original and estimated PSDs for different values of probability p. The proposed method leads to far better performances for the spectral estimator than a classical off-line method [4] for ARMA identification of uniformly sampled signals, even in the case where 20% of the samples are lost.

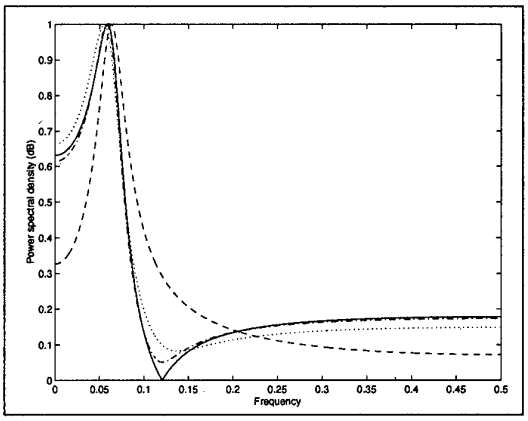


Fig. 2: Original PSD (—), estimated PSD: classical off-line method (- -), proposed method: periodic sampling $p = 1$ (-.-), missing samples $p = 0.8$ (...)

Data compression may be achieved by means of non-periodic transmission [5]. The proposed algorithm is an answer to the need of an efficient reconstruction algorithm in the receiver in the case of ARMA modeled signals (for instance speech coding).

References

[1] R. Veldhuis, "Restoration of lost sample in digital signals," *Prentice hall*, 1990.

[2] R. H. Jones,"Fitting a continuous time autoregression to discrete data,"*Applied times series analysis III*, pp. 651–682, 1981.

[3] Y. Rozen and B. Porat,"Optimal ARMA Parameter Estimation Based on the Sample Covariances for Data with Missing Observations,"*IEEE Trans. on Inform. Theory*, vol. 35, pt. II, pp. 342–349, 1989.

[4] L. Ljung,"System Identification Theory for the User", *Prentice hall, Englewood Cliffs, N. J.*, 1987.

[5] S. Mirsaidi and J. Oksman, "An ADPCM-like system based on non uniform signal transmission",*International Workshop on Sampling Theory and Applications*,pp. 139–143,1997, Aveiro (Portugal).

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Fault-Tolerant Dynamic Systems

Christoforos N. Hadjicostis[1]
UIUC, Dept. of ECE and CSL
148 C&SRL, 1308 W. Main Street
Urbana, IL 61801
e-mail: chadjic@uiuc.edu.

George C. Verghese
MIT, Dept. of EECS
Room 10-092, 77 Mass. Av.
Cambridge, MA 02139
e-mail: verghese@mit.edu.

Abstract — **We use unreliable system replicas and unreliable voters to construct redundant dynamic systems that tolerate transient failures in their state transition and error correcting mechanisms. Using low density parity check (LDPC) codes, we develop a fault-tolerant scheme that efficiently protects linear finite state machines (LFSM's) with identical dynamics but distinct input sequences and states. The scheme achieves a probability of failure that remains below any given bound for any pre-specified (finite) time-interval using a constant amount of hardware (XOR gates and voters) per LFSM.**

I. Introduction

A *dynamic system* evolves according to an internal *state* that influences its future states/outputs. The effect of a transient failure in the state transition mechanism may last over several time steps (even though the cause does not persist). A dynamic system (e.g., a finite-state machine) in which the probability of making a transition to an incorrect next state is p_s and is independent between different time steps, follows the correct state trajectory for L time steps with probability $(1-p_s)^L$. A common solution is to use modular redundancy with feedback: a voter feeds back to all systems the state agreed upon by the majority of them. If the voter fails with probability p_v, this approach will *not* work: after L time steps, the probability that the system has followed the correct state trajectory is at best $(1-p_v)^L$.

II. Fault-Tolerant Scheme

Consider a variant of modular redundancy that uses n system replicas (initialized at the same state and supplied with the same inputs) and n voters, each of which receives "ballots" from all n systems and feeds back a correction to only *one* of the systems. Since a fault-free voter recovers the correct state of the underlying dynamic system as long as more than half of the n systems are in the correct state, our (conservative) goal is to ensure that, with high probability, the fault-tolerant implementation has no *overall failure* (i.e., it operates with at least $\lceil \frac{n}{2} \rceil$ systems in the correct state at any given time step).

Theorem, [1]: *Suppose each system takes a transition to an incorrect state with probability p_s and each voter feeds back an incorrect state with probability p_v (independently between systems, voters and time steps). The probability of an overall failure at or before time step L is bounded above by $L\sum_{i=\lfloor n/2 \rfloor}^{n} \binom{n}{i} p^i(1-p)^{n-i}$, where $p \equiv p_v + (1-p_v)p_s$. This probability goes down* exponentially *with the number of systems n if and only if $p < \frac{1}{2}$.*

An LFSM is an FSM with state evolution $\mathbf{q}_s[t+1] = \mathbf{A}\mathbf{q}_s[t] \oplus \mathbf{b}x[t]$, where $\mathbf{q}_s[t]$ is the d-dimensional *state vector*, $x[t]$ is the input, and $\mathbf{A}$, $\mathbf{b}$ are constant matrices of appropriate dimensions (all vectors and matrices have entries from $GF(2)$). If we take k such LFSM's and let them run in parallel (each with *different* initial states and *different* input streams), we get

$$\begin{bmatrix} \mathbf{q}_1[t+1] & \cdots & \mathbf{q}_k[t+1] \end{bmatrix} = \mathbf{A}_c \begin{bmatrix} \mathbf{q}_1[t] & \cdots & \mathbf{q}_k[t] \end{bmatrix} \oplus \mathbf{b} \begin{bmatrix} x_1[t] & \cdots & x_k[t] \end{bmatrix}.$$

If we post-multiply both sides of the above equation by $\mathbf{G}^T$ (where $\mathbf{G}$ is an $n \times k$ encoding matrix of a linear code), we get the following n encoded parallel instantiations

$$\begin{bmatrix} \xi_1[t+1] & \cdots & \xi_n[t+1] \end{bmatrix} = \mathbf{A}_c \begin{bmatrix} \xi_1[t] & \cdots & \xi_n[t] \end{bmatrix} \oplus \mathbf{b} \underbrace{\left(\begin{bmatrix} x_1[t] & \cdots & x_k[t] \end{bmatrix} \mathbf{G}^T \right)}_{e(x_1[t], x_2[t], \cdots, x_k[t])}$$

We have n LFSM's performing k *different* encoded instantiations of the given LFSM. We employ LDPC codes (with K "1's" in each row and J "1's" in each column of their parity check matrix) and use the approach in [2] to perform error-correction (each bit can be corrected via a mechanism that uses unreliable XOR gates and unreliable voters).

Theorem, [1]: *Assume that the 2-input XOR gates fail with probability p_x and the $(J-1)$-bit voters fail with probability p_v. Let J be a fixed* even *integer greater than 4, let K be an integer greater than J, and let p be such that $p > \binom{J-1}{J/2}[(K-1)(2p+3p_x)]^{J/2} + p_v + p_x$. Then there exists a sequence of (n,k) LDPC codes such that the probability of an overall failure at or before time step L is bounded above by $LdCk^{-\beta}$ where*

$$\beta = -\frac{\log\left\{(J-1)(K-1)\binom{J-2}{J/2-1}[(K-1)(2p+3p_x)]^{J/2-1}\right\}}{2\log[(J-1)(K-1)]} - 3,$$

$$C = \frac{J}{(1-J/K)^3}(2p+3p_x)\left[\frac{1}{2K} - \frac{1}{2J(K-1)}\right]^{-(\beta+3)}$$

The code redundancy is $\frac{n}{k} \leq \frac{1}{1-J/K}$ and the hardware used per LFSM (including the error-correcting mechanism) is bounded above by a constant.

[1]This work has been supported in part by fellowships from the National Semiconductor Corporation and the Grass Instrument Company and in part by a grant by the University of Illinois at Urbana-Champaign.

References

[1] C. N. Hadjicostis, Coding Approaches to Fault Tolerance in Dynamic Systems. PhD thesis, EECS Department, Massachusetts Institute of Technology, Cambridge, Massachusetts, 1999.

[2] M. G. Taylor, "Reliable information storage in memories designed from unreliable components," *The Bell System Journal*, vol. 47, pp. 2299–2337, December 1968.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On the Necessary Density for Spectrum-blind Nonuniform Sampling[1]

Michael Gastpar
Department of Communication Systems
Swiss Federal Institute of Technology
CH-1015 Lausanne, Switzerland
e-mail: michael.gastpar@epfl.ch

Yoram Bresler
Coordinated Science Laboratory
Dept. of Electrical and Computer Engineering
University of Illinois at Urbana–Champaign
Urbana, IL 61801, USA
e-mail: ybresler@uiuc.edu

Abstract — **It is known that in the absence of distortion, the minimum average sampling density for a multiband signal is given by its spectral occupancy [1]. Furthermore, there exist nonuniform sampling patterns of the same average sampling density such that reconstruction is feasible even if the actual spectral support of the multiband signal is unknown [2]. This is called spectrum-blind nonuniform sampling. However, if the samples are distorted, an increased sampling density may lead to superior reconstruction.**

Suppose that a fidelity criterion is imposed on the reconstruction. To satisfy this, it is necessary to sample at an increased density. In this paper, we consider additive noise distortion of the samples, and the fidelity criterion is the probability that the spectral support is correctly reconstructed. In [3], we consider samples distorted by quantization, with a mean-square reconstruction error fidelity criterion.

I. Nonuniform Sampling

Consider a complex-valued length-N sequence $x \in C^N$ with discrete Fourier transform (DFT) $X \in C^N$, where $X(m) = 1/\sqrt{N} \sum_{n=0}^{N} x(n) e^{-j\frac{1}{N} 2\pi nm}$. Let x be a multiband sequence of spectral occupancy q/N, i.e. let X have (at most) q non-zero components in arbitrary locations, indexed by $\underline{K} = \{k_1, \ldots, k_q\}$, where $k_i \in \{0, \ldots N-1\}$. The spectral occupancy for this vector is $\Omega = q/N$. Define the vector $x_{\underline{c}}$ containing only p of the N components of x, at locations indexed by $\underline{c} = \{c_1, \ldots, c_p\}$. These are the nonuniform samples, with average sampling density $\rho = p/N$. In matrix notation, we can write $x_{\underline{c}} = A_{\underline{c},\underline{K}} S$. Here, S contains the q non-zero components of X, and $A_{\underline{c},\underline{K}}$ is the submatrix of the inverse DFT matrix that is obtained by only retaining the rows with indices in $\underline{c}$ and the columns with indices in $\underline{K}$. We consider the case of distorted samples $y_{\underline{c}} = x_{\underline{c}} + z = A_{\underline{c},\underline{K}} S + z$, where $z \sim \mathcal{N}_c(0, \sigma^2 I)$ is (complex) white Gaussian noise.

II. Necessary Sampling Density

Let the location of the q nonzero components of X be distributed uniformly over all possibilities, and let their (complex) values be distributed as circularly normal, $S \sim \mathcal{N}_c(0, \sigma_S^2 I)$. We define the signal-to-noise ratio (SNR) $\beta = \sigma_S^2/\sigma^2$. It can be shown [4] that for $z = 0$, there exist sampling patterns with sampling density $\rho = \Omega + 1/N$ allowing w.p.1, perfect reconstruction of x from $y_{\underline{c}}$.

We derive a necessary condition for the optimal sampling density for $z \neq 0$. It follows from considering mutual informations. We start by noting that by the data processing lemma, $I(x_{\underline{c}}; y_{\underline{c}}) \geq I((S, \underline{K}); y_{\underline{c}}) = I(\underline{K}; y_{\underline{c}}) + I(S; y_{\underline{c}}|\underline{K})$, which yields

$$\max I(x_{\underline{c}}; y_{\underline{c}}) \geq \max_{\{A_{\underline{c},\underline{K}}\}} \left\{ I(\underline{K}; y_{\underline{c}}) + I(S; y_{\underline{c}}|\underline{K}) \right\}, \quad (1)$$

where first, the max is taken on both sides over all sets $\{A_{\underline{c},\underline{K}}\}$ of matrices satisfying $\left(A_{\underline{c},\underline{k}} A_{\underline{c},\underline{k}}^H\right)_{ii} = \Omega$ (which preserves $E|x_{\underline{c}}(i)|^2 = \Omega\sigma_S^2$); then, on the LHS, the max is taken over all distributions of $x_{\underline{c}}(i)$ for which $E|x_{\underline{c}}(i)|^2 = \Omega\sigma_S^2$ as for the true $x_{\underline{c}}(i)$. The term on the left in Eqn. (1) is simply the capacity of a (complex) additive white Gaussian noise (AWGN) channel with input power constraint $\Omega\sigma_S^2$ and additive noise variance σ^2, thus $\max I(x_{\underline{c}}; y_{\underline{c}}) = p \log_2(1 + \Omega\beta)$.

Next, consider $I(\underline{K}; y_{\underline{c}})$ in Eqn. (1). This is the mutual information across the digital channel from $\underline{K}$ to $y_{\underline{c}}$. A lower bound on the mutual information follows from Fano's inequality, $I(\underline{K}; y_{\underline{c}}) \geq H(\underline{K}) - H_b(P_e) - P_e \log_2\left(\binom{N}{q} - 1\right)$.

Last, consider $I(S; y_{\underline{c}}|\underline{K})$ in Eqn. (1). It is the mutual information across the channel between S and $y_{\underline{c}}$. This is also a Gaussian channel, but its input is not iid. The achieved mutual information is found by averaging over all $\underline{k}$ as $I(S; y_{\underline{c}}|\underline{K}) = E_{\underline{K}} \log_2 \det\left(I_q + \beta A_{\underline{c},\underline{K}}^H A_{\underline{c},\underline{K}}\right)$. For each $\underline{k}$, the maximum over $A_{\underline{c},\underline{k}}$ subject to the aforementioned constraint is achieved (by the geometric-arithmetic mean inequality) by $A_{\underline{c},\underline{k}}$ that has orthogonal columns, yielding $I(S; y_{\underline{c}}|\underline{K}) = q \log_2(1 + \beta\rho)$. This proves the following:

Theorem (Necessary Condition). The optimal sampling density $\rho = p/N$ has to satisfy

$$\rho \log_2(1 + \beta\Omega) \geq \frac{1}{N}\left[\log_2\binom{N}{q} - H_b(P_e) - P_e \log_2\left(\binom{N}{q} - 1\right)\right] + \Omega \log_2(1 + \beta\rho)$$

Letting $N \to \infty$ in the theorem, we obtain

$$\rho \log_2(1 + \beta\Omega) \geq \Omega \log_2(1 + \beta\rho) + (1 - P_e) H_b(\Omega), \quad (2)$$

which is sharp in the limit $\beta \to \infty$, because it reduces to $\rho \geq \Omega$. For finite SNR β, $\rho > \Omega$, with the excess density given by (2).

References

[1] R. E. Kahn and B. Liu, "Sampling representations and the optimum reconstruction of signals," *IEEE Trans. Info. Theory*, vol. 11, pp. 339–347, 1965.

[2] P. Feng and Y. Bresler, "Spectrum-blind minimum-rate sampling and reconstruction of multiband signals," in *Proc. IEEE Int. Conf. Acoust. Speech Sig. Proc.*, Atlanta, GA, May 1996, vol. 3, pp. 1689–1692.

[3] M. Gastpar and Y. Bresler, "On the necessary density for spectrum-blind nonuniform sampling subject to quantization," in *Proc. IEEE Int. Conf. Acoust. Speech Sig. Proc.*, Istanbul, Turkey, June 2000.

[4] R. Venkataramani and Y. Bresler, "Further results on spectrum blind sampling of 2D signals," in *Proc. IEEE Int. Conf. Image Proc., ICIP*, Chicago, Oct. 1998, vol. 2, pp. 752–756.

[1]This work was supported in part by by NSF Grant No. MIP 97-07633 and DARPA Contract F49620-98-1-0498, administered by AFOSR.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Decoding the 6-error-correcting $\mathbf{Z}_4$-linear Calderbank-McGuire code

Jyrki Lahtonen, *Member*, IEEE
Department of Mathematics,
University of Turku, FIN-20014,
Turku, Finland.

I. Introduction

Calderbank and McGuire discovered 2 remarkable $\mathbf{Z}_4$-linear codes [2],[3]. The binary Gray images of these codes have respective parameters $(64, 2^{37}, 12)$ and $(64, 2^{32}, 14)$ and thus have 2 (resp. 4) times as many code words as the best known linear codes of the same length and minimum distance.

A decoding algorithm for the 5-error-correcting code is given in [4]. The approach there (following the ideas of the pioneers of $\mathbf{Z}_4$-codes) is to split the study into several cases according to the Lee type of the error vector. Then the Galois ring algebra is used to decide, whether the syndromes are compatible with an error vector of the prescribed type. Unfortunately, it seems to be very difficult to apply this method to the case of the six-error-correcting code. A different approach (presented as an alternative in [4]) is required.

Using the ideas presented here it is easy to also develop a list decoding algorithm for the 5-error-correcting code. I will discuss this possibility.

II. Outline of the decoding algorithm

The 6-error-correcting Calderbank-McGuire code C is a submodule of $\mathbf{Z}_4^{32}$. The code is defined by BCH-like parity checks involving the elements of the Teichmuller set inside the Galois ring $GR(4^5)$. If β is a generator of the non-zero Teichmuller elements, the code C is defined by the following $GR(4^5)$-valued parity checks

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \beta & \beta^2 & \cdots & \beta^{30} \\ 0 & 1 & \beta^3 & \beta^6 & \cdots & \beta^{90} \\ 0 & 1 & \beta^5 & \beta^{10} & \cdots & \beta^{150} \end{pmatrix}.$$

We remark that a parity check for the 5-error-correcting Calderbank-McGuire code is obtained from the above matrix H simply by multiplying the last row by 2.

We express words $\mathbf{x}$ of C 2-adically, i.e. $\mathbf{x} = \mathbf{u}(\mathbf{x}) + 2\mathbf{v}(\mathbf{x})$, where $\mathbf{u}$ and $\mathbf{v}$ are binary vectors of length 32. Using H it is easy to see (cf. [3]) that here $\mathbf{u}$ must be a word of the Reed-Muller code $R(2,5)$ and that each $\mathbf{u} \in R(2,5)$ determines a coset $f(\mathbf{u}) + R(2,5)$ with the property that $\mathbf{u} + 2\mathbf{v} \in C$, if and only if $\mathbf{v} \in f(\mathbf{u}) + R(2,5)$. One of the reasons, why C has such nice distance properties is that $f(\mathbf{u}) + R(2,5)$ is actually in $R(3,5)/R(2,5)$, whenever $\mathbf{u}$ is a vector of minimum weight 8.

We can similarly write any error vector $\mathbf{e}$ in the form $\mathbf{e} = \mathbf{u}(\mathbf{e}) + 2\mathbf{v}(\mathbf{e})$ with binary $\mathbf{u}$ and $\mathbf{v}$. Here simple key observations are that in order to get an error vector $\mathbf{e}$ of Lee weight at most 6, the Hamming weight of $\mathbf{u}$ must not exceed 6. Furthermore, if the Hamming weight of $\mathbf{u}$ is 5 or 6, then the support of $\mathbf{v}$ must be contained in the support of $\mathbf{u}$. Another useful observation is that, if we also consider $-\mathbf{e} = \mathbf{u}(\mathbf{e}) + 2(\mathbf{v}(\mathbf{e}) + \mathbf{u}(\mathbf{e}))$, we see that either $\mathbf{v}(\mathbf{e})$ or $\mathbf{v}(-\mathbf{e}) = \mathbf{v}(\mathbf{e}) + \mathbf{u}(\mathbf{e}) \pmod 2$ has Hamming weight at most 3.

So given a received vector $\mathbf{y} = \mathbf{u}(\mathbf{y}) + 2\mathbf{v}(\mathbf{y}) = \mathbf{x} + \mathbf{e}, \mathbf{x} \in C$ we decode it as follows. First reduce the $\mathbf{Z}_4$-valued components modulo 2 and then decode the resulting vector $\mathbf{u}(\mathbf{y})$ with a *full* decoding algorithm for the code $R(2,5)$. We require such a decoding algorithm theat gives a list all possible error patterns of weight at most 6, i.e. all the words of weight at most 6 that lie in the coset $\mathbf{u}(\mathbf{y}) + R(2,5)$. These are then the candidates for the vector $\mathbf{u}(\mathbf{e})$. We then process the list and for all candidates $\mathbf{u}$ try to find a matching $\mathbf{v}$ taking all the above observations into account.

III. Full decoding of $R(2,5)$

A complete decoding algorithm for $R(2,5)^*$ has been given by Seroussi and Lempel [5]. It is based on an earlier binary matrix factorization algorithm due to Lempel. I will describe that algorithm as an application of the theory of symmetric bilinear forms over a binary vector space. It is quite simple to extend their algorithm to a complete decoding algorithm for $R(2,5)$. The covering radius of $R(2,5)$ is six. So after this stage we get a single candidate $\mathbf{u}$, namely a coset leader of $\mathbf{u}(\mathbf{y}) + R(2,5)$.

The weight distribution of all the cosets of $R(2,5)$ has been determined by Berlekamp and Welch [1]. From their data one sees that any coset has at most 8 words of weight at most 5 and at most 35 words of weight 6. Altogether our list of candidates $\mathbf{u}$ may contain up to 36 elements. Luckily simple applications of affine geometry allow us to find all the low weight words in a coset, when a leader is known. A relatively efficient way of achieving this is to precompute look-up tables of low weight words for certain standard coset leaders (one for each orbit of the group of affine transformations) and modify the Lempel–Seroussi algorithm to always reduce into one of the standard cases. Thus we can meet all the requirements of the main algorithm and hence succesfully decode all the error patterns of Lee weight at most 6.

References

[1] E. R. Berlekamp and L. R. Welch,"Weight Distribution of the Cosets of the (32,6) Reed–Muller Code," *IEEE Trans. Inform. Theory*, vol. 18 no. 1, pp. 203–207, January 1972.

[2] A. R. Calderbank and G. McGuire, "Construction of a $(64, 2^{37}, 12)$ code via Galois rings," *Des. Codes Cryptogr.*, vol. 10 no. 2, February 1997.

[3] A. R. Calderbank, G. McGuire, P. V. Kumar and T. Helleseth, "Cyclic Codes Over $\mathbf{Z}_4$, Locator Polynomials, and Newton's Identitied," *IEEE Trans. Inform. Theory*, vol. 42 no. 1, pp. 217–226, January 1996.

[4] C. Rong, T. Helleseth and J. Lahtonen, "On Algebraic Decoding of the $\mathbf{Z}_4$-linear Calderbank–McGuire Code," *IEEE Trans. Inform. Theory*, vol. 45 no. 5, pp. 1423–1434, July 1999.

[5] G. Seroussi and A. Lempel, "Maximum Likelihood Decoding of Certain Reed–Muller codes," *IEEE Trans. Inform. Theory*, vol. 29 no. 3, pp. 448–450, May 1983.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On Algebraic Decoding of the $\mathbb{Z}_4$-Linear Goethals-like Codes

Kalle Ranto
Turku Centre for Computer Science
Lemminkäisenkatu 14 A
FIN-20520 Turku, Finland
e-mail: kara@utu.fi

Abstract — **We present an algebraic decoding algorithm for all $\mathbb{Z}_4$-linear Goethals-like codes $\mathcal{C}_k$ introduced by Helleseth et al. We show how Dickson polynomials can be used to solve syndrome equations.**

I. Introduction

Let m be an odd integer and let $\mathbb{Z}_4$ denote the ring of integers modulo 4. Let also $R = \mathrm{GR}(4, m)$ be a Galois ring of characteristic 4 with 4^m elements. The group of units in R contains a unique cyclic subgroup $\mathcal{T} = \{0, 1, \beta, \ldots, \beta^{2^m-2}\}$ of order $2^m - 1$. Every element of R can be expressed uniquely in the form $A + 2B$ where $A, B \in \mathcal{T}$. We have the natural modulo 2 reduction map $\mu : R \to \mathbb{F}$ where $\mathbb{F}$ is a finite field of order 2^m. The Gray map $\phi : \mathbb{Z}_4^{2^m} \to \mathbb{F}_2^{2^{m+1}}$, defined by $\phi(0) = 00$, $\phi(1) = 01$, $\phi(2) = 11$ and $\phi(3) = 10$, maps a $\mathbb{Z}_4$-codeword componentwisely to a binary codeword.

Helleseth, Kumar and Shanbhag [1] observed that the $\mathbb{Z}_4$-linear codes $\mathcal{C}_k$ with parity-check matrices

$$H_k = \begin{bmatrix} 1 & 1 & 1 & 1 & \ldots & 1 \\ 0 & 1 & \beta & \beta^2 & \ldots & \beta^{2^m-2} \\ 0 & 2 & 2\beta^{2^k+1} & 2\beta^{(2^k+1)2} & \ldots & 2\beta^{(2^k+1)(2^m-2)} \end{bmatrix}$$

have the same weight distributions whenever $\gcd(k, m) = 1$. They have $2^{2m+1-3m-2}$ codewords and minimum Lee distance 8. The Gray images of these codes $\phi(\mathcal{C}_k)$ are nonlinear binary codes which have the same Hamming weight distribution as the Goethals code. Helleseth and Kumar [2] presented a complete decoding algorithm for the code $\mathcal{C}_1$. In this talk we sketch an algebraic decoding algorithm for all codes $\mathcal{C}_k$, which corrects errors with Lee weight ≤ 3.

II. Dickson polynomials

In the decoding procedure we solve the roots of an equation $D_n(x, u) = v$, where $\gcd(n, 2^m - 1) = 1$ and

$$D_n(x, u) = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n}{n-i} \binom{n-i}{i} (-u)^i x^{n-2i}$$

is a Dickson polynomial. It satisfies the functional equation $D_n(x + y, xy) = x^n + y^n$, which implies that the roots can be solved effectively by Cardan's method.

For further details see for example the survey [3].

III. Main results

Let X, Y, Z, A, B, C denote elements in $\mathcal{T}$ and x, y, z, a, b, c their images in $\mathbb{F}$ under μ-mapping. The syndrome of the error vector $\mathbf{e} \in \mathbb{Z}_4^{2^m}$ is $\mathbf{S} = \mathbf{e}H_k^T = (t, A + 2B, 2C)$, where $t \in \mathbb{Z}_4$. The decoding algorithm in [2] can be straightforwardly generalized in the cases $t = 0$ and $t = 2$ but in the case $t = \pm 1$ we need the Dickson polynomials.

Theorem 1. *Let $\mathbf{S} = (1, A+2B, 2C)$ denote the syndrome of a coset.*

(i) If $b = 0$ and $c = a^{2^k+1}$, then the coset leader has Lee weight 1 and is uniquely determined by $x = a$ and $e_X = 1$.

(ii) If $b \neq 0$ and $c = a^{2^k+1}$, then the coset leader has Lee weight 3 and is uniquely determined by $x = a+b$, $e_X = 2$, $y = a$, and $e_Y = 3$.

(iii) If $b \neq 0$, $c \neq a^{2^k+1}$ and $\mathrm{Tr}(\frac{b^{2^k+1}}{a^{2^k+1}+c}) = 0$, then the coset leader has Lee weight 3. The coset leader is uniquely determined by $e_X = e_Y = 1$, $e_Z = 3$, $D_{2^k-1}(z + a, b^2) = \frac{a^{2^k+1}+c}{b^2}$ and x and y are the zeros of $T^2 + (z + a)T + b^2 + az = 0$. In particular in the case $k = 2$ the variable z should satisfy $(z + a)^3 + b^2(z + a) = \frac{a^5+c}{b^2}$.

(iv) If $b \neq 0$, $c \neq a^{2^k+1}$ and $p(T) = T^3 + aT^2 + (a^2 + b^2)T + \sigma_3$ has three distinct zeros in $\mathbb{F}$ where σ_3 satisfies $D_n(\sigma_3 + a^3 + ab^2, b^6) = \frac{a^{2^k+1}+c}{d}$ and

$$\begin{cases} n = \frac{2^k+1}{3} \text{ and } d = 1 & \text{if } 2 \nmid k \\ n = \frac{2^k-1}{3} \text{ and } d = b^2 & \text{if } 2 \mid k, \end{cases}$$

then a coset leader has Lee weight 3 and is uniquely determined such that x, y, z are the three distinct zeros of $p(T)$ in $\mathbb{F}$ and $e_X = e_Y = e_Z = 3$. Especially, when $k = 2$ the condition for σ_3 can be stated as $\sigma_3 = \frac{c+a^5+a^3b^2+ab^4}{b^2}$.

(v) If none of (i)–(iv) hold, then any coset leader has Lee weight ≥ 5.

Acknowledgments

The author wishes to thank Jyrki Lahtonen for several useful discussions and also for suggesting this problem.

References

[1] Tor Helleseth, P. Vijay Kumar, and A. Shanbhag, "Codes with the Same Weight Distributions as the Goethals Codes and the Delsarte-Goethals Codes," *Designs, Codes and Cryptography*, vol. 9, no. 3, pp. 257–266, 1996.

[2] Tor Helleseth and P. Vijay Kumar, "The Algebraic Decoding of the Z_4-Linear Goethals Code," *IEEE Trans. Inform. Theory*, vol. 41, no. 6, pp. 2040–2048, 1995.

[3] R. Lidl, G. L. Mullen, and G. Turnwald, *Dickson polynomials*, vol. 65 of *Pitman Monographs and Surveys in Pure and Applied Mathematics*, Longman Scientific & Technical, Harlow, 1993.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Gröbner Bases and Alternant Codes over Galois Rings

Eimear Byrne
Department of Mathematics
National University of Ireland
Cork, Ireland
e-mail: eimear.byrne@ucc.ie

Patrick Fitzpatrick
Department of Mathematics
National University of Ireland
Cork, Ireland
e-mail: fitzpat@ucc.ie

Abstract —

We give a new algorithm for the solution of the Hamming metric decoding problem for alternant codes over a Galois ring R. First we develop a comprehensive theory of Grobner bases over $R[x_1, \ldots, x_n]$, which is of independent interest. By specialising to the case of one variable, we show that the solution of the key equation can be determined as a certain minimal element in a Gröbner basis of the solution module.

I. Introduction

In [IPE97] a modified Berlekamp-Massey algorithm was presented as part of a (Hamming metric) decoding procedure for BCH and RS codes defined over Galois rings. The problem of constructing and decoding alternant codes over Galois rings was addressed in [AIP98] by adapting the techniques of [IPE97]. In this paper we give a new algorithm for decoding alternant codes over Galois rings.

Let $P = GR(p^n, r_1)$ be a Galois ring of characteristic p^n defined by a basic irreducible polynomial of degree r_1 over $\mathbf{Z}_{p^n}$, and let $R = GR(p^n, r_2)$ be the Galois extension of P, where $r_1 \mid r_2$, defined by a basic irreducible polynomial of degree r_2/r_1 over P. Let R^* be the group of units of R, and let $G = \langle \zeta \rangle$ be the unique cyclic subgroup of R^* of order $p^{r_2} - 1$, whose elements are the roots of $x^{p^{r_2}-1} - 1$. An alternant code $C(N, r, \alpha, \gamma, P)$ of length N with symbols from P is defined as follows. Let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_N)$ be a vector of distinct elements of R, with the condition that $\alpha_i - \alpha_j$ be a unit for all $i \neq j$, and let $\gamma = (\gamma_1, \gamma_2, \ldots, \gamma_N)$ be a vector with non-zero components $\gamma_j \in R^*$. The *alternant code* $C = C(N, r, \alpha, \gamma, P)$ is the P–submodule of P^N defined by the parity check matrix

$$\mathbf{H} = \begin{pmatrix} \gamma_1 & \gamma_2 & \cdots & \gamma_N \\ \gamma_1\alpha_1 & \gamma_2\alpha_2 & \cdots & \gamma_N\alpha_N \\ \vdots & \vdots & \vdots & \vdots \\ \gamma_1\alpha_1^{q-1} & \gamma_2\alpha_2^{q-1} & \cdots & \gamma_N\alpha_N^{q-1} \end{pmatrix}.$$

A straightforward modification of the BCH bound establishes that C has minimum Hamming distance greater than q. Error polynomials, the syndrome polynomial S, the error locator polynomial Σ, and the error evaluator polynomial Ω all take the same form as their counterparts over a field and satisfy the key equation $\Sigma S \equiv \Omega \bmod x^q$. The decoding problem is equivalent to solving this congruence subject to certain conditions.

In [F95] new algorithms corresponding to the Euclidean, Berlekamp-Massey, and Peterson-Gorenstein-Zierler algorithms for the solution of the key equation were derived using Gröbner bases. Each of these algorithms is computationally at least as efficient as its classical analogue [F95, FJ98]. This approach has been extended to rational approximation and interpolation problems, and to the solution of multivariable congruences [F96, F97]. In this paper we apply similar principles to decoding alternant codes defined over a Galois ring.

II. Gröbner bases in $R[x_1, \ldots, x_n]$

We generalise the theory of Gröbner bases to the specific context of a Galois ring R. Many of our results are exact analogues of those holding over a field. However, their proofs are complicated by the change in significance of the coefficients, which may be zero divisors in R. We establish a division algorithm and the existence of Gröbner bases and give a generalisation of Buchberger's algorithm in which, at each stage, a set of (appropriately defined) S–polynomials to be included in the new basis is augmented by certain p-power multiples of the elements of the current basis.

III. Gröbner bases in $R[x]^2$ and decoding

The general structure of a Gröbner basis of a submodule of $R[x]^2$ is given by

Theorem 1 *Let A be an R–submodule of $R[x]^2$ Then A has a Gröbner basis of the form*

$$\{(a_0, b_0), \ldots, (a_{n-1}, b_{n-1}), (c_0, d_0), \ldots, (c_{n-1}, d_{n-1})\}$$

satisfying, for all $i, j \in \{0, \ldots, n-1\}$
i. $\mathrm{lm}(a_i, b_i) = (p^i x^{\partial a_i}, 0)$, $\mathrm{lm}(c_i, d_i) = (0, p^j x^{\partial d_j})$
ii. $\partial a_i \leq \partial a_j$ *for* $i \geq j$, $\partial d_i \leq \partial d_j$ *for* $i \geq j$.

Define the solution module $M = \{(a, b) : aS \equiv b \bmod x^q\}$. It is easy to see that $\{(1, S), (0, x^q)\}$ is a basis of M. Our main result is that the required solution may be found by converting this to a Gröbner basis.

Theorem 2 *The solution (Σ, Ω) of the key equation required for decoding the alternant code $C(N, r, \alpha, \gamma, P)$ is (up to equivalence) the minimal regular element of the Gröbner basis of the solution module M under the term order $<_{-1}$.*

References

[AIP98] A. de Andrade, J. C. Interlando, and R. Palazzo Jnr., On alternant codes over commutative rings, preprint.

[F95] P. Fitzpatrick, On the key equation, *IEEE Trans. IT* 41 (1995) 1290-1302.

[F96] ———, On the scalar rational interpolation problem, *Math. Contr. Sig., Syst.* 9, (1996) 352-369.

[F97] ———, Solving multivariable congruences by change of term order, *J. Symb. Comp.*, 24 (1997) 505–510.

[FJ98] ———, S.M. Jennings, Comparison of two algorithms for decoding alternant codes, *Appl. Alg. in Eng., Comm. and Comp.* 9 (1998) 211–220.

[IPE97] J. C. Interlando, R. Palazzo Jnr., M. Elia, On the decoding of Reed-Solomon and BCH codes over integer residue rings, *IEEE Trans. IT* 43 (1997) 1013-1021.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

$O(\log_2 m)$ Iterative Algorithm for Multiplicative Inversion in $GF(2^m)$

Sumio Morioka and Yasunao Katayama
IBM Research, Tokyo Research Laboratory
1623-14 Shimotsuruma, Yamato, Kanagawa 242-8502, Japan
{E02716, yasunaok}@jp.ibm.com

Abstract — **A new algorithm that can calculate the multiplicative inverses in $GF(2^m)$ with $O(\log_2 m)$ iterations is presented. While this algorithm requires in total the same number of multiplications ($[\log_2(m-1)] + Hw(m-1) - 1$) with the best known algorithm [1], the latency, if mapped to a hardware, can be reduced significantly ($[\log_2(m-2)] + 1$), comparable to the best case result, which is implemented using Fermat's little theorem.**

I. Traditional Algorithms

One of the famous inversion algorithms is to calculate a formula $x^{-1} = x^{2^m-2} = x^{2^1} x^{2^2} \cdots x^{2^{m-1}}$, following Fermat's little theorem (Figure 1a). If this formula is mapped into a sequential circuit, the latency is $m-2$ multiplications. If mapped to a combinational circuit, the latency can be improved to $[\log_2(m-2)] + 1$ by arranging multiplications like a tree.

In [1], Itoh and Tsujii proposed an improved algorithm that requires the least number of multiplications ever known (Figure 1b). The latency is at most twice as long as that of Fermat's theorem; $[\log_2(m-1)] + Hw(m-1) - 1$ multiplications where $Hw()$ denotes Humming weight. It is difficult to shorten the latency, since the multiplications need to be performed in a sequential manner.

II. The Proposed Algorithm

Figure 2 shows our new algorithm and Figure 3 shows some example computation sequences by using our algorithm. After the $([\log_2(m-1)] + 1)$-th iteration of for-loop, a multiplicative inverse is obtained in a register y_2. Please note that the first multiplication to y_2 and the last multiplication to y_1 are always unnecessary, although this is not described in Figure 2, for simplicity.

Clearly, our algorithm requires in total the same number of multiplications with Itoh and Tsujii's algorithm. The latency, however, is only $[\log_2(m-2)] + 1$ multiplications, since in the for-loop, calculation of the values of y_1 and y_2 can be performed in parallel, if mapped to a hardware. This algorithm can be used in any value of m and any basis representations, and also can be implemented not only as a sequential circuit but also as a combinational circuit. We believe that combining our algorithm with a composite-field based method in [1,2] will make a very fast and compact inversion circuit possible, if m is not a prime number.

Appendix. Correctness Proof of Our Algorithm

Suppose that $m-1$ is represented by

$$m-1 = \Sigma_{i=0}^{s} 2^{t_i} \quad \text{where} \quad t_s > t_{s-1} > \cdots > t_0. \tag{1}$$

From (1),

$$\forall k (s \geq k \geq 1); (m-1) \bmod 2^{t_k} = \Sigma_{i=0}^{k-1} 2^{t_i}, \tag{2}$$

and also

$$(m-1) \bmod 2^{t_0} = 0. \tag{3}$$

From Figure 2, the output of our algorithm x_{out} is

$$x_{out} = \Pi_{h=0}^{s} x * *\{(2^{(2**t_h)} - 1) \cdot 2^{(((m-1) \bmod (2**t_h))+1)}\}. \tag{4}$$

From (2),(3) and (4),

$$x_{out} = x * *(\Sigma_{h=0}^{s}(2^{u_h} - 2^{u_{h-1}})) \quad \text{where} \quad u_h = (\Sigma_{i=0}^{h} 2^{t_i}) + 1. \tag{5}$$

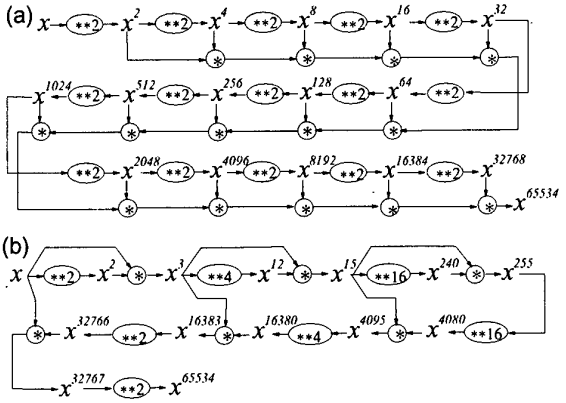


Figure 1. Computation sequences of multiplicative inverse ($m = 16$). (a) Fermat's little theorem. (b) Itoh and Tsujii's algorithm.

```
y1 := x;
y2 := 1;
for k = 0 to [log2(m-1)] do begin
  if (bit-k of (m-1)) = 1 then
    y2 := y2 × (y1 * *2^(((m-1) mod (2**k))+1));
  end if;
  y1 := y1 × (y1 * *2^(2**k));  /* x * *(2^(2**(k+1)) - 1) will be stored */
end for;
write y2;
```

Figure 2. The proposed iterative algorithm.

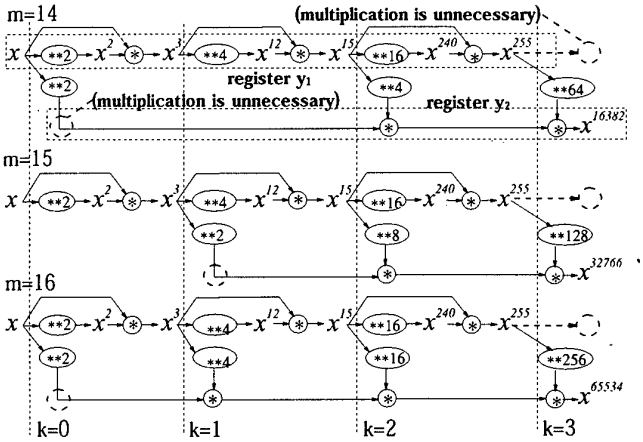


Figure 3. Computation sequences by our algorithm.

From (1) and (5),

$$x_{out} = x * *(2^{u_s} - 2^1) = x * *(2^m - 2) = x^{-1}. \qquad \square$$

References

[1] T.Itoh and S.Tsujii, "A Fast Algorithm for Computing Multiplicative Inverses in $GF(2^m)$ Using Normal Bases," *Information and Computation,* vol.78, no.3, pp.171-177, 1988.

[2] J.Guajardo and C.Paar, "Efficient Algorithms for Elliptic Curve Cryptosystems," *proc. of 17th Annual Intl. Cryptology Conf. (CRYPTO'97)*, LNCS1294, pp.342-356, 1997.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Interleavers for Unpunctured Symmetric Turbo Codes

Johann A. Briffa
Dept. Comms. & Computer Eng.
University of Malta
Msida MSD 06, Malta
E-mail: jabrif@eng.um.edu.mt

Victor Buttigieg
Dept. Comms. & Computer Eng.
University of Malta
Msida MSD 06, Malta
E-mail: vjbutt@eng.um.edu.mt

Abstract — **The Turbo code interleaver design problem is considered for relatively large block sizes, where the effect of trellis termination is less marked. An optimised interleaver design technique based on simulated annealing is proposed – performance is significantly better than the Berrou-Glavieux interleaver without an increase in delay.**

I. Introduction

The classical use of interleavers is to randomise the location of errors, enabling the use of random-error-correcting codes on channels with burst error patterns. Turbo coding also introduces a further dimension to interleaver requirements, due to the effects of the iterative algorithm. Most optimised interleaver design techniques in the literature are based on the JPL's S-random interleaver algorithm [1]. While S-random interleavers perform well, the technique was not intended as a basis for advanced interleaver design. Its main shortcomings are that it is not guaranteed to produce the required interleaver and that it only aims at achieving a spread S.

II. Optimised Interleaver Design

Simulated annealing [2] can be used to design optimised interleavers by defininining an energy function based on a predefined set of requirements. We use a random interleaver as an initial state, and define the perturbation function as a swap of two random interleaver entries, ensuring that the interleaver is always valid. The energy function used is:

$$E = \sum_{i,j} \frac{5.\nu}{\sqrt{(i-j)^2 + [\lambda(i) - \lambda(j)]^2}} \qquad (1)$$

where $i, j \in [0, \tau - 1]$, τ is the block size, ν is the encoder memory, and $\lambda()$ is the interleaving function. This energy function attempts to 'push' bit-pairs away from the origin in the Input-Output Distance Spectrum (IODS)[1], increasing the spread of the interleaver. In contrast with the JPL technique it does not guarantee a particular spread; however, it pushes points away from the origin even beyond the spread boundary.

III. Results

We restrict ourselves to unpunctured rate-$\frac{1}{3}$ symmetric Turbo codes with $\nu = 2$ and generator[2] $(1, 5/7)$. In order to avoid the effects of trellis termination, we also choose $\tau = 1024$. As a reference for performance, we implement a uniform interleaver by using a different random interleaver for every block simulated [3]. We compare our interleaver design with this uniform interleaver, a rectangular interleaver, the design used by Berrou and Glavieux [4], and an S-random interleaver in Fig. 1. Our design achieves a BER of 10^{-5} at $\frac{E_b}{N_0} = 1.35$ dB.

[1] A two-dimensional histogram, with the axes being the distance between bit-pairs at the input and output of the interleaver [3].

[2] Polynomials are denoted as g_a or g_a/g_b, where g_a is the feedforward and g_b is the feedback polynomial, in octal.

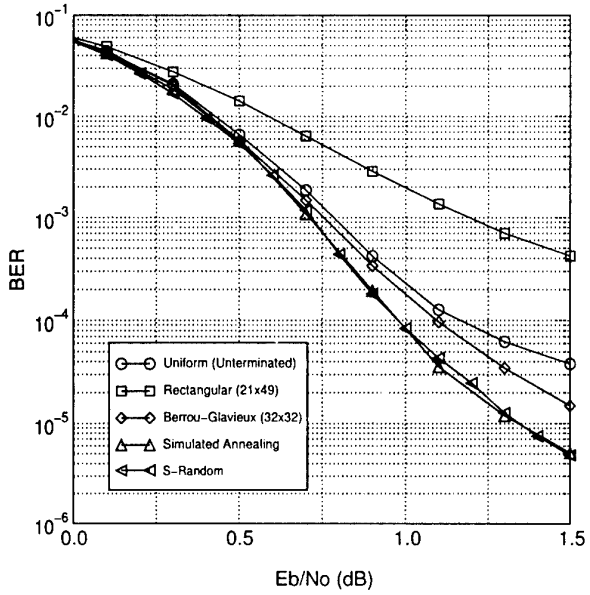


Fig. 1: Turbo code BER simulation (10 iterations)

IV. Conclusions

Our new interleaver design performs at least as well as the S-random interleaver. However, using our technique it is easier to include design restrictions, for example to make the interleaver correctly-terminating or odd-even. Also, more sophisticated energy functions matched to the component codes may be considered, particularly for use with punctured codes. Utilising some performance enhancement techniques, the complexity of the energy function grows only as $O(\tau)$, making it suitable for use with large block sizes.

References

[1] Dariush Divsalar and Fabrizio Pollara, "Multiple turbo codes for deep-space communications," TDA progress report 42-121, Jet Propulsion Laboratory, California Institute of Technology, May 15th, 1995.

[2] William H. Press, Saul A. Teukolsky, William T. Vetterling, and Brian P. Flannery, *Numerical Recipes in C: The Art of Scientific Computing*, Cambridge Universty Press, second edition, 1992.

[3] Johann A. Briffa, *Interleavers for Turbo Codes*, M.Phil. thesis, University of Malta, Faculty of Engineering, 1999.

[4] Claude Berrou and Alain Glavieux, "Near optimum error correcting coding and decoding: Turbo-codes," *IEEE Transactions on Communications*, vol. 44, no. 10, pp. 1261–1271, Oct. 1996.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Interleaver Design Using Backtracking and Spreading Methods

Marco Breiling[1], Stein Peeters[2], and Johannes Huber
Lehrstuhl für Nachrichtentechnik II, Universität Erlangen-Nürnberg, Cauerstr. 7, D-91058 Erlangen, Germany
Tel.: (+) 9131-85-27668, Fax: (+) 9131-85-28919, Email: breiling@LNT.de, http://www.LNT.de/~breiling

Abstract — **We propose a new algorithm for Turbo code interleaver design, which is based on the conventional s–random approach and whose complexity grows only linearly with the interleaver length.**

Designing the interleaver $\boldsymbol{\pi} = (\pi_1; ..; \pi_K)$ of length K of a Turbo code serves to increase the code's minimum distance $\delta_{\min}$ and hence to lower the *error floor* of the Word and Bit Error Rates (WER/BER). An efficient method was presented in [1]. Examinations show that for so–designed interleavers, the codeword at $\delta_{\min}$ is mainly caused by a combination of an input word $\mathbf{u}^{(1)}$ of the first component encoder (identical to the Turbo encoder input $\mathbf{u}$) and a second component input word $\mathbf{u}^{(2)}$ as shown in Fig. 1. In this example, "1001" represents an *error pattern*, i.e. an input sequence causing a **short** error event in a component code trellis. The s–random interleaver $\boldsymbol{\pi}$ does not avoid that the four "1"s in the *two* error patterns of $\mathbf{u}^{(1)}$ are mapped crosswise to *two* error patterns in $\mathbf{u}^{(2)}$, since the two "1"s belonging to each error pattern in $\mathbf{u}^{(1)}$ are spread to distant positions in $\mathbf{u}^{(2)}$, and hence the spreading condition of [1] is satisfied. However, this unlucky mapping of positions can be avoided and $\delta_{\min}$ can be increased by modifying the interleaver design algorithm.

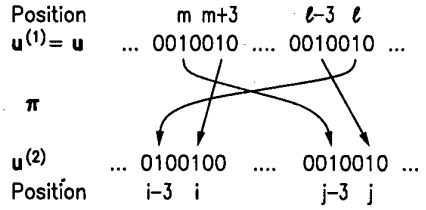


Figure 1: Unlucky mapping of positions

The proposed algorithm incorporates the s–random method of [1] and hence, it successively determines π_1 to π_K. In step l, we set up the set $\mathcal{A}_l \subset \{1; ..; K\}$ of possible values for π_l, which have not already been assigned to π_t in earlier steps $t < l$, and which satisfy the spreading condition of [1]. Moreover, step l consists in determining and discarding values of $\mathcal{A}_l$, which would cause an unlucky mapping like in Fig. 1.

Determining these unfavourable values in $\mathcal{A}_l$ can be done very efficiently using a recursive backtracking approach, which is shortly outlined using the example of Fig. 1. Our basic observation is that any "1" present in $\mathbf{u}^{(1)} = (u_1^{(1)}; ..; u_K^{(1)})$ or $\mathbf{u}^{(2)} = (u_1^{(2)}; ..; u_K^{(2)})$, respectively, must belong to an error pattern. Otherwise the associated codeword has large weight and can be ignored, since we consider and try to avoid only low weight codewords. In step l, we consider exclusively $\mathbf{u}^{(1)}$ with $u_l^{(1)} = 1$ and $u_t^{(1)} = 0$, $\forall t > l$. Our starting point for the backtracking is that the "1" in $u_l^{(1)}$ must belong to an error pattern (as reasoned above). Every possible error pattern must be considered, and for each of them, we must proceed in a backtracking manner. In our example of Fig. 1, we consider only the error pattern "1001" in $u_{l-3}^{(1)}$ to $u_l^{(1)}$. Since $\pi_{l-3} = j$ has already been determined, we know that $u_j^{(2)} = 1$. Following the above reasoning, the "1" in $u_j^{(2)}$ must belong to an error pattern, for which we must consider every possibility. In the Fig., we consider "1001" in $u_{j-3}^{(2)}$ to $u_j^{(2)}$. For the case that $j-3$ has earlier been assigned to π_m, $m < l$, we conclude that $u_m^{(1)} = 1$. Every possible new error pattern containing $u_m^{(1)} = 1$ must be considered in $\mathbf{u}^{(1)}$ (in the Fig. "1001" in $u_m^{(1)}$ to $u_{m+3}^{(1)}$). Finally, for $\pi_{m+3} = i$, we find that $u_i^{(2)} = 1$. We must thus discard $i-3$ from $\mathcal{A}_l$, since this prevents the assignment $\pi_l = i-3$, which would otherwise complete the unlucky mapping in Fig. 1. When all unfavourable values have been discarded from $\mathcal{A}_l$, then π_l is randomly chosen from the remaining values. The backtracking algorithm works also for error patterns of weight > 2. The complexity of a complete interleaver design grows linearly with K.

We verified the proposed algorithm by designing an interleaver of length $K = 200$ for a Turbo code of rate 1/2 employing $M = 2$ component codes (generator polynomials: $(1; 5/7)$). In the design, we used $s = 8$ and considered all error patterns of weight ≤ 3. For a termination of both component trellises, this Turbo code attains $\delta_{\min} = 14$. Fig. 2 shows the WER (upper curves) and BER (lower curves) for varying E_b/N_0 (received energy per information bit over the one–sided noise power spectral density) for a simulated transmission using coded BPSK over an AWGN channel. The performance is compared to using a pure s–random interleaver [1] with $s = 10$ (expected $\delta_{\min} \leq 12$) and a *uniform interleaver* [2] (mean $\delta_{\min} \leq 6$) of the same length. We can clearly see the improved BER and particularly WER for higher E_b/N_0.

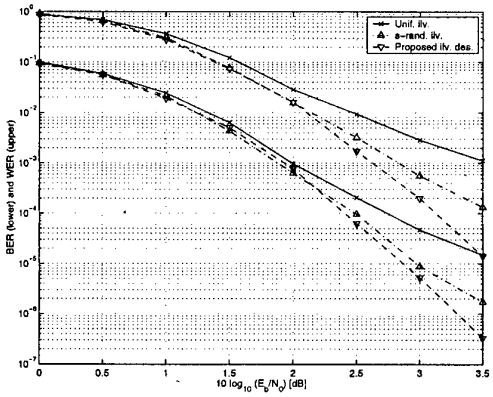


Figure 2: Simulation results

References

[1] S. Dolinar and D. Divsalar, "Weight Distributions for Turbo Codes Using Random and Nonrandom Permutations", *JPL-TDA Progress Report*, pp. 56–65, 1995.

[2] S. Benedetto and G. Montorsi, "Unveiling Turbo Codes: Some Results on Parallel Concatenated Coding Schemes", *IEEE Trans. on Info. Th.*, pp. 409–428, 1996.

[1]M. Breiling is sponsored by the Fraunhofer Gesellschaft – Institut für Integrierte Schaltungen, Erlangen.

[2]S. Peeters is now working for BU Satellite Communications, Nortel Dasa Network Systems, Friedrichshafen/Germany.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

An Interleaver Design Algorithm based on a Cost Matrix for Turbo Codes

Didier Le Ruyet
Laboratoire Signaux et Systèmes
Conservatoire National des Arts et Métiers
75141 Paris Cedex 03, France
e-mail: leruyet@cnam.fr

Hong Sun
Departement Electronic and Information Engineering
Huazhong University of Science and Technology
430074 Wuhan, China
e-mail: hsun@hust.edu.cn

Han Vu Thien
Laboratoire Signaux et Systèmes
Conservatoire National des Arts et Métiers
75141 Paris Cedex 03, France
e-mail: vu-thien@cnam.fr

Abstract — **In this paper the design of interleavers for Turbo Codes is considered. The proposed algorithm is based on a Hamming weight cost matrix. It optimizes both the minimal distance of Turbo Codes and the passing of extrinsic information. Simulation results show that for short lengths these interleavers improve the error performances at high SNR.**

I. Introduction

It is admitted that the interleaver is the key element of Turbo Codes [1] [2]. In order to optimize the distance spectrum and the minimal distance of Turbo Codes, the interleaver should map input sequences $u(D)$ which generate low weight output sequences $y_1(D)$ with interleaved sequences $v(D)$ which generate high weight output sequences $y_2(D)$, and vice versa. Due to the iterative structure of the turbo decoder, the interleaver should also guarantee a good passing of extrinsic information from one decoder to the other. The proposed interleaver optimizes both these two criteria. In order to increase the minimal distance, a Hamming weight cost matrix is used for the construction. The second goal is achieved since the proposed interleaver belongs to the family of cycle optimized interleavers [3]. The interleaver is built element by element using a tree search method.

Let $\boldsymbol{u} = [u_0, u_1, \ldots, u_{N-1}]$ and $\boldsymbol{v} = [v_0, v_1, \ldots, v_{N-1}]$ respectively be the input and output sequences of the interleaver. We have the relation : $\boldsymbol{v} = \boldsymbol{u}I$ where $I = \{a_{ij}\}_{N\times N}$ with $a_{ij} \in \{0,1\}$ and $\sum_j a_{ij} = \sum_i a_{ij} = 1$. We can also define the interleaver with the permutation vector $E = [e(0), e(1), e(2), \ldots, e(N-1)]$ where $e(i) = j \Leftrightarrow a_{ij} = 1$

II. Interleaver Design

For the construction of E, we will use a cost matrix J of same dimension as I. $J = \{b_{ij}\}_{N\times N}$ b_{ij} is equal to the Hamming weight of the lowest Hamming weight code generated from the input sequences $u(D)$ with Hamming weight $w \le w_{MAX}$ and supposing $a_{ij} = 1$. Each new element $e(n)$ is chosen according to both criteria defined previously.

1. initialization :
   $b_{ij}(0) = +\infty \quad \forall i, j$
   $e(0)$ is chosen randomly
2. for $(n = 1, 2, \ldots, N-1)$:
   -update of $b_{ij}(n) \quad (i \ge n) \quad \forall j$:

$$b_{ij}(n) = \min\left[b_{ij}(n-1), \min_{\mathcal{C}}\left(w + \sum_{k=0}^{N-1} y_{1k} + \sum_{k=0}^{N-1} y_{2k}\right)\right]$$

with $\mathcal{C} = \{u(D) = D^{l_0} + D^{l_1} + D^{l_2} + \cdots + D^{l_{w-1}}\}$

$$w = \sum_{k=0}^{N-1} u_k \le w_{MAX} \quad \text{and} \quad w \le n+1$$

$$\text{with} \quad l_0 < l_1 < \cdots < l_{w-3} < n-1, \tag{1}$$

$$l_{w-2} = n-1, \quad l_{w-1} > n-1 \tag{2}$$

-choice of $e(n)$:

$$\text{let} \quad \mathcal{E}1 = \{j \mid b_{nj} \ge D_{MAX}\} \tag{3}$$

$$\mathcal{E}2 = \{j \mid |i-j| + |e(i) - e(j)| \ge L, \quad i = n-1, n-2, \ldots, n-L-2\} \tag{4}$$

$e(n) \in \mathcal{E} = \mathcal{E}1 \cap \mathcal{E}2$. $e(n)$ is chosen randomly in $\mathcal{E}$.

Equations (1) and (2) reduce the set $\mathcal{C}$ of input sequences $u(D)$ to test for each n. Equation (3) corresponds to the minimal distance constraint. Equation (4) corresponds to the cycle optimized constraint which imposes that two bits separated by X bits ($X \le L-2$) in the input sequence $u(D)$ should be separated by at least $L-2-X$ bits in the sequence $v(D)$. $\mathcal{E}$ is the set of all the new positions satisfying both constraints. This method allows us to build an interleaver with minimal distance D_{MAX} and minimum cycle L. From [3], it is possible to build an interleaver with $L < \sqrt{N} + 2$. If the tree search fails ($\mathcal{E} = \emptyset$), the procedure should be started again. To obtain an interleaver with the greatest minimal distance, the procedure must be repeated by increasing the value D_{MAX} until it is no longer possible to build the interleaver.

III. Results and Conclusion

Simulations using a R=1/3 Turbo Codes with two 8 states RSC's with generator $(15/17)_8$ were performed. For N=105 bits, the parameters obtained with w_{MAX}=3 are D_{MAX}=19 and L=10. Simulation results show that, at high SNR, the performances of Turbo Codes using this interleaver are 0.1dB better than the best interleavers available in the literature [4].

References

[1] C. Berrou, A. Glavieux, P. Thitimajshima., "Near Shannon limit error correcting coding and decoding : Turbo-codes," *Proc. ICC'93*, Geneva, Switzerland, pp. 1064-1070, May. 1993.

[2] S. Benedetto and G. Montorsi, "Unveiling Turbo Codes: Some Results on Parallel Concatenated Coding Schemes," *IEEE Trans. Inform. Theory*, vol. 42, No. 2, pp. 409-428, March 1996.

[3] D. Le Ruyet and H. Vu Thien, "Design of Cycle Optimized Interleavers for Turbo Codes," *submitted to Int. Symp. on Turbo Codes and Related Topics*, Brest, France, Sept. 2000.

[4] D. Divsalar and F. Pollara, "Weight distributions for Turbo Codes using random and nonrandom permutations," *TDA Progress Report*, 42-123, JPL, pp. 56-65, Aug. 1995.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Interleaver design for Turbo codes

H. Sadjadpour & N. Sloane
AT&T Labs-research,
Florham Park, NJ.

G. Nebe
Lehrstuhl B für Mathematik,
RWTH Aachen, Germany.

M. Salehi
Department of Electrical Eng.,
Northeastern University, MA.

Abstract — **A new interleaver design to improve the performance of the Turbo codes is presented here. Two criteria are considered in the design of the interleaver; the distance spectrum properties of the code and the correlation between the input information data and the soft output of each decoder corresponding to its parity bits. A deterministic interleaver design based on these criteria is also proposed here.**

I. Introduction

Turbo codes[1] have an impressive near Shannon limit error correcting performance. This superior performance of Turbo codes compared to convolutional codes is only achievable when the length of the interleaver is very large, on the order of several thousand bits. For large block size interleavers, most random interleavers perform well.

An interleaver π is a permutation $i \mapsto \pi(i)$ that maps a data sequence of N input symbols into the same sequence in a new order. An S-random [2] interleaver is a semi-random interleaver that performs better than most random interleavers. Each randomly selected integer is compared to S previously selected random integers. If the distance between this integer and previously selected random integers is greater than S, then it is selected. Otherwise, a new random integer will be chosen and this process is repeated until all N distinct integers are selected in this random order. This interleaver design assures that the short cycle events are avoided. Short cycle event occurs when two bits are close to each other before and after interleaving.

II. 2-step S-random interleaver design

A new interleaver design, 2-step S-random interleaver, is presented here based on the S-random interleaver. The 2-step S-random interleaver is designed under the constraint to increase the minimum effective free distance of the Turbo code without increasing the correlation properties between the information input data sequence and the soft output of each decoder corresponding to its parity bits. The criterion used in the second step of the design is based on the revised version of iterative decoding suitability (IDS) condition that is described in [3-4].

Step 1: Each randomly selected integer $\pi(i)$ is compared with the previous selections $\pi(j)$ to check that if $i - j \leq S_1$ then $|\pi(i) - \pi(j)| > S_1$. We also insist that π must satisfy $|i - \pi(i)| > S_2$. S_1 and S_2 are two constants.

Step 2: Choose the maximum pre-determined weight w_{det} for input data sequences and the minimum permissible effective free distance code $d_{min,w_{det}}$. Find all input data sequences of length N and weight $w_l \leq w_{det}$ and their corresponding effective free distance d_{w_l} for the Turbo encoder with an interleaver design based on step 1 such that $d_{w_l} \leq d_{min,w_{det}}$. All these input data sequences are divisible before and after interleaving by the feedback polynomial (usually a primitive polynomial) of the Turbo encoder. Consider the first input data block of weight w_1 with non-zero elements in locations $(i_1, i_2, \ldots, i_{w_1})$ and $d_{w_1} \leq d_{min,w_{det}}$. Compute $IDS_{(new)}$ based on [4] for the original interleaver designed in step 1. Set $j = i_1 + 1$ and find the pair $(j, \pi(j))$. Interchange the interleaver pairs $(i_1, \pi(i_1))$ and $(j, \pi(j))$ to create a new interleaver, i.e., $(i_1, \pi(j))$ and $(j, \pi(i_1))$. Compute the new IDS, $IDS'_{(new)}$, based on the new interleaver design. If $IDS'_{(new)} \leq IDS_{(new)}$, replace the interleaver by the new one. Otherwise, set $j = j + 1$ and continue. Repeat this operation for all input data sequences with a minimum weight of $w_l \leq w_{det}$ and $d_{w_l} \leq d_{min,w_{det}}$. After completing this operation, return to step 2 and find all input data sequences of weight $w_l \leq w_{det}$ with $d_{w_l} \leq d_{min,w_{det}}$ for the new interleaver. Continue this step until it converges and there is no input data sequence of weight $w_l \leq w_{det}$ with $d_{w_l} \leq d_{min,w_{det}}$. Obviously if $d_{min,w_{det}}$ is selected a large value, the second step may never converge, and in this case $d_{min,w_{det}}$ should be reduced.

An interleaver design proposed in [6] is based on the joint S-random criteria and elimination of all error patterns of weight w_i. However, in practice the joint optimization criteria will not converge easily and therefore the value of S must be reduced and w_i restricted to only weight two inputs. By separating these two criteria into two steps, we can easily find the appropriate interleaver satisfying each step separately.

In some applications we need to have a deterministic interleaver to reduce the hardware requirements for the Turbo encoder and decoder. The following theorem describes a technique to design a deterministic interleaver based on step 1.

Theorem 1: Let $\alpha \in \mathbf{N}$ be a natural number such that $gcd(\alpha, N) = 1$ and $\alpha - 1$ divides N. Then there is a permutation $\pi \in S_N$ satisfying (i) and (ii) with $S_1 := min(\alpha, \frac{N}{\alpha+1})$ and $S_2 := \lfloor \frac{\alpha-1}{2} \rfloor$. Let $\beta := \lfloor \frac{\alpha-1}{2} \rfloor$ and define $\pi : \{1, \ldots, N\} \to \{1, \ldots, N\}$ by $\pi(i) := \alpha \cdot i + \beta$, where $\pi(i)$ has to be interpreted as the number $\pi(i) \in \{1, \ldots, N\}$ that is congruent to $\alpha \cdot i + \beta$ modulo N.

References

[1] C. Berrou, A. Glavieux, and P. Thitimajshima, *"Near Shannon Limit Error-Correcting Coding and Decoding: Turbo Codes,"* Proceeding of IEEE ICC 93, pp. 1064-1070.

[2] S Dolinar and D. Divsalar, *"Weight Distribution for Turbo codes Using Random and Nonrandom Permutations,"* JPL Progress report 42-122, pp. 56-65, August 15, 1995.

[3] J. Hokfelt, O. Edfors, and T. Maseng, *"Turbo Codes: Correlated Extrinsic Information and its Impact on Iterative Decoding Performance,"* Proceeding of IEEE VTC '99, Houston, Texas.

[4] H.R. Sadjadpour, M. Salehi, N.J. Sloane, and G. Nebe, *Interleaver design for short block length Turbo codes,"* submitted of ICC2000, New Orleans, LA.

[5] S. Benedetto and G. Montorsi, *"Design of Parallel Concatenated Convlolutional Codes, "* IEEE Trans. on Comm., vol. 44, no. 5, pp. 591-600, May 1996.

[6] A.K. Khandani, *"Optimization of the interleaver structure for Turbo codes,"* Proceeding of the 1999 Canadian workshop on Information theory, pp. 25-28, June 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Source Code with Cost as A Nonuniform Random Number Generator

Te Sun Han and Osamu Uchida[1]
Graduate School of Information Systems
University of Electro-Communications
Chofugaoka 1-5-1, Chofu, Tokyo, 182-8585 Japan
e-mail: han@is.uec.ac.jp, o-uchida@hn.is.uec.ac.jp

Abstract — **We show that an optimal source code with cost function for code symbols can be regarded as a random number generator generating a random sequence (not necessarily a sequence of *fair coin* bits) as the target distribution in the sense that the normalized conditional divergence between the distribution of the generated codeword distribution and the target distribution vanishes as the block length tends to infinity.**

I. Introduction

In 1998, Visweswariah *et al.* [1] and Han [2] have independently shown that an optimal variable-length source code can be regarded as a variable-length random number generator in the sense that the normalized divergence distance between the distribution of the generated codeword process and the *uniform* distribution vanishes as the block length tends to infinity.

On the other hand, as is well known, if we impose *unequal costs* on code symbols, it is no longer optimal to use the code which minimizes the average codeword length. Karp [3] has given an algorithm for constructing minimum-redundancy prefix codes with unequal cost symbols. Naturally, there would exist a bias in the frequency of code symbols generated by an optimal source code with cost. Can we then consider the optimal variable-length source code with cost as a variable-length *nonuniform* random number generator? The purpose of this study is to demonstrate that the answer to this question is "yes".

II. Variable-length Source Coding with Cost

Let $\mathcal{X}$ be a *countably infinite* source alphabet and $\mathcal{Y}$ be a *finite* code alphabet, respectively. In the sequel all the logarithms are taken to the base $K \equiv |\mathcal{Y}|$, where $|\mathcal{Y}|$ denotes the cardinality of $\mathcal{Y}$. We denote the set of all non-null finite length sequences taken from $\mathcal{Y}$ by $\mathcal{Y}^*$. Let us now define a *general source* as an infinite sequence $\mathbf{X} = \{X^n = (X_1^{(n)}, \cdots X_n^{(n)})\}_{n=1}^{\infty}$ of n-dimensional random variables X^n where each component random variable $X_i^{(n)}$ $(1 \le i \le n)$ takes values in $\mathcal{X}$. The class of sources thus defined covers a very wide range of source including all nonstationary and/or nonergodic sources.

Next, we define the *cost function* $c : \mathcal{Y}^* \to \mathbf{R}^+ \equiv (0, +\infty]$ as follows: First, each symbol $y \in \mathcal{Y}$ is assigned the corresponding cost $c(y)$ such that $0 < c(y) \le +\infty$ $(\forall y \in \mathcal{Y})$, and then the *additive* cost $c(\mathbf{y})$ of $\mathbf{y} = (y_1, y_2, \cdots, y_k) \in \mathcal{Y}^k$ is defined by $c(\mathbf{y}) \equiv \sum_{i=1}^{k} c(y_i)$.

Definition 1 : R is called an *achievable variable-length source coding cost-rate* for the source $\mathbf{X}$ if there exists a variable-length prefix encoder $\varphi_n : \mathcal{X}^n \to \mathcal{Y}^*$ given the cost function $c : \mathcal{Y}^* \to \mathbf{R}^+$ such that $\limsup_{n\to\infty} \frac{1}{n} E\{c(\varphi_n(X^n))\} \le R$, and the infimum of R that are achievable variable-length source coding cost-rates is denoted by $R_v^c(\mathbf{X})$, which we call the *infimum achievable variable-length source coding cost-rate*.

Theorem 1 : For any general source $\mathbf{X}$, we have

$$R_v^c(\mathbf{X}) = \frac{1}{\alpha_c} \limsup_{n\to\infty} \frac{1}{n} H(X^n),$$

where the *cost capacity* α_c is the positive unique root α of the equation $\sum_{y\in\mathcal{Y}} K^{-\alpha c(y)} = 1$ and $H(X^n) \equiv -\sum_{\mathbf{x}\in\mathcal{X}^n} P_{X^n}(\mathbf{x}) \log P_{X^n}(\mathbf{x})$.

III. Source Code with Cost as A Nonuniform Random Number Generator

Given a variable-length prefix encoder $\varphi_n : \mathcal{X}^n \to \mathcal{Y}^*$, we define $\mathcal{D}_m \equiv \{\mathbf{x} \in \mathcal{X}^n \mid l(\varphi_n(\mathbf{x})) = m\}$ for any positive integer m, where $l(\cdot)$ denotes the length of a string, and we put $\mathcal{J}(\varphi_n) \equiv \{m | \Pr\{X^n \in \mathcal{D}_m\} > 0\}$. For any $m \in \mathcal{J}(\varphi_n)$, we define X_m^n as the random variable taking values in $\mathcal{D}_m$ with the distribution given by $P_{X_m^n}(\mathbf{x}) \equiv \frac{P_{X^n}(\mathbf{x})}{\Pr\{X^n \in \mathcal{D}_m\}}$ $(\mathbf{x} \in \mathcal{D}_m)$. For any positive integer m, $V^{(m)}$ indicates an i.i.d. sequence of length m. Let us now define the conditional divergence by

$$D(\varphi_n(X^n)||V^{(I_n)}|I_n) \equiv \sum_{m\in\mathcal{J}(\varphi_n)} \Pr\{I_n = m\} D(\varphi_n(X_m^n)||V^{(m)})$$

where I_n is the random variable such that $I_n = m$ for $X^n \in \mathcal{D}_m$.

Then, we have the following main theorem.

Theorem 2 : We assume that the entropy rate of the general source $\mathbf{X}$ has the limit $\lim_{n\to\infty} \frac{1}{n} H(X^n)$. Let $\varphi_n : \mathcal{X}^n \to \mathcal{Y}^*$ be any *optimal* variable-length prefix encoder in the sense that

$$\lim_{n\to\infty} \frac{1}{n} E\{c(\varphi_n(X^n))\} = R_v^c(\mathbf{X}).$$

If we define the probability distribution $\mathbf{q}_c = \{q_c(y)\}_{y\in\mathcal{Y}}$ corresponding to the cost function c by $q_c(y) = K^{-\alpha_c c(y)}$ $(y \in \mathcal{Y})$, then we have

$$\lim_{n\to\infty} \frac{1}{n} D(\varphi_n(X^n)||V^{(I_n)}|I_n) = 0,$$

where $V^{(m)}$ stands for the i.i.d. sequence of length m subject to the distribution $\mathbf{q}_c$.

References

[1] K. Visweswariah, S. R. Kulkarni and S. Verdu, "Source codes as random number generators," *IEEE Trans. Inform. Theory*, vol. 44, pp.462-471, Mar. 1998.

[2] T. S. Han, *Information-Spectrum Methods in Information Theory*, Baifukan-Press, Tokyo, 1998 (In Japanese).

[3] R. M. Karp, "Minimum redundancy coding for the discrete noiseless channel," *IRE Trans. Inform. Theory*, vol. IT-7, pp.27–38, Jan. 1961.

[1] O. Uchida is now with the Dept. of Network Engineering, Kanagawa Institute of Technology, Atsugi, Kanagawa, 243-0292 Japan.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Random Number Approximation Problem for Discrete Memoryless Sources

Yasutada Oohama
Graduate School of Information Science
and Electrical Engineering, Kyushu University
6-10-1 Hakozaki, Higashi-ku, Fukuoka 812, Japan
e-mail: oohama@csce.kyushu-u.ac.jp

Abstract **We consider the simulation problem of generating random sequences from an arbitrary prescribed discrete memoryless source (DMS) by using a random sequence from a given DMS. We propose two simple algorithms and give some explicit results for their asymptotic performances.**

I. Introduction

Simulation problems of generating random sequences from a prescribed information source by using a random sequence from a given information source is called random number problem. Recently, simple and efficient algorithms for random number problem and the analysis of their performances were studied by Han and Hoshi [1], Uyematsu and Kanaya [2] and Oohama [3]. We deal with the simulation of generating random sequences of fixed length from an arbitrary prescribed discrete memoryless source (DMS) by using a random sequence of fixed length from a given DMS. We propose two simple algorithms and derive explicit results for their asymptotic performances. Our results contain some of the results of Uyematsu and Kanaya [2] and Oohama [3] as special cases.

II. Random Number Approximation Problem

Let X and Y be random variables taking values in finite sets $\mathcal{X}$ and $\mathcal{Y}$, respectively. The distributions of X and Y are denoted by $P_X = \{P_X(x)\}_{x\in\mathcal{X}}$ and $P_Y = \{P_Y(y)\}_{y\in\mathcal{Y}}$ respectively. Let $\mathcal{P}(\mathcal{X})$ and $\mathcal{P}(\mathcal{Y})$ denote the set of all probability distributions on $\mathcal{X}$ and $\mathcal{Y}$, respectively. Consider two stationary discrete memoryless sources $\{X_t\}_{t=1}^{\infty}$ and $\{Y_t\}_{t=1}^{\infty}$. For each $t = 1, 2, \cdots$, X_t and Y_t obeys the same distribution as those of X and Y, respectively. We write random sequences of lengths n and m from information sources as $X^n = X_1X_2\cdots X_n$ and $Y^m = Y_1Y_2\cdots Y_m$, respectively.

The Fixed to Fixed random number approximation problem discussed here is as follows. Let $\varphi_n : \mathcal{Y}^m \to \mathcal{X}^n$. Let $\Phi(r)$ denote the set of all the map φ_n that satisfies the rate constraint $m \le nr$. By the map φ_n, the random sequence Y^m is transformed into the sequence $\varphi_n(Y^m)$, which is used as an approximation of the random sequence X^n. We consider the approximation error measured by the variational distance between the distributions of $\varphi_n(Y^m)$ and X^n denoted by $d(\varphi_n(Y^m), X^n)$.

Next, we explain our proposed algorithms for approximation. Let i_X be an one-to-one map from $\mathcal{X}^n$ to $\{1, 2, \cdots, |\mathcal{X}|^n\}$, where $|A|$ denotes the cardinality of the set A. Let $P_X^n(x^n)$, $x^n \in \mathcal{X}^n$ denote the probability of x^n and $I_X(x^n)$ be a subinterval of $[0, 1)$ given by $I_X(x^n) = [L_X(x^n), L_X(x^n)+P_X(x^n))$, where $L_X(x^n) = \sum_{a^n:i(a^n)<i(x^n)} P_X^n(a^n)$. Definitions and notations for Y are the same as those for X. In the proposed algorithms the map φ_n has the following form. For $y^m \in \mathcal{Y}^m$ define $\varphi_n(y^m) = x^n$ if $L_Y(y^m) \in I_X(x^n)$. In the arithmetic algorithm the map i_X is determined according to some lexicographical order of sequences in $\mathcal{X}^n$. In the sorting algorithm the map i_X is determined according to the descending order of values of probabilities of sequences in $\mathcal{X}^n$. The definition of i_Y for Y is the same as that for X.

To state our results for the performances of the above two algorithms, set

$$F_\lambda(R, P_X) = \min_{P\in\mathcal{P}(\mathcal{X})} \{[\lambda(R - H(P) - D(P\|P_X))]^+ + D(P\|P_X)\}$$

$$F_+(R, P_X) = \lim_{\lambda\to+\infty} F_\lambda(R, P_X),$$

$$F_-(R, P_X) = \lim_{\lambda\to-\infty} F_\lambda(R, P_X).$$

where $[t]^+ = \max\{0, t\}$. Let $R_-(P_X) = \min_{x\in\mathcal{X}}(-\log P_X(x))$, $R_+(P_X) = \max_{x\in\mathcal{X}}(-\log P_X(x))$ and set

$$\mathcal{R}_s = \left\{(R, \tilde{R}) : \begin{array}{l} R \ge rR_-(P_Y), \\ rF_-(\frac{R}{r}, P_Y) \le \tilde{R} \le R_+(P_X) \end{array}\right\}.$$

Define two functions by

$$E_a(r, P_X, P_Y) = \min_{R\ge rR_-(P_Y)} \max\left\{F_1(R, P_X), rF_-\left(\frac{R}{r}, P_Y\right)\right\}$$

$$E_s(r, P_X, P_Y) = \min_{(R,\tilde{R})\in\mathcal{R}_s} \left\{[R - \tilde{R}]^+ + \max\left\{F_+(\tilde{R}, P_X), rF_-\left(\frac{R}{r}, P_Y\right)\right\}\right\}.$$

Our main results are as follows.

Theorem 1 For any $r > 0$ and the sequence of maps $\{\varphi_n : \varphi_n \in \Phi_n(r)\}_{n=1}^{\infty}$ defined by the arithmetic algorithm

$$\lim_{n\to\infty}\left(-\frac{1}{n}\right)\log d(\varphi_n(Y^m), X^n) \ge E_a(r, P_X, P_Y). \quad (1)$$

Theorem 2 For any $r > 0$ and the sequence of maps $\{\varphi_n : \varphi_n \in \Phi_n(r)\}_{n=1}^{\infty}$ defined by the sorting algorithm

$$\lim_{n\to\infty}\left(-\frac{1}{n}\right)\log d(\varphi_n(Y^m), X^n) \ge E_s(r, P_X, P_Y). \quad (2)$$

References

[1] T. S. Han and M. Hoshi, "Interval algorithm for random number generation," *IEEE Trans. Inform. Theory*, vol. 43, pp. 599-611, March 1997.

[2] T. Uyematsu and F. Kanaya, "Channel simulation by interval algorithm: A performance analysis for interval algorithm," *IEEE Trans. Inform. Theory*, vol. 45, pp. 2121-2129, Sept. 1999.

[3] Y. Oohama, "Arithmetic and sorting algorithms for fixed to fixed random number generation and their performance analysis," preprint.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On Rate of Source Conversion by Concatenating Code/Parse Trees

Hiroyoshi Morita, Kingo Kobayashi, and Mamoru Hoshi
University of Electro-Communications,
Chofu, Tokyo 182-8585, Japan
e-mail: {morita,kingo,hoshi}@is.uec.ac.jp

Abstract — **Source conversion by means of two binary prefix codes is considered. A source sequence is encoded into a stream of codewords by the first code. Then, the stream is parsed into codewords of the second, which consequently produces another source sequence. The conversion rate is investigated in the context of the combined source-(d,k) coding.**

I. Introduction

In the combined source-(d,k) coding scheme as introduced by Kerpez [1], an arithmetic code performs source coding and (d,k)-constrained channel coding simultaneously. While its mechanism looks very similar to the interval algorithm for generating random numbers proposed by Han and Hoshi [2], Kerpez's code essentially consists of an arithmetic encoder for an information source and an arithmetic decoder for the maxentropic source associated with the (d,k) constraints [3]. Using these two codes, Kerpez's code converts a given source to another, say to the maxentropic source.

To study on source conversion more generally, we investigate the coding performance of the combination of two binary prefix codes ϕ_1 and ϕ_2: the first code ϕ_1 maps an information source sequence $\boldsymbol{X} = X_1X_2\cdots$ over $\mathcal{X} = \{\alpha_1,\ldots,\alpha_D\}$ into the intermediate binary process $\boldsymbol{Y} = \phi_1(X_1)\phi_1(X_2)\cdots$ over $\mathcal{Y} = \{0,1\}$ while the second parses $\boldsymbol{Y}$ into $\boldsymbol{Y} = \phi_2(Z_1)\phi_2(Z_2)\cdots$, and outputs $\boldsymbol{Z} = Z_1Z_2\ldots$ over $\mathcal{Z} = \{\gamma_1,\ldots,\gamma_R\}$.

The conversion rate ρ is the ratio of the length of $\boldsymbol{Z}$ to that of $\boldsymbol{X}$. More precisely, we define

$$\rho(\boldsymbol{X},\phi_1,\phi_2) \triangleq \limsup_{\ell\to\infty} N(\phi_1(X^\ell),\phi_2)/\ell$$

where $\phi_1(X^\ell) = \phi_1(X_1)\cdots\phi_1(X_\ell)$ and $N(\boldsymbol{y}^k,\phi_2)$ is the number of codewords completely parsed by ϕ_2 for $\boldsymbol{y}^k \in \mathcal{Y}^k$.

In this article, we obtain a formula on conversion rate for an independent and identically distributed (*i.i.d.*) source $\boldsymbol{X}$ and apply it to the problem of the combined source and (d,k)-constrained channel coding.

II. A Formula on Conversion Rates

Fixed $\boldsymbol{Y} = \boldsymbol{y} \in \mathcal{Y}^\infty$, we expect that for a sufficiently long subsequence $\boldsymbol{y}^m$ ($m >> 1$), the ratio $N(\boldsymbol{y}^m,\phi_2)/N(\boldsymbol{y}^m,\phi_1)$ is close to the conversion rate. In fact, if $\boldsymbol{X}$ is *i.i.d.*, then $\{N(\boldsymbol{Y}^m,\phi_1),\ m \geq 0\}$ with $N(\boldsymbol{Y}^0,\phi_1) = 0$ is a renewal process [4] with mean $E|\phi_1(X)|$, i.e., the average codeword length of ϕ_1 for $\boldsymbol{X}$. Hence, the strong law for renewal processes says $\lim_{m\to\infty} N(\boldsymbol{Y}^m,\phi_1)/m \overset{a.s.}{=} 1/E|\phi_1(X)|$ where $\overset{a.s.}{=}$ means the convergence with probability one. However, $\{N(\boldsymbol{Y}^m,\phi_2),\ m \geq 0\}$ is not a renewal process since the process $\{\phi_2(Z_1),\phi_2(Z_2),\ldots\}$ is not always *i.i.d.* except the case the probability of X is D-adic, that is, each of $p_k \triangleq \Pr\{X_i{=}\alpha_k\}$ equals $D^{-\ell}$ for some ℓ.

To overcome this difficulty, we get the insight into a Markov chain which exists behind $\boldsymbol{Y}$. Here, for $i = 1,2$, let T_i be a binary tree whose paths from the root to external nodes uniquely correspond to codewords of ϕ_i by labelling 0 and 1 to the left and right branches of internal nodes, respectively. The set of states of the chain consists of internal nodes of T_1. And the state transition probability P can be recursively given by initially assigning probabilities p_k ($k = 1,\ldots,D$) to the corresponding external nodes. Then, $\boldsymbol{Y}$ is given as the output process of the chain which emits the label 0 or 1 according to a branch passed through in every transition.

Now, construct a joint Markov process with the state set consisting of pairs of internal nodes of T_1 and T_2. Its transition probability is automatically deduced from P. Then, $\boldsymbol{Y}$ can be thought as the output process of the joint Markov chain as well. Having considered its stationary probability, we showed that $\lim_{m\to\infty} N(\boldsymbol{Y}^m,T_2)/m \overset{a.s.}{=} 1/E|\phi_2(Z)|$ where Z is a random variable with the stationary probability of $\boldsymbol{Z}$.

Theorem 1 Given an *i.i.d.* source $\boldsymbol{X}$, and prefix codes ϕ_1 and ϕ_2,

$$\rho(\boldsymbol{X},\phi_1,\phi_2) \overset{a.s.}{=} E|\phi_1(X)|/E|\phi_2(Z)|.$$

III. Rate of Combined Source-(d,k) Coding

Let $\mathcal{C}_{d,k}$ be the set of binary strings $0\cdots01$ consisting of i consecutive zeros followed by a symbol 1 for $i = d, d{+}1,\ldots,k$. Let $f_{(d,k)}$, or simply f, be a one-to-one mapping from $\mathcal{Z}$ to $\mathcal{C}_{d,k}$ where $|\mathcal{Z}| = k - d + 1$. After converting the source sequence $\boldsymbol{X}$ to $\boldsymbol{Z}$ through ϕ_1 and ϕ_2, we apply f to each symbol in $\boldsymbol{Z}$. Then we obtain a (d,k)-constrained sequence $f(\boldsymbol{Z}) \triangleq f(Z_1)f(Z_2)\cdots$. Let us define the conversion rate $\tilde{\rho}(\boldsymbol{X},\phi_1,\phi_2,f)$ of the combined coding by

$$\tilde{\rho}(\boldsymbol{X},\phi_1,\phi_2,f) \triangleq \limsup_{\ell\to\infty} \frac{1}{\ell}\sum_{\gamma\in\mathcal{Z}} |f(\gamma)|\,\tilde{N}(\phi_1(X^\ell),\phi_2,\gamma)$$

where $\tilde{N}(\boldsymbol{y}^m,\phi_2,\gamma)$ is the frequency of $\phi_2(\gamma)$ parsed from $\boldsymbol{y}^m$.

Theorem 2 $\tilde{\rho}(\boldsymbol{X},\phi_1,\phi_2,f) \overset{a.s.}{=} \rho(\boldsymbol{X},\phi_1,\phi_2)\,E|f(Z)|$.

Finally, we obtain the following theorem.

Theorem 3 There exists a series of pairs of $\phi_1^{(t)}\colon \mathcal{X}^t \to \mathcal{Y}^*$ and $\phi_2^{(t)}\colon \mathcal{Z}^t \to \mathcal{Y}^*$ such that

$$\lim_{t\to\infty} \tilde{\rho}(\boldsymbol{X},\phi_1^{(t)},\phi_2^{(t)},f_{(d,k)}) \overset{a.s.}{=} \frac{H(X)}{\log\lambda}$$

where $\mathcal{Y}^*$ is the set of all finite sequences over $\mathcal{Y}$, $H(X)$ is the entropy rate of $\boldsymbol{X}$, and λ is the largest positive root of $\sum_{i=d+1}^{k+1} x^{-i} = 1$.

References

[1] K.J. Kerpez, "Runlength codes from sources codes," *IEEE Trans. Inform. Theory*, vol.37, pp.682–687, 1991.

[2] T.S. Han and M. Hoshi, "Interval Algorithm for Random Number Generation," *IEEE Trans. Inform. Theory*, vol.43, pp.599–611, 1997.

[3] K.A.S. Immink, *Coding Techniques for Digital Recorders*, Prentice Hall, 1991.

[4] R. Gallager, *Discrete Stochastic Processes*, Kluwer Academic Pub., Boston, 1995.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Almost Sure Convergence Theorems of Rate of Coin Tosses for Random Number Generation by Interval Algorithm

Tomohiko UYEMATSU
Dept. of Computer Science
Tokyo Institute of Technology
Ookayama, Meguro-ku, Tokyo 152-8552, Japan
e-mail: uematsu@ss.titech.ac.jp

Fumio KANAYA
Dept. of Information Science
Shonan Institute of Technology
Fujisawa-shi, Kanagawa 251-0046, Japan
e-mail: fkanaya@info.shonan-it.ac.jp

Abstract — **This paper deals with the interval algorithm proposed by Han and Hoshi for random number generation, and evaluates the efficiency of the algorithm for each sample path instead of evaluating overall expectation. We show a theorem in the almost-sure sense to give bounds on the sup generating rate as well as on the inf generating rate for each sample of input and output processes.**

I. Introduction

This paper deals with the most general random number generation problem by interval algorithm [1] where the process of repeated coin tosses and that of repeated random number generations are general processes subject to neither stationarity nor ergodicity but consistency restrictions. We are concerned with the case in which the target process should be generated exactly subject to the prescribed probability measure, and concentrate on the almost sure asymptotic property of the generating rate of each sample, i.e. the number of coin tosses per output sample of the general process. To this end, we introduce the minimum length function to indicates the length of the shortest prefix of sample $x \in \mathcal{A}^\infty$ from the general source with which the interval algorithm generates the n-length prefix of some sample $y \in \mathcal{A}^\infty$ subject to the target probability measure. Then we define *sup generating rate* and *inf generating rate* of each input sample. As a result, we prove a theorem in the almost-sure sense to give bounds on the sup generating rate as well as on the inf generating rate for each sample of input and output processes.

II. Basic Definitions

(a) General sources

Let $\mathcal{A}$ be a finite set and $(\mathcal{A}^\infty, \mathcal{F})$ a measurable space, where $\mathcal{A}^\infty$ is the set of all strings of infinite length that is formed from the symbols in $\mathcal{A}$, and $\mathcal{F}$ is a σ-field of subsets of $\mathcal{A}^\infty$. Let μ be a probability measure defined on $(\mathcal{A}^\infty, \mathcal{F})$. Then we call $(\mathcal{A}^\infty, \mathcal{F}, \mu)$ a probability space. We call μ a general process [2]. Throughout this article, we assume for μ neither stationarity nor ergodicity but consistency restrictions.

An extension of the interval algorithm for general sources was indicated in [1, Remark 12]. So, we omit the description of the algorithm.

(b) Inf generating rate and sup generating rate

The minimum length function $L_I^n : \mathcal{A}^\infty \to \mathbf{N}$ is defined as the length of the shortest prefix of sample $x \in \mathcal{A}^\infty$ from the general source ν with which the interval algorithm generates the n-length prefix of some sample $y \in \mathcal{A}^\infty$ subject to the target probability μ. Here it should be understood that $L_I^n(x)$ is defined as $+\infty$ if the above set is empty. We call $L_I^n(x)$ the minimum length of x. Further, we define the *sup generating rate* for any source sample x as

$$\bar{l}_I(x) = \limsup_{n\to\infty} \frac{1}{n} L_I^n(x) \quad \forall x \in \mathcal{A}^\infty.$$

Similarly, the *inf generating rate* is defined as

$$\underline{l}_I(x) = \liminf_{n\to\infty} \frac{1}{n} L_I^n(x) \quad \forall x \in \mathcal{A}^\infty.$$

III. Main results

We require the following hypotheses to prove the theorem as well as the consistency restrictions for μ and ν :

H1: There exists a positive number α such that

$$\liminf_{n\to\infty} \frac{1}{n} \log \frac{1}{\nu(x^n)} \geq \alpha \quad \nu\text{-a.s.}$$

H2: There exists a positive number β such that

$$\liminf_{n\to\infty} \frac{1}{n} \log \frac{1}{\mu(x^n)} \geq \beta \quad \mu\text{-a.s.}$$

Suppose that for the input sample $x \in \mathcal{A}^\infty$, the output sample $y \in \mathcal{A}^\infty$ is generated by the interval algorithm. Then, the following theorem holds.

Theorem :

$$\frac{\underline{h}_\mu(y)}{\overline{h}_\nu(x)} \leq \underline{l}_I(x) \leq \frac{\overline{h}_\mu(y)}{\overline{h}_\nu(x)} \quad \text{a.s.}$$

$$\frac{\underline{h}_\mu(y)}{\underline{h}_\nu(x)} \leq \bar{l}_I(x) \leq \frac{\overline{h}_\mu(y)}{\underline{h}_\nu(x)} \quad \text{a.s.}$$

where $\underline{h}_\nu(x)$ and $\overline{h}_\nu(x)$ (resp. $\underline{h}_\mu(y)$ and $\overline{h}_\mu(y)$) are *inf ν-complexity rate* and *sup ν-complexity rate* (resp. inf and sup μ-complexity rates) defined in [2]. Especially, if both processes ν and μ are stationary ergodic, then

$$\underline{l}_I(x) = \bar{l}_I(x) = \frac{h_\mu}{h_\nu} \quad \text{a.s.}$$

where h_ν (resp. h_μ) denotes the entropy rate of the process ν (resp. μ).

It should be noted this theorem is an extension of the results in [3] where we only deal with i.i.d. processes.

References

[1] T. S. Han and M. Hoshi, "Interval algorithm for random number generation," *IEEE Trans. Inform. Theory*, vol. 43, pp. 599-611, 1997.

[2] J. Muramatsu and F. Kanaya, "Almost-sure variable-length source coding theorems for general sources," *IEEE Trans. Inform. Theory*, vol. 45, pp. 337-342, 1999.

[3] T. Uyematsu and F. Kanaya, "Channel simulation by interval algorithm: A performance analysis of interval algorithm," *IEEE Trans. Inform. Theory*, vol. 45, no.6, pp.2121-2129, 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

A new upper bound on the reliability function of the Gaussian channel

A. Ashikhmin
Bell Labs, Lucent Technologies
600 Mountain Ave, Murray Hill, NJ 07974
aea@research.bell-labs.com

A. Barg
Bell Labs, Lucent Technologies
600 Mountain Ave, Murray Hill, NJ 07974
abarg@research.bell-labs.com

S. Litsyn
Department of EE-Systems
Tel Aviv University
Ramat Aviv 69978, Israel
litsyn@eng.tau.ac.il

Abstract — **Upper bounds on the reliability function of the Gaussian channel were derived by Shannon in 1959 [1]. Kabatiansky and Levenshtein [2] obtained a low-rate improvement of Shannon's "minimum-distance bound". Together with the straight-line bound this provided an improvement upon the sphere-packing bound in a certain range of code rate.**

In this work we prove a bound better than the KL bound on the reliability function. Employing the straight-line bound, we obtain a further improvement of Shannon's results. As intermediate results we prove lower bounds on the distance distribution of spherical codes and a tight bound on the exponent of Jacobi polynomials of growing degree in the entire orthogonality segment.

Let S^{n-1} be a sphere of radius $\sigma\sqrt{An}$ in $\mathbf{R}^n$, where A is the signal-to-noise ratio in the channel and σ^2 is the variance of the Gaussian noise along each coordinate. A code W is a finite subset of S^{n-1}. The number $R = (1/n)\ln|W|$ is called the rate of W. Let $d(W) := \min_{\mathbf{x},\mathbf{y}\in W,\ \mathbf{x}\neq\mathbf{y}} \mathrm{dist}\,(\mathbf{x},\mathbf{y})(0 \leqslant d(W) \leqslant 2\sigma\sqrt{An})$, be the minimum distance of W. Suppose that W is used for transmission over the Gaussian channel. Let $P_e(W) = \frac{1}{|W|}\sum_{\mathbf{x}\in W} P_e(\mathbf{x})$ be the error probability of W under maximum likelihood decoding. Let

$$P_e(R,A,n) = \min_{W:R(W)\geqslant R} P_e(W)$$

$$E(R,A,n) = -\frac{1}{n}\log P_e(R,A,n).$$

Shannon [1] introduced the function $E(R,A) = \lim_{n\to\infty} E(R,A,n)$ and called it the *reliability function* of the channel. Computing this function forms a central problem of information theory. In the same paper Shannon proved the sphere-packing upper bound on $E(R,A)$ in the form

$$E(\theta,A) \leqslant \frac{A}{2} - \frac{\sqrt{A}g(\theta,A)\cos\theta}{2} - \ln(g(\theta,A)\sin\theta), \tag{1}$$

(here $g(\theta,A) = \frac{1}{2}(\sqrt{A}\cos\theta + \sqrt{A\cos^2\theta + 4})$, $\theta = \arcsin(e^{-R})$), and the minimum-distance bound

$$E(R,A) \leqslant E_{md}(R,A) = (A/8)d^2(R),$$

where $d(R)$ is any upper bound on the distance of a code of rate R. Kabatyansky and Levenshtein [2] proved a new upper bound on the distance of spherical codes in the form $d(R) \leqslant \delta(\rho(R))$, where $\delta(x) = \sqrt{2}(\sqrt{1+x} - \sqrt{x})/\sqrt{1+2x}$, $\rho(R)$ is the root of the equation $R = (1+\rho)H(\frac{\rho}{1+\rho})$, and H is the natural entropy function. Using this bound in $E_{md}(R,A)$ together with the straight-line bound, they improved [2] upon Shannon's results in a certain range of code rates.

The main result of the present paper is the following theorem.

Theorem 1 *The reliability function of the Gaussian channel with signal-to-noise ratio A satisfies the upper bound*

$$E(R,A) \leqslant \min_{0\leqslant\rho\leqslant\rho(R)} \max_{w,d} \Big[\min(A\frac{d^2}{8}, A\frac{w^2}{8} - \mathcal{A}(w))\Big], \tag{2}$$

where R is a value of the code rate,

$$0 \leqslant d \leqslant \delta(\rho(R)), \quad d \leqslant w \leqslant \delta(\rho),$$

$$\mathcal{A}(w) = \min\Big\{\frac{Ad^2w^2}{8(4w^2-d^2)}, F\big(1-\frac{1}{2}w^2,\rho\big)\Big\},$$

and

$$F(x,\rho) = R - (1+\rho)H\Big(\frac{\rho}{1+\rho}\Big) + \ln\Big(\frac{1}{2}\big(x + \sqrt{(1+2\rho)^2x^2 - 4\rho(1-\rho)}\big)\Big) + (1+2\rho)\ln\frac{(1+2\rho)x + \sqrt{(1+2\rho)^2x^2 - 4\rho(1-\rho)}}{2(1+\rho)}$$

Bound (2) is better than the minimum-distance bound on $E(R,A)$ of [2]. Together with the straight-line bound related to it, (2) also improves upon the sphere-packing exponent (1) in a larger range of code rates than the results in [2].

The proof consists of the following 4 steps:

–a general theorem on the distance distribution of spherical codes. This theorem carries over to the spherical case the techniques developed recently in [3], [4],

–asymptotic bounds on the exponent of Jacobi polynomials P_k (this is an extension of a result in [2] on the asymptotics of the extremal zero of P_k),

–asymptotic bounds on the distance distribution of spherical codes, and

–bounding below the error probability of decoding for a code with a known distance distribution.

References

[1] C. E. Shannon, *Probability of error for optimal codes in Gaussian channel*, Bell Syst. Techn. Journ. **38** (1959), no. 3, 611–656.

[2] G. Kabatyansky and V. I. Levenshtein, *Bounds for packings on the sphere and in the space*, Problemy Peredachi Informatsii **14** (1978), no. 1, 3–25.

[3] A. Ashikhmin and A. Barg, "Binomial moments of the distance distribution: Bounds and applications," *IEEE Trans. Inform. Theory*, **45**, 1999, pp. 438–452.

[4] S. Litsyn, "New upper bounds on error exponents," *IEEE Trans. Inform. Theory*, **45**, 1999, pp. 385–398.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

AWGN Coding Theorems from Ensemble Weight Enumerators

D. Divsalar and S. Dolinar[1]
Jet Propulsion Laboratory
California Institute of Technology
Pasadena CA 91109 USA
dariush@shannon.jpl.nasa.gov
sam@shannon.jpl.nasa.gov

H. Jin and R. McEliece[2]
Department of EE
California Institue of Technology
Pasadena, CA 91125 USA
hui@systems.caltech.edu
rjm@systems.caltech.edu

Abstract — **In this paper we develop AWGN coding theorems for ensembles of codes for which we can calculate, or at least closely estimate, the ensemble weight enumerator. As a rule, for such an ensemble we can find a threhold c such that if $E_b/N_0 > c$, then the ensemble maximum-likelihood error probability appraoches zero. This threshold is always better, and usually much better, than can be obtained from the union bound. The role of low-weight codewords is key.**

I. Introduction

Coding theory has been revolutionized by the discovery of that certain random ensembles of codes ("turbo" style codes, LDPC codes, and their relatives) can be effectively decoded with iterative message-passing algorithms. Of course a random ensemble is a candidate for iterative decoding only if it has the potential for good performance, as measured by its maximum-likelihood decoding performance. In this paper we will develop a technique for finding the ML potential for a broad class of random ensembles, on the AWGN channel. A weaker, but more broadly applicable, technique is the subject of a companion paper [2].)

II. Ensemble Weight enumerators

By an *ensemble* of linear codes we mean a sequence $\mathcal{C}_{n_1}, \mathcal{C}_{n_2}, \ldots$ of sets of linear codes of a common rate R, where $\mathcal{C}_{n_i}$ is a set of (n_i, k_i) codes with $k_i/n_i = R$. We assume that the sequence $n_1, n_2, \ldots$ approaches infinity. If C is an (n,k) code in the ensemble, we denote the weight enumerator of C by the list $A_0(C), A_1(C), \ldots, A_n(C)$. The *average weight enumerator* for the set $\mathcal{C}_n$ is defined as the list

$$\overline{A}_0^{(n)}(C), \overline{A}_1^{(n)}(C), \ldots, \overline{A}_n^{(n)}(C),$$

where

$$\overline{A}_h^{(n)} = \frac{1}{|\mathcal{C}_n|} \sum_{C \in \mathcal{C}_n} A_h(C) \qquad \text{for } h = 0, 1, \ldots, n.$$

Also, we define the *ensemble spectral shape* :

$$r(\delta) = \lim_{n \to \infty} \frac{1}{n} \log \overline{A}_{\lfloor \delta n \rfloor}^{(n)} \qquad \text{for } 0 < \delta < 1,$$

assuming that the limit exists. In this case, we may write

$$\overline{A}_h^{(n)} = e^{n(r(\delta) + o(1))},$$

where $\delta = h/n$.

For technical reasons, we need to make the following two assumptions about the behavior of $\overline{A}_h^{(n)}$, for $h = o(n)$. Both assumptions say, roughly, that there are not too many words of low weight in the ensemble.

- *Assumption 1*: There exist a sequence of integers d_n such that $d_n \to \infty$ and

$$\lim_{n \to \infty} \sum_{h=1}^{d_n} \overline{A}_h^{(n)} = 0.$$

- *Assumption 2*:

$$\lim_{\delta \to 0} \frac{r(\delta)}{\delta} \leq 0.$$

It is our goal to prove an AWGN coding theorem for such an ensemble, i.e., a theorem that says that if E_b/N_0 exceeds a certain threshold, then $\overline{P}_E^{(n)} \to 0$ as $n \to \infty$, where $\overline{P}_E^{(n)}$ denotes the ensemble average probability of (word) error for a maximum-likelihood decoder. In the next section, we will give a formula for such a threshold based on a recent result of Divsalar.

III. Definition of the Divsalar Threshold

For an ensemble of the type discussed in Section II, we can define the *Divsalar threshold* as follows:

$$c_D = \sup_{0 < \delta < 1} \frac{1 - \delta}{\delta} \frac{1 - e^{-2r(\delta)}}{2}.$$

The derivation of this threshold is explained in [1]. (The threshold corresponding to the union bound is $c_U = \sup_{0<\delta<1} \frac{r(\delta)}{\delta}$.)

IV. The Main Theorem.

Theorem. *For an ensemble of rate R which satisfies the two assumptions cited in Section II, if $E_b/N_0 > (1/R)c_D$, then*

$$\lim_{n \to \infty} \overline{P}_E^{(n)} = 0.$$

Using the result of this theorem, and the known expressions for $r(\delta)$ for the ensembles of low-density parity-check codes and "repeat-accumlulate" codes [3], we can obtain very good values for the ML thresholds for these codes.

References

[1] D. Divsalar, "A simple tight bound on error probability of block codes with application to turbo codes," TMO Progress Report 42-139 (November 1999). available at http://tmo.jpl.nasa.gov/tmo/progress_report/42-139/139L.pdf.

[2] Hui Jin and Robert J. McEliece, "General Coding Theorems for Turbo-Like Codes," Proc. ISIT 2000.

[3] D. Divsalar, H. Jin, and R. J. McEliece, "Coding theorems for 'turbo-like' codes," in *Proc. 36th Allerton Conf. on Communication, Control and Computing*, pp. 201-210, 1998.

[1]The work of these authors was supported the National Aeronautics and Space Administration.

[2]The work of these authors was supported by NSF grant no. CCR-9804793, and grants form Sony and Qualcomm.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Gaussian ISI Channels and the Generalized Likelihood Ratio Test

Amos Lapidoth
ETF E 107 ETHZ
CH-8092 Zürich
Switzerland
lapidoth@isi.ee.ethz.ch

Emre Telatar
EPFL - DSC - LTHI
CH-1015 Lausanne
Switzerland
Emre.Telatar@epfl.ch

Abstract — **Decoders employing the generalized likelihood ratio test can achieve rates that can be achieved by maximum likelihood decoders on ISI channels even though they are ignorant of the channel characteristics.**

I. Introduction

A variety of communication systems can be modeled accurately by an intersymbol interference (ISI) channel. In many situations, however, the exact nature of the interference may not be known at the time of the system design. In this note, we consider the performance of a particular decoding rule that, in contrast to maximum likelihood (ML), operates with imprecise knowledge of the channel.

The question of the existence of universal decoders for the ISI channel has been previously addressed [1]. It is known that universal decoders do exist for this class of channels. However, the existence proof suggests a very complicated construction, one that requires to consider all ML decoders for all the possible ISI channels, and to form a "merging" of these decoders into a single universal one. As such, the complexity of the evaluation of any particular codeword is very high.

For the case of discrete memoryless channels the situation is simpler. The maximum mutual information decoder first suggested in [2] and widely popularized in [3] employs a relatively simple decoding rule: given a received sequence $\mathbf{y}$, and a candidate codeword $\mathbf{x}$, compute a score $\max_Q Q(\mathbf{y}|\mathbf{x})$, where the maximization is taken over all DMC probability laws. The decoder then chooses the codeword with the highest score. It is known that this decoding rule is universal. Even though the cost of codeword evaluation is more than that of maximum likelihood decoding, it is still much less than that of universal decoders based on merging.

The natural generalization of the above decoding rule leads to the so called "Generalized Likelihood Ratio Test" (GLRT): Let the possible channels be parametrized by θ with P_θ denoting the probability law of the corresponding channel. Given a received sequence $\mathbf{y}$, compute the score of $\mathbf{x}$ as $\max_\theta P_\theta(\mathbf{y}|\mathbf{x})$, and choose the codeword with the highest score.

That universal decoders do exist for the ISI channel does not imply that the GLRT decoder performs well; there are classes of channels for which there exists a universal decoder, but GLRT performs poorly [4]. In this presentation, we will investigate the performance of the GLRT on ISI channels. In particular we will show that as far as achievable rates are concerned, the GLRT decoder performs as well as the maximum likelihood decoder.

II. Results

If the spectral characteristics of an ISI channel are known in advance, the codebook used over this channel will be designed accordingly; in particular, the capacity of the channel can be achieved via water pouring. Since we assume that the ISI coefficients are not known in advance, we will consider the case in which the codewords are chosen to have a flat spectrum. We will content ourselves by considering the rates achievable by GLRT decoders and ML decoders when the codebook is chosen as such. Since the codebook is not spectrally matched to the channel we have no hope of achieving the true capacity of the channel; but we feel that to have assumed that the transmitter is designed with the knowledge of the channel whereas the receiver is not would have been artificial. In all the cases considered below, the transmitter is subject to an average power constraint P.

We will assume that the channel filter $\boldsymbol{\alpha}$ has at most a given duration J, and that the output of the channel at time k is related to the channel input $\mathbf{x}$ via

$$Y_k = (\boldsymbol{\alpha} * \mathbf{x})_k + Z_k, \quad k = 1, \ldots, n,$$

where $*$ denotes cyclic convolution and Z_k are i.i.d, circularly symmetric Gaussian random variables with $E[Z_1] = 0$, $E[|Z_1|^2] = 1$. The use of cyclic convolutions is motivated for reasons of analytical convenience, but can be justified by prepending each codeword by its last J symbols.

In addition to assuming that $\alpha_k = 0$ for $k \geq J$, we will further assume that the filter $\boldsymbol{\alpha}$ satisfies a norm constraint $\sum_j |\alpha_j|^2 \leq H$.

The GLRT decoder then works as follows: given a received $\mathbf{y}$, it assigns to each codeword $\mathbf{x}$ a score $\min_{\mathbf{a}} \|\mathbf{y} - \mathbf{a} * \mathbf{x}\|$ where the minimum is taken over all filters $\mathbf{a}$ of at most J taps that satisfy the energy constraint $\|\mathbf{a}\|^2 \leq H$. The decoder then declares the codeword of smallest score.

We show that for randomly chosen codes (with independently chosen codewords, each codeword chosen either uniformly on the sphere or with i.i.d. Gaussian components), the error probability for the GLRT decoder decays to zero as long as the code rate is less than

$$\int_0^1 \log\bigl(1 + P|\alpha(\theta)|^2\bigr)\, d\theta,$$

where $\alpha(\theta) = \sum_k \alpha_k e^{i2\pi\theta k}$ is the Fourier transform of the channel impulse response. We thus see that for ISI channels, GLRT decoders can achieve all rates the ML decoder can.

References

[1] M. Feder and A. Lapidoth, "Universal Decoding for Channels with Memory," *IEEE Transactions on Information Theory*, v. 44, no. 5, pp. 1726–1745, September, 1998.

[2] V. D. Goppa, "Nonprobabilistic mutual information without memory," *Problems in Controls and Information Theory*, v. 4, pp. 97–102, 1975.

[3] I. Csiszar and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, New York: Academic Press, 1981.

[4] A. Lapidoth and J. Ziv, "On the Universality of LZ-Based Decoding Algorithm," *IEEE Transactions on Information Theory*, v. 44, no. 5, pp. 1746–1755, September, 1998.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Lower Bound to the Feedback Capacity of the Colored Gaussian Noise Channel

Thierry E. Klein[1] Robert G. Gallager
Laboratory for Information and Decision Systems
Massachusetts Institute of Technology
77, Massachusetts Avenue, office 35-303
Cambridge, MA 02139 USA
e-mail: teklein@mit.edu, gallager@lids.mit.edu

Abstract — **In this work, we present a new lower bound on the feedback capacity of the colored Gaussian noise channel. Under the assumption of large power, this lower bound is shown to be strictly larger than the non-feedback capacity. Insight into the role of the feedback and the capacity-achieving strategy have been obtained.**

I. Introduction

In [1], Cover and Pombra have characterized the feedback capacity of the discrete-time, real, colored Gaussian noise channel with noiseless feedback, but their expression still involves an unsolved maximization problem. Since then, most of the work has concentrated on finding upper bounds on the capacity. The only lower bound published in the literature says that the feedback capacity cannot be smaller than the non-feedback capacity. To our knowledge, a specific feedback strategy, applicable for any noise process, that shows that the feedback capacity is strictly larger (when this is actually the case) than the non-feedback capacity has not been published in the literature prior to our work.

II. Problem formulation

The single-user, discrete-time, colored Gaussian noise channel is described by the equation relating the transmitted signal $X[n]$ to the received signal $Y[n]$ at time n:

$$Y[n] = X[n] + Z[n] \tag{1}$$

where $Z[n]$ is the Gaussian noise at time n. We will consider transmission over this channel for N time steps and assume that $Z[1], \cdots, Z[N]$ are jointly Gaussian and zero-mean with covariance matrix K_Z. Without feedback, $X[n]$ is only a function of the message U to be transmitted; however with feedback, $X[n]$ may also depend on past values of the noise process $Z[1], \cdots, Z[n-1]$. The transmitter is power-constrained by $\sum_{n=1}^{N} E\left[X[n]^2\right] \leq N\overline{P}$.

III. Previous work

Let $C_{N,FB}(\overline{P})$ be the capacity in bits per transmission over N time steps if feedback is available and the transmitter is constrained to an average power $\overline{P}$. The expression for the feedback capacity and the form of the capacity-achieving feedback strategy are determined as follows in [1]:

$$C_{N,FB}(\overline{P}) = \max_{tr(K_X) \leq N\overline{P}} \frac{1}{2N} \log\left\{\frac{|K_{X+Z}|}{|K_Z|}\right\} \tag{2}$$

where the maximization is taken over all feedback strategies of the form: $X = U + FZ$ where U is a Gaussian vector and is independent of the noise process Z and F is a strictly lower triangular matrix, since the feedback has to be strictly causal.

IV. New Lower Bound on Feedback Capacity

Determing the feedback capacity reduces to a joint optimization problem over K_U and F, which is not easily solved in closed form. However by fixing a strictly lower triangular matrix F and finding the optimal K_U for that given F, we will determine a lower bound on the feedback capacity, parametrized by F. Under the assumption of large enough power $\overline{P}$, it is obtained that:

$$C_{N,FB}(\overline{P}) \geq \frac{1}{2N} \log\left\{\frac{\left(\overline{P} + \frac{1}{N} tr\left(K_Z\right) + \frac{2}{N} tr\left(F K_Z\right)\right)^N}{|K_Z|}\right\} \tag{3}$$

By chosing a particular feedback matrix F, it is shown that the feedback capacity is strictly larger than the non-feedback capacity:

Theorem 1 *For any noise covariance matrix K_Z of a colored noise noise process, let $F = F_{LLSE}$ be the linear least squares prediction matrix. The difference between the feedback and the non-feedback capacity is then bounded below by:*

$$C_{N,FB}(\overline{P}) - C_N(\overline{P}) \geq \frac{1}{2} \log\left\{1 + \frac{\frac{2}{N} tr\left(F_{LLSE} K_Z\right)}{\overline{P} + \frac{1}{N} tr\left(K_Z\right)}\right\} > 0 \tag{4}$$

In this feedback strategy, the linear least squares prediction of the noise is *added* to the information part of the signal to form the transmitted signal. Note that this prediction is known at the transmitter, but not at the receiver. And it turns out that this strategy gives the receiver added information about the noise. It is surprising that whitening the effective noise process encountered by the information signal is not a beneficial strategy. The new lower bound provided can be further tightened by introducing an amplification factor and by considering $F = \alpha F_{LLSE}$, where $\alpha \geq 1$. The tightest bound achievable through our family of strategies is obtained when increasing α until the assumption of large enough power is violated.

References

[1] T. Cover and S. Pombra, "Gaussian Feedback Capacity", in *IEEE Trans. Inform. Theory*, vol 35, No. 1, January 1989.

[1]This work was conducted under Lincoln Laboratory contract BX-7036.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Traitor Traceable Signature Scheme

Yuji Watanabe[1]
Institute of Industrial Science
University of Tokyo
7-22-1 Roppongi, Minatoku, Tokyo
106-8558, Japan
mue@imailab.iis.u-tokyo.ac.jp

Yuliang Zheng
Monash University
McMahons Road, Frankston,
Melbourne, Victoria 3199,
AUSTRALIA
Yuliang.Zheng@infotech.monash.edu.au

Hideki Imai[1]
Institute of Industrial Science
University of Tokyo
7-22-1 Roppongi, Minatoku, Tokyo
106-8558, Japan
imai@iis.u-tokyo.ac.jp

Abstract — **The new signature scheme, *traitor traceable signature scheme* is presented, which allows the signer to convince any arbiter of the recipient's infringement, if the recipient distributes illegally the signature which he got. We use the techniques of a proof of knowledge of discrete logarithm[1][2], identification of double spender in an off-line electronic cash[3][4], and a signcryption scheme[5]. Our scheme consists of 3-move and it is more compact and efficient compared with the previous scheme[6], due to eliminate the cumbersome cut-and-choose like techniques. Moreover, our accusation protocol does not require the private-key of the recipient of signature, i.e., signer can convince any arbiter of the recipient's infringement without help of original recipient.**

I. Introduction

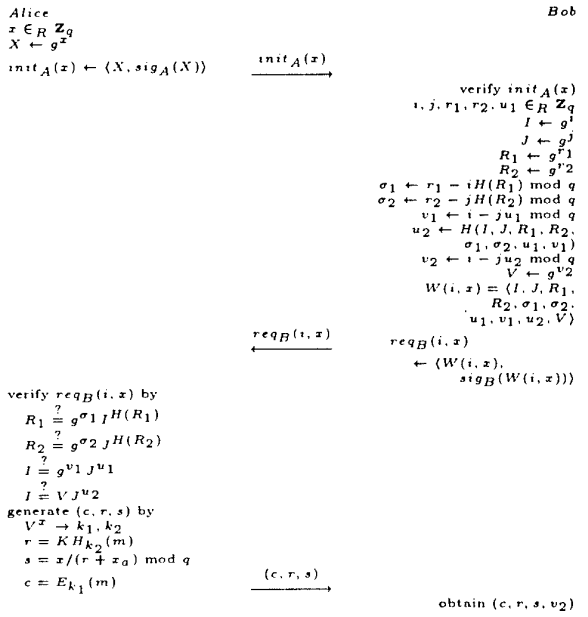
In a conventional digital signature scheme, after issueing the digital document with his signature, the signer cannot convince anyone who has leaked his signed document, since he can reproduce it arbitrarily. Recently, [6] proposed that the technique of tracing traitor[7][8] could be applied to the message with signature in order to prevent illegal proliferation of it. This approach is effective in case that both the message and signature are valuable for anyone.

However, this method[6] is not efficient in communication and computation, due to involve the cumbersome cut-and-choose like technique. Moreover, [6] has the following two problems, 1) an accusation protocol requires the private-key of the recipient of signature. Therefore, if the recipient is not available, the arbiter cannot make decision of accusation, 2) after accusation protocol, the signer can know the complete signature which is known only by recipient before accusation. This means that [6] is not robust against signer making wrong accusations.

II. Traitor traceable signature

In this paper, we propose the new signature scheme, *traitor traceable signature*, which solves several problems of [6] : 1) if the recipient distributes illegally the signature which he got, our scheme allows the signer to convince any arbiter of the recipient's infringement, 2) We use the technique of a proof of knowledge of discrete logarithm, identification of double spender in an off-line electronic cash, and a signcryption scheme, which are well estimated to be (provably) secure, 3) our scheme consists of 3-move and it is more compact and efficient compared with the previous scheme[6], due to eliminate the cumbersome cut-and-choose like techniques, 4)our accusation protocol does not require the private-key of the recipient of signature (the signer can convince any arbiter of the recipient's infringement without help of original recipient), 5)the signature can be generated to the recipient only once per each execution of this protocol in order to prevent the signer from making wrong accusations.

Table 1: Traitor Traceable Signature Scheme



References

[1] A. Fiat and A. Shamir. How to prove yourself: practical solutions to identification and signature problems. In *Proc. of Crypto'86*, pages 186–194, 1986.

[2] C. P. Schnorr. Efficient identification and signatures for smart cards. In *Proc. of Eurocrypt'89*, pages 688–689, 1989.

[3] W. Mao. Blind certification of public keys and efficiently revocable electronic cash: Secure against capable attackers. In *HPL-96-134*, 1996.

[4] S. Brands. Untraceable off-line cash in wallets with observers. In *Proc. of Crypto'93*, pages 302–318, 1993.

[5] Y. Zheng. Digital signcryption or how to achieve cost (signature & encryption << cost (signature) + cost (encryption). In *Proc. of Crypto'97*, pages 165–179, 1997.

[6] K. Baba, K. Iwamura, Y. Zheng, and Hideki Imai. A protocol to detect who has leaked a signed document. In *Proc. of SCIS'99 (in Japanese)*, pages 257–262, 1999.

[7] B. Chor, A. Fiat, and M. Naor. Tracing traitors. In *Proc. of Crypto '94*, pages 257–270, 1994.

[8] K.Kurosawa and Y.Desmedt. Optimum traitor tracing and new direction for asymmetricity. In *Proc. of Eurocrypt '98*, pages 145–157, 1998.

[1]This work was performed in part of Research for the Future Program (RFTF) supported by Japan Society for the Promotion of Science (JSPS) under contract no. JSPS-RFTF 96P00604.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

An Efficient Traitor Tracing Scheme for Broadcast Encryption

Maki Yoshida and Toru Fujiwara
Department of Informatics and Mathematical Science, Osaka University
1-3 Machikaneyama, Toyonaka, Osaka, 560-8531 Japan
e-mail: {maki-yos,fujiwara}@ics.es.osaka-u.ac.jp

Abstract — **An efficient traitor tracing scheme for broadcast encryption is proposed. Its security depends on the difficulty of discrete logarithm problem and is equivalent to ElGamal public-key cryptosystem even when subscribers collude. The proposed scheme is the first one which satisfies all the following features: The tracing algorithm is black box tracing; All the traitors are identified from a captured pirate decoder; The data supplier can encrypt the contents such that only a specific subset of subscribers' decoders can decrypt it; The encryption algorithm is public-key.**

I. Introduction

A *broadcast distribution system* (BDS) is a system where the data supplier broadcasts the contents in encrypted form and gives each subscriber a decoder containing a secret decryption key, e.g., pay-TV. For a BDS, there are two requirements: At least one traitor can be identified from a captured pirate decoder which is constructed by t or less traitors; The data supplier can prevent s or less subscribers from decrypting the broadcasted contents in encrypted form. Here, s and t are parameters. To the authors' knowledge, only the BDS in [1] satisfies both $s > 0$ and $t > 0$, while it is not efficient. We construct an efficient BDS by limiting its security and the parameters to computationally theoretical one and $s = t$, respectively. The proposed BDS is based on the BDS with $s = 0$ and $t > 0$ in [2] and uses the idea of a group key distribution scheme in [3] to make $s > 0$. Compared with the BDS in [2], the proposed BDS can identify traitors even if a captured pirate decoder is used only as a black box. Note that, for a group key distribution, there is no need to trace traitors. Actually, that is not discussed in [3].

II. Proposed System

We label all the n subscribers from 1 to n. The set of all the n subscribers is denoted by Φ, i.e., $\Phi = \{1, 2, ..., n\}$. Let p and q be prime numbers with $q|p-1$. The multiplicative group of order $p-1$ is denoted by Z_p^*. Let g be a q-th root of unity, and G_q denote a subgroup of Z_p^* of order q, i.e., $G_q = \{g^z : 0 \le z < q\}$. Let I_q denote the set of nonnegative integers less than q. All the subscribers and the data supplier agree on the prime numbers p, q and the generator g.

The secret decryption key for the subscriber i is $d_i = (i, f(i))$, where $f(x) \triangleq a_0 + a_1 x + a_2 x^2 + \cdots + a_t x^t \bmod q$ with $a_0, a_1, \ldots, a_t \in I_q$. The encryption key is $e = (p, g, y_0, y_1, \ldots, y_t)$, where $y_i = g^{a_i}$ with $0 \le i \le t$.

The broadcasted contents in encrypted form consists of an enabling part and a cipher part. The cipher part is the symmetric encryption of the contents under a session key. For each distribution, a session key is chosen randomly. Let Λ denote the set of t or less subscribers whom the data supplier prevents from obtaining the contents encrypted under the session key k_s. For k_s and $\Lambda \triangleq \{x_1, x_2, \ldots, x_{|\Lambda|}\}$, the data supplier generates the enabling part, denoted $B(k_s, \Lambda)$, $(g^r, k_s y_0^r, (x_1, g^{rf(x_1)}), (x_2, g^{rf(x_2)}), \ldots, (x_t, g^{rf(x_t)}))$ where r is a random element in I_q and relatively prime to $p-1$, and every x_i with $|\Lambda| < i \le t$ is chosen from $I_q \setminus (\Phi \cup \{0\})$. $g^{rf(x_i)}$ can be computed from e and r by $g^{rf(x_i)} = (y_0 \times y_1^{x_i} \times y_2^{x_i^2} \times \cdots \times y_t^{x_i^t})^r$.

For $B(k_s, \Lambda)$, only a subscriber m with $m \notin \Lambda$ can compute $g^{rf(0)}$ by performing Lagrange interpolation formula for $f(x)$ implicitly in the exponent of g^r, and obtain k_s.

Suppose a pirate decoder constructed by a coalition $\mathcal{C}$ of t or less traitors is captured. Even if the pirate decoder is used only as a black box, the traitors can be identified as follows: For every set of t subscribers, denoted by Λ, generate the enabling part $B(k_s, \Lambda)$ where k_s is taken over G_q at uniformly random; Give every generated enabling part to the pirate decoder; Suppose that the pirate decoder does not output the session key for the l enabling parts, $B(k_{s1}, \Lambda_1), B(k_{s2}, \Lambda_2), \ldots, B(k_{sl}, \Lambda_l)$; The set of all the traitors is $\bigcap_{i=1}^{l} \Lambda_i$ under the same assumption that in [1] where a pirate decoder outputs the contents as long as the input is an enabling part and at least one traitor is not in Λ. The reason is that $\mathcal{C} \subseteq \Lambda_i$ for every Λ_i with $1 \le i \le l$ and there is no $\mathcal{C}'$ such that $\mathcal{C} \subset \mathcal{C}' \subseteq \Lambda_i$ with $1 \le i \le l$ under the above assumption.

III. Discussion on Efficiency and Security

When evaluating a BDS, two complexity measures are to be considered: the size of an enabling part and that of a secret decryption key. The enabling part consists of $2t + 2$ elements in Z_p^* and each secret decryption key consists of two elements in Z_p^*. The proposed system is much more efficient than the BDS in [1] where those are $O(t^2)$ and $O(t^6)$, respectively, and as efficient as the most efficient system in [2] where those are $t + 1$ and 1, respectively.

Even if the encryption key e is made public, for every Λ with $|\Lambda| \le t$, the computational complexity for Λ to compute k_s is shown to be as hard as to compute a plaintext in ElGamal public-key cryptosystem over Z_p^*. The computational complexity for $\mathcal{C}$ to obtain a secret decryption key $(u, f(u))$ where $u \notin \mathcal{C}$, when given e and traitors' secret decryption keys d_i with $i \in \mathcal{C}$, is shown to be as hard as the discrete logarithm problem over Z_p^*.

References

[1] D.R. Stinson and R. Wei, "Key preassigned traceability schemes for broadcast encryption," SAC '98, Lecture Notes in Computer Science, vol. 1556, pp.144–156, 1998.

[2] K. Kurosawa and Y. Desmedt, "Optimum traitor tracing and asymmetric schemes," EUROCRYPT '98, Lecture Notes in Computer Science, vol. 1403, pp.145–157, 1998.

[3] N. Matsuzaki, J. Anzai and T. Matsumoto, "A method for masked sharing of group keys (II)," (in Japanese) IEICE Technical Report, ISEC98-124, March 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Inherently Large Traceability of Broadcast Encryption Scheme

Kaoru Kurosawa
Tokyo Institute of Technology
kurosawa@ss.titech.ac.jp

Takuya Yoshida
Tokyo Institute of Technology
takuya@ss.titech.ac.jp

Yvo Desmedt [1]
Florida State University
desmedt@cs.fsu.edu

Abstract — **We say that a broadcast encryption scheme is a (c, N)-Broadcast Exclusion Scheme (BEx) if a center can exclude c or less users among N users. In this paper, we present an efficient (c, N)-BEx which has inherently large traceability by showing a new construction of cover free families.**

I Previous works

Assume that there exist secure block ciphers. It was recently shown that a (c, N)-BEx is obtained from a cover free family by Kumar et al. [1] and the authors [2] independently. Kumar et al. also presented a construction of cover free families such that *overhead* $= O(c^2)$, which is independent of N, by using algebraic geometry codes, where *overhead* $\triangleq$(the length of a ciphertext)/(the length of a plaintext).

A set system is a pair $(X, \mathcal{B})$, where $X \triangleq \{1, 2, \ldots, v\}$ and $\mathcal{B}$ is a set of blocks $B_i \subset X$ with $i = 1, 2, \ldots, N$. We consider a set system such that $|B_i| = k$ for $i = 1, 2, \ldots, N$.

Definition I.1 *[3] We say that $\{X, \mathcal{B}\}$ is a (v, N, k, c, D)-cover free family if $|B_{i_0} \setminus \bigcup_{j=1}^{c} B_{i_j}| \geq D$ for $\forall B_{i_1}, \ldots, \forall B_{i_c}$ and for $\forall B_{i_0} \notin \{B_{i_1}, \ldots, B_{i_c}\}$.*

On the other hand, a broadcast encryption scheme is said to have c-traceability if when a set of at most c users (who are not necessarily excluded) pool their keys together to construct a "pirate decoder", at least one of the users (a traitor) involved can be identified from the decoder [4].

Definition I.2 *[5] We say that $(X, \mathcal{B})$ is a c-(v, N, k) traceable set system if for $\forall B_{i_1}, \ldots, \forall B_{i_c}$ and for $\forall B_{i_0} \notin \{B_{i_1}, \ldots, B_{i_c}\}$,*

$$|F \cap B_{i_0}| < \max_{1 \leq j \leq c} |F \cap B_{i_j}| \quad (1)$$

for any $F \subset \bigcup_{j=1}^{c} B_{i_j}$ such that $|F| = k$.

In the c-traceability scheme, B_i is the key of user i and F corresponds to the pirate key. From Eq.(1), we see that a traitor is detected by computing $\max_i |F \cap B_i|$.

II Proposed construction

In [1, page 614], it was remarked that cover free families could be used to construct traceability schemes. Actually, we can prove the following theorem.

Theorem II.1 *If there exists a (v, N, k, c, D)-cover free family, then there exists a (c, N)-BEx such that overhead $= v/D$. Further, if $k < D + \lceil D/c \rceil$, then it can be used as a c-traceability scheme as well.*

[1] A part of this research was funded by NSF CCR-9903216.

In this section, we show a construction of cover free families which satisfy both *overhead* $= O(c^2)$ and $k < D + \lceil D/c \rceil$ by using almost strongly universal hash functions. Even for BExs only, our construction is conceptually much simpler and much easier than that of [1].

Let X and Y be finite sets such that $|X| \geq |Y|$. Let H be a set of functions such that $h : X \to Y$ for each $h \in H$. Let $|H| = v$, $|X| = m$, $|Y| = n$.

Definition II.1 *[6] We say that H is an ϵ-almost strongly universal (ϵ-$ASU_2(v, m, n)$) hash function family provided that the following two conditions are satisfied:*

1. *for any $x \in X$ and any $y \in Y$, there exist exactly $|H|/|Y|$ functions $h \in H$ such that $h(x) = y$.*
2. *for any two distinct elements $x_1, x_2 \in X$ and for any two (not necessarily distinct) elements $y_1, y_2 \in Y$, there exist at most $\epsilon|H|/|Y|$ functions $h \in H$ such that $h(x_i) = y_i$, $i = 1, 2$.*

Theorem II.2 *If there exists an ϵ-$ASU_2(v, m, n)$ hash function family H, then there exists a (v, N, k, c, D)-cover free family such that $N = mn$, $k = v/n$, $D = \frac{v}{n}(1 - c\epsilon) + 1$.*

Theorem II.3 *There exists a ϵ-$ASU_2(v, m, n)$ hash function family such that $v = q^{l+2}$, $n = q$, $m = q^{lq^t}$ and*

$$\epsilon = \frac{l}{q} + \frac{1}{q^{l-t}} - \frac{1}{q^l}$$

for $1 \leq \forall t < \forall l < \forall q =$ prime power.

Corollary II.1 *There exists a (v, N, k, c, D)-cover free family such that $v = q^{l+2}$, $N = q^{lq^t+1}$, $k = q^{l+1}$ and $D = q^{l+1} - c(lq^l + q^{t+1} - q) + 1$ for $1 \leq \forall t < \forall l < \forall q =$ prime power.*

Corollary II.2 *Let q be a prime power and let $c = \sqrt{q/3}$. Then there exists a (c, N)-BEx such that overhead $= O(c^2)$. Further, it can be used as a c-traceability scheme as well.*

(Proof) Let $t = 1$ and $l = 2$.

References

[1] Kumar, Rajaoplan and Sahai.: Coding construction for blacklisting problems without computational assumptions, Advances in Cryptology – CRYPTO '99, Lecture Notes in Computer Science #1666. Springer-Verlag (1999) 609–623

[2] T.Yoshida, Y.Desmedt and K.Kurosawa: How to break the bound of Broadcast Encryption, submitted to Crypto'99.

[3] Dyachkov, A.G. ; Rykov, V.V. ; Rashad and A.M. Source: Problems of Control and Information Theory, vol.18, no.4, pp. 237-250 (1989) ISSN: 0370-2529 CODEN: PUTIAI In English

[4] B. Chor, A. Fiat, and M. Naor. "Tracing traitors". In *Proc. of Crypto'94, Lecture Notes in Computer Science, LNCS 839, Springer Verlag*, pages 257–270, 1994.

[5] D. Stinson and R. Wei. "Combinatorial properties and constructions of traceability schemes and frameproof codes". In *SIAM J. on Discrete Math., vol.11, no.1*, pages 41–53, 1998.

[6] J. L. Carter and M. N. Wegman, "Universal classes of hash functions," J. Computer and System Sci., Vol. 18, pp. 143–154, 1979.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Reducing Oblivious String Transfer to Universal Oblivious Transfer

Stefan Wolf [1]

Abstract — **It is shown that oblivious transfer of strings can be reduced to the weakest version of oblivious bit transfer, where the receiver can choose to obtain arbitrary (but incomplete) information about the pair of bits sent. This solves an open problem posed by Brassard and Crépeau.**

I. Equivalence Between Oblivious Transfers

Important cryptographic primitives, such as secure message transmission, key agreement, or secure multi-party computation, can often be reduced to apparently much weaker primitives such as noisy communication channels or correlated randomness. In this note we present an information-theoretic reduction of so-called *1-out-of-2 oblivious string transfer* to a weak variant of oblivious bit transfer, called *universal oblivious transfer*. Oblivious-transfer primitives are of central importance for many cryptographic protocols. In principle, oblivious transfer allows for carrying out any secure two-party computation.

The standard *oblivious bit transfer* (bit OT) between two parties corresponds to a binary erasure channel with erasure probability 1/2: The sender's input is a bit b, which the receiver learns with probability 1/2, whereas otherwise, he obtains no information about b. The sender on the other hand does not learn whether the bit has been received or not.

In *1-out-of-2 bit OT* ($\binom{2}{1}$-OT for short) the sender sends two one-bit messages, exactly one of which the receiver can choose to read, remaining completely ignorant about the other one, such that the sender does not get any information about which message has been chosen. In *1-out-of-2 k-bit-string OT* ($\binom{2}{1}$-OT^k) the messages are k-bit strings instead of single bits.

The problem of reducing *string* OT to *bit* OT was studied by many authors (see [1] and the references therein). In [1], a reduction was presented based on so-called *privacy amplification* by hashing with linear functions. It was even shown that $\binom{2}{1}$-*OT^k with security s*, i.e., such that with probability at least $1 - 2^{-s}$, the receiver obtains no information at all about one of the transmitted strings, even when given the other, can be reduced to $n = O(k + s)$ realizations of *generalized OT (GOT)*, where the receiver can choose to learn any one-bit function (such as b_0, $b_0 \oplus b_1$, or $b_0 \wedge b_1$) about the two bits b_0 and b_1 sent. Protocol BC, which achieves this, works as follows. First, GOT is applied n times with random input bits (x_i, y_i). Then, the two k-bit messages m_0 and m_1 to be sent by $\binom{2}{1}$-OT^k are blinded by (i.e., xor-ed with) two k-bit strings $h_0(x_1, \ldots, x_n)$ and $h_1(y_1, \ldots, y_n)$, respectively, where h_0 and h_1 are two linear functions from n-bit to k-bit strings, chosen randomly and published by the sender.

It was stated as an open problem in [1] how this result generalizes to a primitive offering the receiver the possibility to obtain *arbitrary* (probabilistic) information about the pair (b_0, b_1). We show that the most optimistic answer is the correct one: Whenever the information the receiver obtains in such *universal OT (UOT)* does not completely determine (b_0, b_1), then string OT can be reduced to this primitive. The argument is based on the fact that among all types of an adversary's side information about a single bit with given error probability, there exists a "strictly worst case," namely information obtained from a symmetric erasure channel. This also allows for simplifying the proofs given in [1] and for improving the results with respect to the involved constants. Related results in models different from the one of [1] were shown in [2].

II. The Power of Universal OT

Definition 1. Let $\alpha > 0$. In *universal OT with parameter* α (α-UOT), the sender's input is a pair of bits (b_0, b_1). The receiver specifies a possibly probabilistic function Ω which must satisfy $H((b_0, b_1) \,|\, \Omega(b_0, b_1)) \geq \alpha$ if (b_0, b_1) is uniformly distributed. Then the receiver obtains $\Omega(b_0, b_1)$, but no additional information about (b_0, b_1). The sender on the other hand does not learn anything about Ω.

Theorem 1. *Protocol BC reduces $\binom{2}{1}$-OT^k with security s to at most $\lceil (s + 2k) \ln 2 / p_e \rceil$ realizations of α-UOT, where p_e is the unique solution ($\leq 1/2$) to the equation $h(2x) + 2x \log 3 = \alpha$.*

Lemma 2. *Let B be a symmetric binary random variable, and let U be a random variable such that B and U have joint distribution P_{BU}. Let p be the average error probability of guessing B when given U, using the optimal guessing strategy. Then there exists a random variable V with the following properties. First, $\mathcal{V} = \{0, 1, \Delta\}$ and $P_V(\Delta) = 2p$ hold, and for every $u \in \mathcal{U}$, we have $P_{B|U=u,V=\Delta}(0) = P_{B|U=u,V=\Delta}(1)$.*

Proof. Let $u \in \mathcal{U}$, and assume that $a = P_{B|U=u}(0) > P_{B|U=u}(1) = b$. Let V be defined by $P_{V|B=0,U=u}(0) = (a - b)/a$, $P_{V|B=0,U=u}(\Delta) = b/a$, and $P_{V|B=1,U=u}(\Delta) = 1$. Note that $P_{V|U=u}(\Delta) = 2b$, i.e., twice the error probability for guessing B when given $U = u$. □

The idea of the proof of Theorem 1 is as follows. By Fano's inequality, one can conclude that, when the pair (x_i, y_i) is sent by α-UOT, about at least two of the bits x_i, y_i, and $x_i \oplus y_i$, the receiver's error probability when guessing the bit with the optimal strategy is at least p_e. Because of Lemma 2, we can assume that with probability at least $2p_e$, the receiver has no information at all about such a bit. By construction, this implies that with overwhelming probability, the receiver cannot bias $g(h_0(x_1, \ldots, x_n), h_1(y_1, \ldots, y_n))$ for any linear function g with range $\{0, 1\}$ and depending non-trivially on both inputs. In this case, he has no information at all about one of the inputs, even when given the other.

References

[1] G. Brassard and C. Crépeau, "Oblivious transfers and privacy amplification," *Advances in Cryptography – EUROCRYPT' 97*, LNCS, Vol. 1233, pp. 334–345, Springer-Verlag, 1997.

[2] C. Cachin, "On the foundations of oblivious transfer," *Advances in Cryptography – EUROCRYPT' 98*, LNCS, Vol. 1403, pp. 361–374, Springer-Verlag, 1998.

[1] Department of Computer Science, ETH Zürich, CH–8092 Zürich, Switzerland. E-mail: wolf@inf.ethz.ch

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Asymptotically Optimal Waterfilling in Multiple Antenna Multiple Access Channels

Pramod Viswanath,[1]
Department of EECS,
University of California at Berkeley,
Berkeley, CA94720-1772.
e-mail:pvi@eecs.berkeley.edu

David N. C. Tse
Department of EECS,
University of California Berkeley,
Berkeley, CA94720-1772.
e-mail:dtse@eecs.berkeley.edu

Venkat Anantharam
Department of EECS,
University of California Berkeley,
Berkeley, CA94720-1772.
e-mail:ananth@eecs.berkeley.edu

Abstract — **This paper considers "vector multiple access channels" (VMAC) where each user has multiple "degrees of freedom" and studies the effect of power allocation as a function of the channel state on the "sum capacity" defined as the maximum sum of rates of users per unit degree of freedom at which the users can jointly reliably transmit, in an information theoretic sense. A concrete example of a VMAC is a MAC with multiple antennas at the receiver where the antennas provide spatial degrees of freedom. Our main result is the identification of a simple dynamic power allocation scheme that is optimal in a large system, i.e., in the regime of a large number of users and a correspondingly large number of antennas. A key feature of this policy is that, for any user, it depends only on the instantaneous amplitude of the slow fading component of the vector channel of that user alone and the structure of the policy is "waterfilling".**

I. Introduction and Problem Statement

A discrete time baseband frequency flat channel fading model for the multiple antenna, multiple access channel is the following:

$$\mathbf{y}(n) = \sum_{i=1}^{K} x_i(n) h_i^s(n) \mathbf{h}_i^f(n) + \mathbf{w}(n) \ .$$

Here K denotes the number of users and n the channel use instant. The user symbols are denoted by x_i and $\mathbf{y}(n)$ is the received signal (thought of as a N dimensional vector, N being the number of antennas at the receiver) at the antenna array at time instant n. Here $\mathbf{w}(n)$ is an additive white Gaussian noise. The channel (a vector with N components) from user i to the antenna array at time instant n is written as $h_i^s(n)\mathbf{h}_i^f(n)$. Here h_i^s is a scalar that varies *slowly* in time and captures the distance loss and the shadowing effects and thus depends only on the user. The fast fading component which is changing due to the destructive and constructive additions of the signals from multiple paths is represented by the vector $\mathbf{h}_i^f$ which depends on the individual antenna elements. For the purpose of this summary, we will assume that $\{h_i^s(n)\}_n$ and $\left\{\mathbf{h}_i^f(n)\right\}_n$ are independent stationary and ergodic processes. We are interested in the scenario of coherent communication, the scenario when the receiver is able to track the channel variations reliably.

Our performance measure is the long term sum capacity: sum of rates at which users jointly reliably communicate. These rates are time averaged with a power constraint on the users which is also averaged in time. We are interested in the characterizing sum capacity with and without feedback of channel states to the users. If there is no feedback to the users, then a coding theorem shows that the users transmit at constant power. When there is feedback information of the channel state, users can modulate their power based on this knowledge. The problem addressed here is the characterization of the power allocation policies that are optimal in the sense of maximizing sum capacity of the system.

II. Main Result

In the one antenna scenario, there is a simple characterization of the optimal power policy (only the user with the best channel is allowed to transmit and this user uses a waterfilling power policy) and the gap between sum capacity by using this optimal policy and the sum capacity with no channel state feedback is very large (unbounded in the number of users). However, in the general case of multiple antennas, there is no closed form solution to the optimal power policy which for any user is some function of the paths from all the users to the antenna array. Our main result below identifies a simple waterfilling power allocation policy that is optimal in the regime of large number of users and antennas: consider the power policy that for any user depends only on the slow fading component of that user alone and the structure is that of "waterfilling". Observe that in the regime when slow fading is constant over the time scale of communication, this policy simply allocates constant power. Our main result is that this is a very good approximation to the complicated optimal power policy. In particular, this means that feeding back only the slow fading component is asymptotically sufficient in the multiple antenna scenario. Denoting the ratio of users to antennas by $\lfloor \alpha N \rfloor$, we have our main result below.

Theorem 1 *For all α, for all SNR levels, for all fading distributions,*

$$\limsup_{N\to\infty} \sqrt{N} \, (\textit{Sum Capacity with optimal power policy} - \textit{Sum Capacity with waterfilling policy}) < \infty$$

The details of this summary are available in [1].

References

[1] P. Viswanath, D. Tse and V. Anantharam, "Asymptotically Optimal Waterfilling in Vector Multiple Access Channels", accepted in *IEEE Transactions on Information Theory* subject to minor revisions, Feb 2000. Also available as UCB/ERL Memorandum. M99/54.

[1]This work was supported by NSF under grant IRI 97-12131 and by an NSF CAREER Award under grant NCR 97-34090

0-7803-5857-0/00/$10.00 ©2000 IEEE.

A Resource Pooling Result for a CDMA Antenna Array

S.V. Hanly [1]
Dept. of Electrical and Electronic Engineering
University of Melbourne
Parkville Victoria 3052 Australia
e-mail: s.hanly@ee.mu.oz.au

D.N. Tse [2]
Dept. of Electrical Engineering and Computer Science
University of California at Berkeley
Berkeley CA 94720, USA
email: dtse@eecs.berkeley.edu

I. Introduction

We consider a spread spectrum, multi-user channel, with an antenna array at the receiver, and independent flat fading to each antenna from each user. We focus on the case of microdiversity, and show that a curious phenomenon of "resource pooling" arises.

II. Basic Multi-Antenna Model

We consider a sampled discrete-time baseband model for a symbol-synchronous multi-access CDMA system with K users, L receive antennas and processing gain N. The received signal at the lth antenna is given by

$$\mathbf{Y}(l) = \sum_{k=1}^{K} X_k \sqrt{T_k}\gamma_k(l)\mathbf{s}_k + \mathbf{W}(l), \qquad (1)$$

where X_k is the symbol transmitted by user k at transmit power T_k, $\gamma_k(l)$ is the complex fading channel gain from user k to antenna l, $\mathbf{s}_k \in \mathbb{C}^N$ is the signature sequence of user k, $\mathbf{Y}(l) \in \mathbb{C}^N$, and $\mathbf{W}(l)$ is additive white Gaussian noise with variance σ^2, independent across l. The symbol energy $\mathbb{E}[X_i^2]$ is normalized to be 1. Here, we are assuming a flat fading channel model, and the channel gains are assumed to be circular symmetric, as is typical for a baseband model. Furthermore, we make the additional assumption of "microdiversity": we assume that the marginal distributions of the $\gamma_k(l)$s are identical, across both antennas, and users. We will also allow the transmit powers T_ks to depend on the magnitudes of the channel gains $\gamma_k(l)$ for all k and l, but independent of everything else. This models the use of power control.

The optimal linear receiver is known as the MMSE receiver. While an explicit expression for the SIR of the MMSE is well known, we obtain more insight by proving an asymptotic result as the system grows large, under randomly selected signature sequences: assume that the chip values of the sequences are i.i.d. circular symmetric complex Gaussian random variables with mean zero and variance $1/N$, and the sequences of different users are chosen independentliy.

[1]Supported by an Australian Research Council Small Grant
[2]Partially supported by a National Science Foundation Early Faculty Career Award.

III. Main Result

Theorem 1 *Let $P_k = T_k \sum_{l=1}^{L} |\gamma_k(l)|^2$ be the sum of the received powers of user k. Assume that almost surely the empirical distribution of $(P_1, \ldots, P_K)$ converges weakly to a limiting distribution F as N goes large, and that the P_ks are uniformly bounded for all k and N [1]. Then if $N, K \to \infty$ with $K/N \to \alpha$ but L fixed, SIR_1/P_1 converges in probability to a deterministic constant a, where a is the unique positive solution to the fixed-point equation:*

$$a = \frac{1}{\sigma^2 + \frac{\alpha}{L}\mathbb{E}\left[\frac{P}{1+Pa}\right]} \qquad (2)$$

and P is a random variable having distribution F.

Proof See [2]. ∘

This result says that in a wideband system with many users, the SIR of a user does not depend on the specific realization of the signature sequences, the channel gains and the transmit powers. The SIR is a function of the user's own received powers at the antennas and depends on the the interferers' received powers only through the limiting empirical distribution of the P_ks. In a sense, there is an averaging of the effects across the large number of interferers. Furthermore, by comparing this result with our main result in [1], we see that the multiantenna system here is behaving, asymptotically, just like a single antenna system with users per degree of spreading of $\frac{\alpha}{L}$, and received power being the pooled received power from the multi-antenna system.

References

[1] D.N. Tse, S.V.Hanly (1999) "Linear Multiuser Receivers: Effective Interference, Effective Bandwidth and User Capacity," *IEEE Trans. on Information Theory* , vol. 45, No. 2, pp641–657, 1999.

[2] S.V. Hanly, D.N. Tse "Resource Pooling and Effective Bandwidths in CDMA Networks with Multiuser Receivers and Spatial Diversity," to appear in *IEEE Trans. on Information Theory.* in CDMA

[1]This latter assumption is a technicality to simplify the proofs, but we believe that it is not really necessary.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Optimal Dynamic Power Control for CDMA Systems

Jean-François Chamberland
School of Electrical Engineering
Cornell University
Ithaca, NY 14853, USA
e-mail: jfcham@ee.cornell.edu

Venugopal V. Veeravalli [1]
School of Electrical Engineering
Cornell University
Ithaca, NY 14853, USA
e-mail: venu@ee.cornell.edu

Abstract — **The design of binary power control algorithms for cellular communication systems is considered in context of *code division multiple access* (CDMA). The control problem is posed as a tradeoff between the desire for users to meet their *signal-to-interference ratio* (SIR) requirements and the need to minimize the transmitted signal energy over the duration of their calls. The dynamic nature of the wireless channel for mobile users is incorporated in the problem definition. Based on dynamic programming arguments, an optimal single-user solution is obtained.**

I. Introduction

The analysis of power control for wireless multi-access systems has been well documented over the past decades, with new contributions often motivated by the need to address practical issues. Much of the work on uplink power control for CDMA systems has been focusing on static channel models, i.e., models in which the channel gain of every user is assumed constant. The performance results obtained under this assumption will be valid as long as the reaction time of the power control algorithm is small compared to the coherence time of the underlying wireless channel. In other words, the transmitted power of each user is implicitly assumed to converge to its optimal level before any significant change occurs in the channel state. We propose a different approach to the design of power control algorithms and include a dynamic stochastic channel model as part of the problem definition.

II. Problem Formulation

We address the control problem as a tradeoff between the desire for users to meet their SIR requirements and the need to minimize transmitted energy over time intervals in-between control signals. Effectively, this formulation leads to a tradeoff between the user capacity of the overall system and the link quality of individual users. We wish to solve this design problem using dynamic programming. To cast the problem into a dynamic programming framework, we need to develop a discrete-time model for the underlying wireless channel, and to define an appropriate cost function.

We adopt the standard tap-delay line channel model [5] and assume the channel gains to vary slowly with respect to the time interval in-between control signals. In dealing with slowly varying channel gains, it is convenient to develop an equivalent discrete-time channel model for the analog system. After maximal ratio combining, the discrete-time channel gain $G[\cdot]$ becomes a function of the gain coefficients $\{E_\ell[\cdot]|_{\ell=1}^{L}\}$, and is given by $G[k] = \sum_{\ell=1}^{L} |E_\ell[k]|^2$, where L is the number of resolvable paths.

We define the individual cost g as a function of the target SIR $\tilde{\gamma}$, and the actual SIR at the receiver γ. When γ is below the target SIR $\tilde{\gamma}$, a fixed cost is incurred, which accounts for the user not meeting the target SIR requirement. Otherwise, the SIR at the output of the receiver exceeds the target SIR and we make the cost function proportional to the excess of transmitted energy. The cost per stage function captures the tradeoff between the desire for users to meet their SIR requirements and the need to minimize the transmitted energy over the control period.

We pose the optimization problem as a discounted cost infinite horizon problem [4]. The discounting factor $\alpha < 1$ reflects the uncertainty on the time duration of a call and our level of confidence in the accuracy of the channel parameters over time. Given an initial state $\mathbf{x}_0$ (channel plus transmitted power) and a discounting factor, we want to minimize the total cost $J(\mathbf{x}_0) = \lim_{N\to\infty} \mathrm{E}\left[\sum_{k=0}^{N-1} \alpha^k g(\mathbf{x}_k)\right]$. Standard dynamic programming steps lead to an optimal stationary policy which satisfies Bellman's equation.

III. Discussion and Conclusion

The dynamic programming algorithm yields as a solution a look-up table. Although large look-up tables are hard to implement, this solution provides an upper bound on the performance of practical systems. For instance, the performance of the best threshold policy comes close to that of the dynamic programming solution. Thus, the technique we developed can be employed to assess the performance of simpler, easily implementable algorithms.

References

[1] S.V. Hanly, "Capacity and Power Control in Spread Spectrum Macrodiversity Radio Networks," *IEEE Trans. on Communications*, vol. 44(2), pp. 247-256, 1996.

[2] R.D. Yates, "A Framework for Uplink Power Control in Cellular Radio Systems," *IEEE Journal on Selected Areas in Communications*, vol. 13(7), pp. 1341-1348, 1995.

[3] G.J. Foschini and Z. Miljanic, "A Simple Distributed Autonomous Power Control Algorithm and its Convergence," *IEEE Trans. on Vehicular Technology*, vol. 42(4), pp. 641-646, 1993.

[4] D.P. Bertsekas, "Dynamic Programming and Optimal Control," *Athena Scientific*, Belmont, MA, 1995.

[5] J.G. Proakis, "Digital Communication, 3rd Edition," *McGraw-Hill*, New York, NY, 1989.

[1]This research was supported in part by a NSF CAREER/PECASE grant under CCR-9733204, and by the Office of Naval Research under grant N0014-97-1-0823. J.-F. Chamberland was also supported by a Fonds FCAR fellowship.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Admission Control and Resource Allocation for DS-CDMA Networks with Multiple Traffic Classes

Rong-Rong Chen
Coordinated Science Laboratory
University of Illinois at
Urbana-Champaign
Urbana, IL 61801
e-mail: r-chen1@uiuc.edu

Upamanyu Madhow[1]
Department of Electrical and
Computer Engineering
University of California
Santa Barbara, CA 93106
e-mail: madhow@ece.ucsb.edu

Abstract — **The purpose of this paper is to provide a framework for resource allocation and admission control in a DS-CDMA system in which there are several traffic classes with different rates and quality of service requirements. We focus on uplink (mobile to base) transmission, in which the transmissions from different mobiles are uncoordinated. For special cases of two traffic classes, we show that, for large systems, a Gaussian approximation for the interference yields that the boundary of the admission control region is approximately a straight line and the optimal power ratio P_2/P_1 is roughly the same throughout the boundary of the admission control region.**

I. Introduction

Our framework is based on the following assumptions:
(a) The users transmit using fixed-length packets, and are assumed to be synchronized at the packet level. Thus, the system is time-slotted, with a slot equal to a packet duration.
(b) The traffic generated by a user may be bursty (e.g., voice, variable bit rate video, TCP). However, we assume that the bit rate over a given packet is constant, which means that the processing gain over a packet is fixed (since the chip rate is fixed).
(c) The event of packet loss for a given user is well approximated by the event that the Signal-to-Interference-plus-Noise Ratio (SINR) falls below a threshold.

II. System Model

We consider on-off traffic sources here, for which the offered bit rate can take one of only two possible values, the peak rate and zero. For an on-off source of traffic class i, the processing gain when the source is on is determined by its peak rate, and is denoted by N_i. Our purpose is to determine the region determined by the allowable tuples $(K_1, K_2, ...)$, where K_i denotes the number of sources of type i. This also requires determining the optimal values of the received powers $\{P_i\}$, where P_i denotes the desired received power for a user of type i. Our model is simpler than the models in [1] and [2], in that we allow the processing gain to be fixed by the offered rate, and only choose the received powers for the different traffic classes. This enables us to obtain a simpler characterization of the admission control region.

III. Main results

Since we consider on-off sources, at each given time slot, we assume each user of traffic type i is active with probability p_i. The allowable packet loss rate for a user of type i is q_i. The packet loss event for a user of type i is approximated by the event that the SINR seen by the packet falls below a threshold γ_i. For simplicity of illustration, we employ the SINR expression for a chip-synchronous DS-CDMA system with conventional matched filter reception, so that the SINR for a typical packet of type i is given by

$$SINR_i = \frac{P_i N_i}{\sum_{k=1}^{K_i-1} \chi_{ik} P_i + \sum_{j\neq i}^{2} \sum_{k=1}^{K_j} \chi_{jk} P_j + \sigma^2}$$

where χ_{ik} is an on/off indicator (i.e., $\chi_{ik} = 1$ if user k of type i is active, and 0 else), and σ^2 is the background noise power, which indicates the inter-cell interference. The on/off indicators $\{\chi_{ik}\}$ are assumed to be independent random variables and $P[\chi_{ik} = 1] = p_i, P[\chi_{ik} = 0] = 1 - p_i$. We consider the case of two traffic classes. Given K_1 and K_2, we say that (K_1, K_2) is *admissible* if the following conditions are satisfied:

$$P[SINR_i < \gamma_i] < q_i, \; i = 1, 2. \tag{1}$$

Assuming that the contribution of a single user's power to the total transmitted power is negligible, we can rewrite (1) as

$$P[X_1 + rX_2 > a_1] < q_1, \quad P[X_1 + rX_2 > a_2 r] < q_2, \tag{2}$$

where $r = P_2/P_1$, $a_i = N_i/\gamma_i - \sigma^2/P_1$, $X_i = \sum_{k=1}^{K_i} \chi_{i_k}$, $i = 1, 2$. When the system size is large, we may approximate $X_1 + rX_2$ by a Gaussian random variable based on the Central Limit Theorem. For a class of specific scenarios considered in the paper, we obtain the following results:

(a) Given K_1, the number of users of type 1, there is an optimal value of $r(K_1)$ such that the number of users of type 2 admissible is maximized.

(b) For a large system, the maximum number of users of type 2 is approximately a linear function of K_1. Also, the power ratio $r(K_1)$ equals approximately a constant r^*.

Simulation results show that, for large systems, the Gaussian approximation provides an admission region close to the exact admission region, which is also well approximated by fixing the power ratio $r(K_1)$ as a constant r^*.

[1]This work was supported by the National Science Foundation under a CAREER award NSF NCR96-24008CAR and under grant NSF CCR9979381.

References

[1] Michael L. Honig, Joon Bae Kim, "Resource Allocation for Packet Data Transmission in DS-CDMA" *Proc. 33rd Annual Allerton Conference on Communication, Control and computing*, pp. 925–934, 1995.

[2] Seong-Jun Oh, Kimberly M. Wasserman, "Dynamic Spreading Gain Control in Multiservice CDMA Networks", *IEEE Journal on Selected Areas in Communications*, Vol. 17, No. 5, pp. 918–927, May 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Evaluation for Convergence of Wavelet-Based Estimators on Fractional Brownian Motion[1]

Shuhji Kawasaki and Hiroyoshi Morita
Graduate School of Information Systems,
University of Electro-Communications
Chofu, Tokyo, 182-8585
e-mail: {kawasaki,morita}@is.uec.ac.jp

Abstract — **Two wavelet-based estimators on fractional Brownian motion (FBM) are evaluated through the large deviation principle (LDP). These are $\hat{\sigma}_j^2$ and $\hat{H}$, the estimators of (i) the variance of wavelet coefficients of FBM for each scale j and (ii) the Hurst parameter, respectively, where $\hat{H}$ is obtained from the slope of the linear regression of $\hat{\sigma}_j^2$ for a number of scales. Both estimators are shown to be consistent from the ergodic theorem. We perform detailed calculations related to LDP for stationary Gaussian processes with unbounded and non-L^2 power spectrum, to obtain L^1-estimates of the convergence of both estimators. A wavelet-based representation of the bias of the estimators is introduced and successfully used in the theory, reflecting the quantitative analysis results on FBM to the corresponding analysis of wavelet coefficients.**

I. Introduction and Preliminaries

Let the wavelet coefficients $\{d_j(k); j \in \mathbf{Z}, k \in \mathbf{N}_0\}$ of FBM $\{B_H(t);\ t \in \mathbf{R}_+\}$ be

$$d_j(k) = \int B_H(t)\,\overline{\psi_{j,k}(t)}\,dt$$

where $\psi_{j,k}(t) = 2^{-j/2}\psi(2^{-j}t - k)$. Let $T_0 > 0$ be a time instant up to which FBM signal is observed. Then, the number $N_j(T_0) \in \mathbf{N}$ of available wavelet coefficients at scale j up to T_0 satisfies $N_j \sim 2^{-j}T_0$. We assume that wavelet ψ is compactly supported on $\mathbf{R}_+$ and satisfies the vanishing moment condition of sufficient order.

The two estimators we consider are $\hat{\sigma}_j^2(T_0)$ and $\hat{H}_{T_0}$, defined by

$$\hat{\sigma}_j^2 = \frac{1}{N_j}\sum_{k=0}^{N_j-1} |d_j(k)|^2,$$

and

$$\log_2\left(\hat{\sigma}_j^2\right) = (2\hat{H}_{T_0} + 1)j + \text{const.}$$

The following relations are fundamental.

Proposition 1. *For $j = 1, \cdots, J$ and $k \in \mathbf{N}_0$,*

$$d_j(k) \overset{(\mathrm{d})}{=} 2^{(H+(1/2))j}\int_{\mathbf{R}_+} B_H(t+k)\,\overline{\psi(t)}\,dt,$$

where $\overset{(\mathrm{d})}{=}$ denotes equality in distribution.

[1]This work was supported by Japan Society for Promotion of Science, 11740057.

For each fixed $s, t \in \mathbf{R}_+$, let $\{Y_k(s,t); k \in \mathbf{N}_0\}$ be such that $Y_k(s,t) = B_H(s+k) - B_H(t+k)$, $k \in \mathbf{N}_0$. $\{Y_k(s,t); k \in \mathbf{N}_0\}$ is a stationary-increment sequence. Let V_H be variance of $B_H(1)$.

Proposition 2. *For each j,*

$$\hat{\sigma}_j^2 - \mathbf{E}[|d_j(0)|^2]$$

$$\overset{(\mathrm{d})}{=} -2^{(2H+1)j}\cdot\frac{1}{2}\int_{\mathbf{R}_+}\int_{\mathbf{R}_+}\overline{\psi(s)}\,\psi(t)\cdot$$

$$\cdot\left[\frac{1}{N_j}\sum_{k=0}^{N_j-1}\left\{Y_k(s,t)\right\}^2 - V_H|s-t|^{2H}\right]dsdt.$$

II. Results

Using the ergodicity of $\{Y_k\}$, we can obtain the consistency of the estimators, in the form of L^1- and a.s. convergence, as well as L^2-convergence.

The following results are our main theorems.

Theorem 3. *There exists a constant $C_H > 0$ such that*

$$\mathbf{E}\left[\,\left|\,\hat{\sigma}_j^2(T_0) - \mathbf{E}[|d_j(0)|^2]\,\right|\,\right] \le C_H\cdot 2^{(2H+(3/2))j}\cdot T_0^{-1/2}$$

for each j.

The L^2-estimate for $\hat{\sigma}_j(T_0) - \mathbf{E}[|d_j(0)|^2]^{1/2}$ is then immediately obtained from the above.

Theorem 4. *There exists a constant $\bar{C}_H > 0$ so that*

$$\mathbf{E}\left[\,|\,\hat{H}_{T_0} - H\,|^2\,\right] \le \bar{C}_H\cdot T_0^{-1}.$$

Theorems 3 and 4 are derived from the following theorem, which itself is obtained from LDP for stationary Gaussian processes.

Theorem 5. *For each $s, t \in \mathbf{R}_+$ and $N \in \mathbf{N}$,*

$$\mathbf{E}\left[\left|\frac{1}{N}\sum_{k=0}^{N-1}\left\{Y_k(s,t)\right\}^2 - V_H\,|s-t|^{2H}\right|\right]$$

$$\le 4\sqrt{\pi}\left(V_H\,|s-t|^{2H}\right)^2\cdot N^{-1/2}.$$

References

[1] P. Abry, P. Goncalves and P. Flandrin, *Wavelets, Spectrum Analysis, and 1/f Processes*, in *Wavelets and Statistics*, 15-29, Lecture Notes in Statistics, Springer, 1995.

[2] P. Abry and D. Veitch, *Wavelet Analysis of Long-Range-Dependent Traffic*, IEEE Trans. IT-**44**, 2-15, 1998.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

A New Reverse Jacket Transform based on Hadamard Matrix

Moon Ho Lee
Institute of Information & Communication. Department of Information & Communication Engineering
Chonbuk National University, Chonju 561-756, KOREA, moonho@moak.chonbuk.ac.kr

ABSTRACT - This paper present Reverse Jacket Transform[RJT] and a simple decomposition of its matrix which is used to develop a fast algorithm for the RJT. The matrix decomposition is of the form of the matrix products of Hadamard matrices and successively lower order coefficient matrices.

I. INTRODUCTION

The Hadamard transform is an orthogonal matrix with highly practical value for representing signals and images especially for the purposes of data compression[1,2]. The reason for the practicality of this transform is the fact that the elements of the Hadamard matrix are either + 2^0(=1) or – 2^0(=-1) Thus, the computation of the transform of a signal consists of additions and subtractions of the signal samples. Recently, Hadamard matrix has been presented in that Walsh-Hadamard transform is the most known of the non-sinusoidal orthogonal transforms. Walsh-Hadamard matrix is used for the Walsh representation of the data sequences in image coding and for Hadamard-Walsh orthogonal sequence generator in CDMA spread spectrum communication. Their basis functions are sampled Walsh functions which can be expressed in terms of the Hadamard $[H]_N$ matrices. Using the orthogonality of Hadamard matrices we construct a generalized Weighted Hadamard matrices [1,2] called $[RJ]_N$ matrix with a reverse geometric structure. In this paper, $[RJ]_N$ and its 5 case matrix examples are described. $[RJ]_N$ is nonorthogonal but its Hadamard matrix, which is subset of $[RJ]_N$ [1],[2] is orthogonal. In this paper we propose a simple recursive factorization for the [RJ] in terms of the Kronecker product of 2*2[RJ] and Hadamard matrices of consecutively lower orders. A consequence of this factorization is a simple and clear fast Hadamard transform algorithm resulting from a block circulant sparse matrix factorization of the [RJ] matrix.

II. THE PROPOSED RJT

Using the orthogonality of Hadamard matrices use construct weighted Hadamard matrices. The $[RJ]_N$ are a generalized conventional$[WH]_N$ and $[H]_N$ [1],[2]. The [RJT] having geometric structure property. The basic idea of this paper was motivated by the cloths of Reverse Jacket. As our two side jacket is an inside and outside compatible, at least two positions of a Reverse Jacket matrix $[RJ]_N$ are replaced by their inverse; these elements are changed their position and are moved for example from inside of the middle circle to outside or from to inside without loss of signs; this is very interesting phenomenon. This is the reason why we call it.Reverse Jacket matrix.

Definition 2.1

A $(2n \times 2n)$matrix $A=(a_{ij})_{i,j=1}^{2n}$, $n \in \mathbf{N}$ is called *Hamiltonian*, if $[AJ]=[AJ]^T$ with $J=\begin{bmatrix} 0 & I_n \\ -I_n & 0 \end{bmatrix}$,

where $I_n \in \mathbf{R}^{2^k \times 2^k}$ is the unit matrix.

Definition 2.2

We define one more notion related to the Hadamard matrix $[H]_{2^k} \in \mathbf{R}^{2^k \times 2^k}$. Let $[RJ]_{2^k} \in \mathbf{R}^{2^k \times 2^k}$ be a $2^k \times 2^k$ matrix. A $2^k \times 2^k$ matrix $[RJ]_{2^k}$ such that

$$[RJ]_{2^k} = [H]_{2^k}^{-1}[RJ]_{2^k}[H]_{2^k},$$

is called the Reverse Jacket matrix, where k is belong to Integer **N**, **R** is Real number. All its components is $\pm 2^n$,(n=0,1,2).

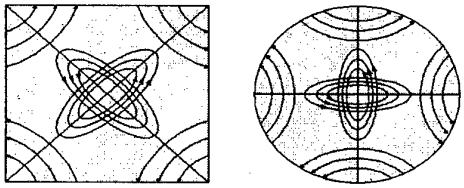


Fig.1. Block-wise circular sparse matrix pattern and Sphere circular sparse matrix like football

Fig 1 shows the expanding block-wise circulant sparse matrix structure. This figure is a plan surface, an interesting point is that the block-wise circulant sparse matrix characterized similiar fashion as football and rotating pattern. This means that when 2×2 sparse matrix is expanded to 4×4 matrix, the element of 2×2 sparse matrix becomes, the pattern of Figure 1.

III. CONCLUSION

The Reverse Jacket matrix is a generalized the weighted Hadamard and the Hadamard matrix. The $[RJ]_N$ matrix has recursive structure and symmetric characteristics. The elements positions of the forward matrix can be replaced by its inverse matrix and the signs of them are not changed between the matrix and its inverse. The $[RJ]_N$ matrix has five cases of basic symmetric matrix according to the construction of elements. The Hadamard matrix is a special case of Reverse Jacket matrix. The fast $[RJ]_N$ transform algorithm is the matrix decomposition of the Hadamard matrices and succesively lower order Weighted coeff.

REFERENCE

[1] Moon Ho Lee, "The Center Weighted Hadamard Transform," IEEE Trans. on Circuits and Systems, Vol. 36, No. 9, pp. 1247-1249, Sep. 1989.
[2] Moon Ho Lee, "The Reverse Jacket Transform and Its fast Algorithm" IEEE Trans. on CAS-II, vol.47, No.1, Jan.2000.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Generalized Sylvester-Type Hadamard Matrices[1]

Jong-Seon No
School of Electrical Engineering,
Seoul National University,
Seoul 151-742, Korea.
e-mail: jsno@snu.ac.kr

Hong-Yeop Song
School of Electrical
and Mechanical Engineering,
Yonsei University,
Seoul 120-749, Korea.
e-mail: hysong@yonsei.ac.kr

Abstract — **In this paper, we generalize Sylvester's construction for (generalized) Hadamard matrices in such a way that m matrices $B_1, B_2, ..., B_m$ (not necessarily distinct) of the same size k and a mtrix C of size m are used as components to construct a (generalized) Hadamard matrix of size mk.**

In this paper, we will prove a construction for generalized Hadamard matrices. This construction is a generalization of Sylvester's construction. Even though it looks obvious, no such generalization has been appeared in a literature as far as both authors are aware of.

Definition 1 *Let G be an abelian group of order g written additively. For a positive integer λ, a generalized Hadamard matrix $GH(g,\lambda)$ is a $g\lambda \times g\lambda$ matrix $[h(i,j)]$, where $1 \le i \le g\lambda$ and $1 \le j \le g\lambda$ denote the row and column indices, respectively, such that, for any $i_1 \neq i_2$, every element of G appears exactly λ times in the list $h(i_1,1) - h(i_2,1)$, $h(i_1,2) - h(i_2,2)$, ..., $h(i_1,g\lambda) - h(i_2,g\lambda)$.*

Remark 2 *A Hadamard matrix of size m is a $GH(2,m/2)$.*

In this paper, we will consider only the generalized hadamard matrices over an abelian group, and abelian groups will be written additively with operation denoted by $+$.

Theorem 3 *We assume that there exists an $m \times m$ generalized Hadamard matrix $C \triangleq [c_{ij}] \triangleq GH(g,\lambda_1)$ over G, where G is an abelian group of order g and $m = g\lambda_1$. We also assume that there exist $B_1, B_2, ..., B_m$ which are (not necessarily distinct) generalized Hadamard matrices $GH(g,\lambda_2)$ over G. Then, the matrix*

$$H = \begin{bmatrix} c_{11}+B_1 & c_{12}+B_2 & \cdots & c_{1m}+B_m \\ c_{21}+B_1 & c_{22}+B_2 & \cdots & c_{2m}+B_m \\ \vdots & \vdots & \vdots & \vdots \\ c_{m1}+B_1 & c_{m2}+B_2 & \cdots & c_{mm}+B_m \end{bmatrix} \quad (1)$$

is a $g^2\lambda_1\lambda_2 \times g^2\lambda_1\lambda_2$ generalized Hadamard matrix $GH(g,g\lambda_1\lambda_2)$ over G, where $c + B_k$ for $c \in G$ is the matrix obtained by adding c to every component of B_k.

Corollary 4 *Using the same notation and assumptions of Theorem 3, the matrix*

$$\begin{bmatrix} c_{11}+B_1 & c_{12}+B_1 & \cdots & c_{1m}+B_1 \\ c_{21}+B_2 & c_{22}+B_2 & \cdots & c_{2m}+B_2 \\ \vdots & \vdots & \vdots & \vdots \\ c_{m1}+B_m & c_{m2}+B_m & \cdots & c_{mm}+B_m \end{bmatrix} \quad (2)$$

is also a $g^2\lambda_1\lambda_2 \times g^2\lambda_1\lambda_2$ generalized Hadamard matrix $GH(g,g\lambda_1\lambda_2)$ over G.

Corollary 5 *If $B_1 = B_2 = \cdots = B_m$ in the construction of Theorem 3, the resulting generalized Hadamard matrix H is of Sylvester type.*

Corollary 6 *If B_k's are the same, except for some column permutations, in the construction of Theorem 3, then the resulting generalized Hadamard matrix H is of Sylvester type up to some column permutation.*

Corollary 7 *Let H be constructed as in Theorem 3 using $B_1, B_2, ..., B_m$ and C. Let H' be constructed as also in Theorem 3 using $B_1', B_2', ..., B_m'$ and the same C. If B_k is the same as B_k' except for some column permutation for $k = 1, 2, ..., m$, then H and H' are the same except for some column permutation.*

[1]This work was supported by the Basic Research Program of the Korea Science and Engineering Foundation (KOSEF) under Grant Number 97-0100-0501-3.

References

[1] S. S. Agaian, *Hadamard Matrices and Their Applications*, Lecture Notes in Mathematics, vol. 1168, Springer-Verlag, New-York, 1980.

[2] T. Beth, D. Jungnickel, and H. Lenz, *Design Theory*, Cambridge University Press, London, 1986.

[3] C. J. Colbourn and W. De Launey "Difference matrices," Chapter IV.11, *CRC handbook of Combinatorial Designs*, edited by C. J. Colbourn and J. H. Dinitz, CRC Press, New York, pp. 287-297, 1996.

[4] R. Craigen, "Hadamard matrices and designs," Chapter IV.24, *CRC handbook of Combinatorial Designs*, edited by C. J. Colbourn and J. H. Dinitz, CRC Press, New York, pp. 370-377, 1996.

[5] W. De Launey, "Generalized Hadamard matrices which are developed modulo a group," *Discrete Mathematics*, vol. 104, pp. 49-65, 1992.

[6] V. Pless and W. C. Huffman, *Handbook of Coding Theory*, Elsevier Science, New York, 1998.

[7] D. V. Sarwate and M. B. Pursley, "Crosscorrelation Properties of Pseudorandom and Related Sequences," *Proceedings of IEEE*, vol. IT-68, pp. 593-619, May 1980.

[8] J. Seberry and M. Yamada, "Hadamard Matrices, Sequences, and Block Design," in book, *Contemporary Design Theory: A Collection of Surveys*, edited by J. H. Dinitz and D. R. Stinson, John Wiley and Sons, pp. 431-560, 1992.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Local LDP for The Shape of Random Young Diagram With Restrictions on Length and Height of Steps

Volodia Blinovsky
Inst. for Information Transmission Problems
Russian Acad. of Sci., Moscow
101447,GSP-4,B.Karetnii per.,19,Russia,
e-mail blinov@postman.ru

Abstract — **We solve the local large deviation problem (LDP) for the shape of random Young diagram when lengths and heights of the steps of the shapes of diagrams take values form given (and in general different for length and height) sets of nonegative integers**

The shape of the Young diagrams Y_n of weight n is the piecewise constant functions with integer lenths and heights of the steps. It the work [1] we establish the local LDP for the shape of random Young diagram with uniform distribution. In the work [2] we consider the case when lengths (or which is equivalent the heights) of the steps take values from given set of positive integers $\mathcal{A} \subset \{0, 1 \ldots\}$.

Here we continue our investigations and consider the case when lengths of the steps take values from the given set $\mathcal{A}$ and heights take value from (in general other) given set $\mathcal{B}$. To solve this problem we use some new considerations and some methods from our previous works.

There exists the natural maping between the Young diagrams of weight n and the nonordered decompositions of n into the sum of natural numbers. We consider the scailing of random Young diagrams of weight n dividing the linear sizes of diagrams by $\sqrt{n}$. Let's κ_n is the shape of the scaled random Young diagram which in turn is the random curve. Define the function $L_1(z)$ and the number L_2 by the following relations Let's $h_2(x)$ satisfies the equality

$$\sum_{i\in\mathcal{A}} e^{-iCx} \sum_{i\in\mathcal{B}} e^{-ih_2} = 1$$

and in turn constant C satisfies the relation

$$\int_0^\infty h_2(x)dx = C.$$

Next we put $L_1 = 2C$ and

$$L_1(z) = zh^1(z) + h^2(z),$$

where h^1, h^2 satisfy the equality

$$\sum_{i\in\mathcal{A}} e^{-ih^1} \sum_{i\in\mathcal{B}} e^{-ih^2} = 1$$

and $h^1(z)$ satisfies the relation

$$z = -\frac{dh^2(h^1)}{dh^1}.$$

We put $L_2 = 2C$.

Next we consider the set of functions $\mathcal{C} \subset L^1([0,\infty))$ such that for every $y \in \mathcal{C}$ there exists $\hat{y} = y$ *a.s.* such that $\hat{y}$ is monotonically nonincreasing and nonegative. Also for every $0 \le x_1 < x_2 < \infty$ the function $\hat{y}$ must satisfy the following relation

$$L_1\left(\frac{\hat{y}(x_1) - \hat{y}(x_2)}{x_2 - x_1}\right) > -\infty. \tag{1}$$

Note, that from the definition of the function $L_1(z)$ and (1) it follows that when $|\mathcal{A}| < \infty$ or $|\mathcal{B}| < \infty$, then $\hat{y}$ is continuous and

$$\min_{i\in\mathcal{A}, j\in\mathcal{B}} \frac{i}{j} \le \hat{y}' \le \max_{i\in\mathcal{A}, j\in\mathcal{B}} \frac{i}{j} \ a.s.$$

The main result of this work contains in the following

Theorem 1 *For the sequence κ_n the following relations are valid*

$$\lim_{\delta\to 0}\lim_{\epsilon\to 0}\lim_{n\to\infty} \frac{\ln P_{n(1\pm\delta)}(\kappa_n \in B(\epsilon, y))}{\sqrt{n}} = -N(y),$$

where

$$N(y) = \begin{cases} L_2 - \int_0^\infty L_1(-\hat{y}'(x))dx, & y \in \mathcal{C}, \\ \infty, & y \notin \mathcal{C} \end{cases}$$

and $B(\epsilon, y) = \{z \in L^1([0,\infty)) : ||z - y|| < \epsilon\}$ is the ball in L^1-space. Notation $P_{n(1\pm\delta)}$ means that we consider Young diagrams with weights in the range $[n(1-\delta), n(1+\delta)]$.

References

[1] V. M. Blinovsky "LDP for Random Young Diagram", Problemy Peredachi Informatsii, vol.35, N1, 1999, pp.61-74

[2] V.M.Blinovsky "Large Deviations For The Shape of A Random Young Diagram With Restrictions", to appear in Discrete Math.

[3] V.M. Blinovsky "General Approach to LDP for Random Young Diagram", in Research Comm. of the Conference in the memory of P.Erdos, Budapest, Hungary, Jul.4–11, 1999, pp. 37-41

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Local and Interweight Spectra of Perfect Binary Codes

Anastasia Yu. Vasil'eva
Sobolev Institute of Mathematics
Koptyug prospect 4,
Novosibirsk, 630090, Russia
e-mail: vasilan@math.nsc.ru

Abstract — **The structure of perfect binary single-error-correcting codes of length $n = 2^t - 1$ is investigated. The concepts of local and interweight spectra of a code are introduced. They are generalizations of the notion of the weight spectrum of a code. Properties of the spectra of perfect codes are studied. The concept of strong distance-invariance of a code is introduced and it is shown that a perfect binary code is strong distance-invariant.**

I. Definitions

A *binary code* C of length n is a subset of the n-cube (that is n-dimensional vector space over $GF(2)$).

Let $\mathbf{x}$ and $\mathbf{y}$ be vertices of the n-cube. We denote the Hamming weight of vertex $\mathbf{x}$ by $wt(\mathbf{x})$ and the Hamming distance between $\mathbf{x}$ and $\mathbf{y}$ by $\rho(\mathbf{x}, \mathbf{y})$.

A code is *distance-invariant* if the number of all codewords at distance $i \in \{0, 1, \ldots, n\}$ from codeword $\mathbf{x}$ does not depend on the choice of the codeword $\mathbf{x}$. A code is called *distance-regular* if for all fixed integers $i, j \in \{0, 1, \ldots, n\}$ the number of codewords $\mathbf{z}$ such that $\rho(\mathbf{x}, \mathbf{z}) = i$, $\rho(\mathbf{y}, \mathbf{z}) = j$ does not depend on the choice of $\mathbf{x}$ and $\mathbf{y}$ but only depends on $\rho(\mathbf{x}, \mathbf{y})$. We call a code *strong distance-invariant* if for every codeword $\mathbf{x}$ and all $i, j, d \in \{0, 1, \ldots, n\}$ the number of codeword pairs $(\mathbf{y}, \mathbf{z})$ such that $\rho(\mathbf{x}, \mathbf{y}) = i$, $\rho(\mathbf{x}, \mathbf{z}) = j$ and $\rho(\mathbf{y}, \mathbf{z}) = d$ does not depend on the choice of $\mathbf{x}$. This property is stronger than distance-invariance and weaker than distance-regularity.

A k-dimensional *face* γ of the n-cube is the set of all vertices of the n-cube with fixed $n - k$ coordinates. A face $\gamma^\perp$ is *orthogonal* across the face γ if the set of face $\gamma^\perp$ fixed positions and the set of face γ free positions coincide. It is clear that the dimension of $\gamma^\perp$ is equal to $n - k$ and the intersection of two orthogonal faces consists of the unique vertex.

Let C be a binary code and $\mathbf{z}$ be a vertex of the face γ. We denote the number of face γ codewords which are at distance i from vertex $\mathbf{z}$ by $v_i^C(\gamma, \mathbf{z})$. We call (see [4]) the vector

$$v^C(\gamma, \mathbf{z}) = \left(v_0^C(\gamma, \mathbf{z}), v_1^C(\gamma, \mathbf{z}), \ldots, v_{dim\,\gamma}^C(\gamma, \mathbf{z})\right)$$

a *local spectrum* of the code C in the face γ with respect to vertex $\mathbf{z}$ (briefly a $(\gamma, \mathbf{z})$-*local spectrum* of the code C).

We denote the number of codeword pairs $(\mathbf{x}, \mathbf{y})$ such that $wt(\mathbf{x}) = i$, $wt(\mathbf{y}) = j$ and the distance between $\mathbf{x}$ and $\mathbf{y}$ is equal to d by $T_d^C(i, j)$. We call the vector

$$T^C(i, j) = \left(T_0^C(i, j), \ldots, T_n^C(i, j)\right)$$

an (i, j)-*weight spectrum* of the code C and the ordered set of (i, j)-weight spectra with $0 \le i, j \le n$ an *interweight spectrum* of the code C.

A *perfect binary single-error-correcting code* C (briefly a *perfect code*) is a subset of the n-cube such that a set of balls of the radius 1 with centers in C is a partition of the n-cube.

II. Results

The local spectra of a perfect code in two orthogonal faces with respect to their common vertex were proved to be in the tight interdependence (see [4]).

Theorem 1: Let γ be a k-dimensional face of the n-cube and $\mathbf{z}$ be the common vertex of γ and $\gamma^\perp$. The $(\gamma^\perp, \mathbf{z})$-local spectrum of a perfect code C is uniquely determined by the $(\gamma, \mathbf{z})$-local spectrum of the code and the generating function of the consequence $v^C(\gamma^\perp, \mathbf{z})$ is

$$\frac{1}{n+1}(1+t)^{n-k} + (1-t)^{\frac{n+1}{2}-k}(1+t)^{\frac{n-1}{2}-k} \times \sum_{q=0}^{k}(-1)^q \left(v_q^C(\gamma, \mathbf{z}) - \frac{1}{n+1}\binom{k}{q}\right) t^q$$

Establishing the relations between interweight and local spectra of a perfect code and using Theorem 1 one can prove the following

Theorem 2: The interweight spectrum of a perfect code is uniquely determined by the fact whether the code contains all-zero vertex or not.

S.P. Lloyd [2], H.S. Shapiro and D.L. Slotnik [3] proved a perfect binary code to be distance-invariant. S.V. Avgustinovich and F.I. Solov'eva [1] proved that among the perfect codes only Hamming codes of length 3 and 7 are distance-regular. ¿From Theorem 2 we have

Theorem 3: A perfect code is strong distance-invariant.

The question on strong distance-invariance of other types of codes is open.

Acknowledgments

The author is grateful to S. V. Avgustinovich for formulating the problem and useful discussions.

References

[1] S. V. Avgustinovich, F. I. Solov'eva, "On distance regularity of perfect binary codes," *Problems of Information Transmission*, vol. 34, no. 3, pp. 247-249, 1998.

[2] S. P. Lloyd, "Binary block coding," *Bell Syst. Tech. J.*, vol. 36, no. 2, pp. 517-535, 1957.

[3] H. S. Shapiro, D. L. Slotnick, "On the mathematical theory of error correcting codes," *IBM J. Res. Develop.*, vol. 3, no. 1, pp. 25-34, 1959.

[4] A. Yu. Vasil'eva, "Local spectra of perfect binary codes," *Discrete analysis and operation research*, vol. 6, no. 1, pp. 16-25, 1999. (in Russian)

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Some Results on Symbol Error-Correcting Codes

C. L. Chen
IBM Corporation
MS P361, 2455 South Road
Poughkeepsie, NY 12601 U.S.A.
E-mail: clchen@us.ibm.com

Abstract - Efficient symbol error-correcting codes of distances 4 and 5 are presented.

I. Introduction

Error-correcting codes have been routinely applied to modern computer memory subsystems. As the capacity of memory chips increases, the applications of error-correcting codes have been gradually shifted from the bit-oriented codes to the symbol-oriented codes.

Symbol error-correcting codes of distances 4 and 5 have been investigated by many researchers [1-5]. In particular, Dumer has constructed several families of codes [3]. Feng, et. al., have improved Dumer's results in the construction of codes of distance 5 [4]. For a symbol of size b, let $q = 2^b$. Feng's codes have the parameters of code length $n = q^m$ and number of check symbols $r = \lceil 7m/3 \rceil + 1$, for odd m.

We present a family of distance 4 codes that are more efficient than those in [1-3]. In the case of distance 5 codes, we construct a family of codes with the same parameters as [4] for even m, thus enlarging the number of available codes for applications.

II. Results

We employ the technique illustrated in [5] for the construction of symbol error-correcting codes. These codes obtained are called subspace subcodes in [6]. The basic idea is to start with a linear code, not necessarily a Reed-Solomon code, with symbols over a finite field. A new code with a smaller symbol size is then obtained by consistently deleting a fixed set of bits from the symbols of the original code.

For distance 4, we start with a code $\mathbf{C_0}$ with symbols over $GF(2^m)$ and parameters $n = 2^{2m} + 1$, and $r = 4$. The first row of the parity-check matrix consists of either the field elements zero or one. We then construct a code $\mathbf{C}(b,c)$ with symbol size of b bits. Let $\mathbf{W} = (w_1, w_2, ..., w_n)$ be a code word of $\mathbf{C}(b,c)$, and let v_i be a binary vector obtained from w_i by attaching c zeros, c=m-b. Then $\mathbf{W}$ is a code word of $\mathbf{C}(b,c)$ if and only if $V = (v_1, v_2, ..., v_n)$ is a code word of $\mathbf{C_0}$. Code $\mathbf{C}(b,c)$ is of length $n = 2^{2(b+c)} + 1$ with the number of check bits $rb = 4b + 3c$. The number of check symbols r is $4 + 3c/b$. Let $q = 2^b$. Then $n = 2^{2c}q^2 + 1$. We have $r = 1 + 1.5 \log_q(n-1)$. The number of check bits is fewer than a distance 4 code in [4] for the same value of n.

A comparison of $\mathbf{C}(b,c)$ with other known codes can be made when r is an integer. Consider $b = 3c$. We have $r = 5$, $n = q^{8/3} + 1$. This is better than the codes in [2], which have $r = 5$ and $n = 2q^2 + 2q + 1$ for $q > 4$, in that the code length is longer. Consider next $b = 1.5c$. We have $r = 6$ and $n = q^{10/3} + 1$. This is also better than the codes in [1], which have $r = 6$ and $n = (q + 2)(q^2 + 1)$.

For distance 5, we apply the same technique to a code of [4] with $n = q^m$ and $r = \lceil 7m/3 \rceil + 1$ to yield a new code with $n = 2^{mc}q^m$ and $r = \lceil (7m + 3)/3 \rceil + \lceil 7m/3 \rceil c/b$. Let $t = c/b$. The new code has $n = q^{(t+1)m}$ and $r = (t+1)\lceil 7m/3 \rceil + 1$. In particular, let $t = 1$, then $n = q^{2m}$ and $r = 2\lceil 7m/3 \rceil + 1$. We have a family of distance 5 codes with n = an even power of q.

References

[1] C. L. Chen, "Error-correcting codes for byte-organized memory systems," *IEEE Transactions on Information Theory*, vol. 32, pp. 181-185, March 1986.

[2] Y. Edel and J. Bierbrauer, "A family of caps in projective 4-space in characteristic 2," dated July 22, 1997, private communication with J. Bierbrauer.

[3] I. Dumer, "Nonbinary double-error-correcting codes designed by means of algebraic varieties," *IEEE Transactions on Information Theory*, vol. 41, pp. 1657-1666, November 1995.

[4] G. L. Feng, X. W. Wu and T. R. N. Rao, "Correction to new double-byte error-correcting codes for memory systems," *IEEE Transactions on Information Theory*, vol. 45, p. 2209, September 1999.

[5] C. L. Chen, "Symbol error-correcting codes for computer memory systems," *IEEE Transactions on Computers*, vol. 41, pp.252-256, February 1992; also presented at the *IEEE International Symposium on Information Theory*, Kobe, Japan, June 1988.

[6] M. Hattori, R. J. McEliece and G. Solomon, "Subspace subcodes of Reed-Solomon codes," *IEEE Transactions on Information Theory*, vol. 44, pp. 1861-1880, September 1998.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

A New Scheme for Building Good Self-Dual Block Codes

J.C.Carlach
France Telecom R&D
DMR/DDH,CCETT-Rennes
4, rue du Clos Courtel
35512 Cesson-Sévigné, France

A.Otmani and C.Vervoux
Université de Limoges
LACO Laboratoire d'Arithmétique,
Calcul Formel et Optimisation
87060 Limoges, France

Abstract — **We present a very simple multi-stage encoding scheme of self-dual codes using a [8, 4, 4] extended Hamming code as short base code and bit permutations (or interleavers as in Turbo-Codes[1]) between stages. We describe several examples of interleavers in order to build some extremal codes, with a minimum number of stages, such as the [24, 12, 8] Golay code, [32, 16, 8], [64, 32, 12], and [88, 44, 16] codes. For length 32, we show how to build the 5 non-equivalent extremal QR, RM, F, G, U [32, 16, 8] self-dual codes. We conjecture that this encoding scheme may find good rate-1/2 long block codes[3].**

An example of a [24, 12, 8] Golay code encoder built with a [8, 4, 4] extended Hamming self-dual base code is shown below in figure 1:

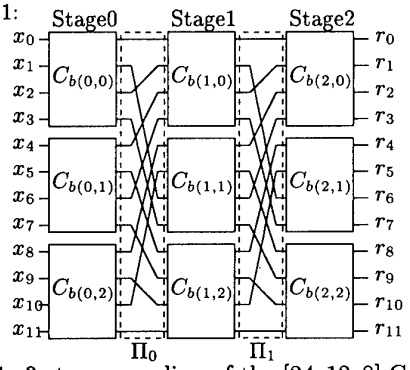


Figure 1: 3-stage encoding of the [24, 12, 8] Golay code.

The two identical permutations Π_0 and Π_1 map the ordered integers set $(0, 1, 2, \ldots, 11)$ into $(0, 2, 4, 6, 8, 10, 1, 3, 5, 7, 9, 11)$. The even (resp. odd) bits are permuted to the upper (resp. lower) bits. In general, the permutations are not identical and not unique for a given code. The first stage 0 transforms the input information bits vector $\mathbf{X} = (x_0, x_1, \ldots, x_{k-1}) = \mathbf{X}^{(0)} = (x_0^{(0)}, x_1^{(0)}, \ldots, x_{k-1}^{(0)})$ into "redundancy" bits vector $\mathbf{R}^{(0)} = (r_0^{(0)}, r_1^{(0)}, \ldots, r_{k-1}^{(0)})$, then the bits of $\mathbf{R}^{(0)}$ are permuted or interleaved by permutation Π_0 to provide the input vector $\mathbf{X}^{(1)}$ of stage 1, and so on until the last stage $(s-1)$ which outputs $\mathbf{R}^{(s-1)}$. The codeword $\mathbf{C}$ is the concatenation of the input information bits vector and the output redundancy vector of the last stage: $\mathbf{C} = (\mathbf{X}^{(0)}, \mathbf{R}^{(s-1)})$. Table 1 summarizes the codes built with permutations defined by the affine application $\tau_{a,b}(z) = a * z + b \ \ (mod.\ k)$ with $a, b \in \boldsymbol{Z}$. Conway and Pless[2] have shown that it exists only 5 non-equivalent extremal type-II self-dual codes of length $n = 32$: the QR[32, 16, 8] and $RM(2, 5)$ codes, and the codes called F, G, and U. We have only found the QR, G and U codes (Cf. Table 2) with identical (at all stages) permutations associated to the linear applications in the multiplicative group **GF(16)** defined by $z \rightarrow \alpha^a z + \alpha^b z^2 + \alpha^c z^4 + \alpha^d z^8$, with $a, b, c, d \in 0, 1, \ldots, 14$ where α is a primitive generator of **GF(16)**. But, we have built, with a minimum of 3 stages, these five [32, 16, 8] codes with couples of non-identical permutations given in Table 3.

Code$[n, k, d_{min}]$	a, b	*Stages*
[16, 8, 4]	1, 0	3
Golay[24, 12, 8]	5, 1	3
G[32, 16, 8]	3, 0	3
[40, 20, 8]	3, 0	3
[56, 28, 12]	5, 1	3
[64, 32, 12]	19, 0	3
[72, 36, 12]	5, 0	3
[88, 44, 16]	35, 0	7

Table 1: Codes obtained with $z \rightarrow a*z+b$ permutations.

Code[32, 16, 8]	*Permutation*	*Stages*
QR[32, 16, 8]	$\alpha^7 z^2 + z^4 + \alpha z^8$	3
G[32, 16, 8]	$\alpha^7 z^8$	3
U[32, 16, 8]	$\alpha^7 z^2 + z^4 + \alpha z^8$	7

Table 2: Length 32 extremal codes built with permutaions associated to linear applications over $GF(16)$.

Code	*Permutations*
QR	$\Pi_0 = 0, 4, 8, 12, 1, 5, 9, 13, 2, 6, 10, 14, 3, 7, 11, 15$ $\Pi_1 = 0, 13, 6, 7, 4, 1, 10, 15, 8, 5, 14, 3, 12, 9, 2, 11$
RM	$\Pi_0 = 0, 4, 8, 12, 1, 2, 9, 13, 3, 5, 6, 14, 7, 10, 11, 15$ $\Pi_1 = 0, 5, 14, 3, 4, 13, 10, 7, 8, 9, 2, 15, 12, 1, 6, 11$
F	$\Pi_0 = 0, 4, 5, 8, 1, 2, 6, 12, 3, 7, 9, 13, 10, 11, 14, 15$ $\Pi_1 = 0, 1, 10, 11, 4, 13, 6, 15, 8, 9, 2, 7, 12, 5, 14, 3$
G	$\Pi_0 = 0, 4, 8, 12, 1, 5, 9, 13, 2, 6, 10, 14, 3, 7, 11, 15$ $\Pi_1 = 0, 13, 6, 11, 4, 1, 10, 15, 8, 5, 14, 3, 12, 9, 2, 7$
U	$\Pi_0 = 0, 4, 8, 12, 1, 5, 9, 13, 2, 6, 10, 14, 3, 7, 11, 15$ $\Pi_1 = 0, 13, 6, 3, 4, 1, 10, 11, 8, 5, 14, 7, 12, 9, 2, 15$

Table 3: Permutations of the 5 extremal [32, 16, 8] codes.

Acknowledgments

The authors gratefully acknowledge Pascale Charpin and Anne Canteaut of the "Projet CODES" at INRIA-Rocquencourt, Thierry Berger and Philippe Gaborit of the LACO Laboratory of the Mathematics Department of Limoges University, for their help during this work. The authors would like also to thank France Telecom R&D, INRIA, and UMS-medicis for their support.

References

[1] **C.Berrou, A.Glavieux and P.Thitimajshima**: *Near Shannon Limit Error-Correcting Coding and Decoding : Turbo-Codes.* Proc. of ICC'93, Geneva, May 1993, pp.1064-1070.

[2] **J.H.Conway and V.S.Pless**: *On the Enumeration of Self-Dual Codes*, Journal of Comb. Th., Serie A28, pp.26-53, 1980.

[3] **J.C.Carlach and C.Vervoux**: *A New Family of Block Turbo-Codes*, Proc. of AAECC-13 Symposium, Honolulu, Hawaii, USA, pp.15-16, November 14-19, 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Watermark Codes: Reliable communication over Insertion/Deletion channels.

Matthew C. Davey and David J. C. MacKay
Cavendish Laboratory, Cambridge, CB3 0HE, UK.
Email: mcdavey@mrao.cam.ac.uk, mackay@mrao.cam.ac.uk

Abstract — **A new block code is introduced which is capable of correcting multiple insertion, deletion and substitution errors present in a single block. An inner code resilient to synchronisation errors provides soft inputs to an outer code capable of correcting substitution errors. The decoder does not require knowledge of the block boundaries.**

Many coding methods have been proposed to cope with synchronisation errors. Most fall into one of two categories, either correcting limited synchronisation errors [1, 2] or imposing run-length limiting constraints [3]. In this paper we present a block code capable of correcting multiple synchronisation and substitution errors using a probabilistic decoder. We apply the code to a model binary channel with an input queue. At each use, one of three events occurs. With probability P_i a random bit is inserted into the received stream. With probability P_d the next queued bit is deleted. With probability $P_t = (1 - P_d - P_i)$ the next queued bit is transmitted, with a probability P_s of suffering a substitution error.

The construction of Watermark codes is outlined in figure 1. We first encode our message $\mathbf{m}$ into a vector $\mathbf{d}$ of length N using a standard outer error-correcting code. We use low-density parity-check codes defined over the field $GF(q = 2^k)$ because they can easily utilise the soft information provided by the inner code. Low-density parity-check codes [4] are currently the best known error correcting codes for Gaussian channels [5, 7].

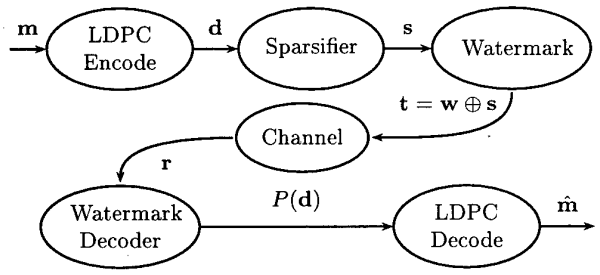


Fig. 1: Watermark codes

For the inner code, we choose a fixed binary vector $\mathbf{w}$ of length $n \times N$, for some $n > k$, which we call the *watermark*. The watermark is known to both encoder and decoder. Suitable choices for $\mathbf{w}$ include pseudo-random and run-length limited sequences. The encoder maps outer codewords $\mathbf{d}$ to sparse messages $\mathbf{s}$ of length $|\mathbf{w}|$ by mapping each q-ary symbol of $\mathbf{d}$ to one of the q sparsest patterns of length n.

Next we form the transmitted vector $\mathbf{t} := \mathbf{w} + \mathbf{s} \bmod 2$. If the message vectors $\mathbf{s}$ are constrained to be sufficiently sparse, and synchronisation errors are sufficiently rare, it is possible for a Hidden Markov Model decoder to recover synchronisation with a small probability of error.

The inner decoder takes the noisy received vector $\mathbf{r}$ and returns an *a posteriori* distribution for each q-ary symbol of $\mathbf{d}$. It should be noted that the decoder does not know the position of the block boundaries. The outer decoder takes the output of the Watermark decoder and attempts to recover the codeword $\mathbf{d}$ and corresponding message $\mathbf{m}$.

Watermark codes can communicate very effectively over insertion/deletion channels. Figure 2 shows rate 1/2, blocklength 4600, watermark codes reaching a block error rate of 10^{-3} with roughly 100 synchronisation errors scattered throughout each block. This compares favourably to previous reports [2] of rate 1/2 blocklength 15840 codes achieving similar block error rate for a channel that made insertion/deletion bursts of expected length 6 on average once every 9 blocks.

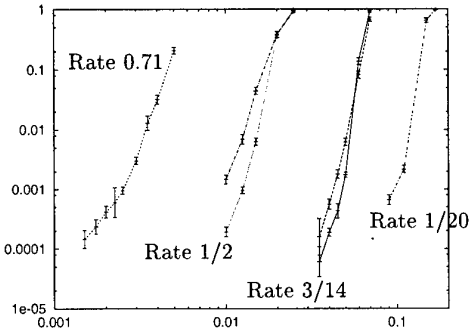


Fig. 2: Performance of concatenated watermark codes with overall rate between 0.7 and 0.05 and blocklengths roughly 5000 bits. Outer codes were regular low-density parity-check codes with mean column weights between 2.6 and 3. The channel substitution probability P_s was zero. Vertical axis: block error rate. Horizontal axis: insertion/deletion probability. Figure reproduced from [6].

References

[1] V. I. Levenshtein, "Binary codes capable of correcting deletions, insertions, and reversals", *Soviet Physics - Doklady*, vol. 10, no. 8, pp. 707–710, February 1966.

[2] P. A. H. Bours, *Codes for Correcting Insertion and Deletion Errors*, PhD thesis, Eindhoven Technical University, June 1994.

[3] B. H. Marcus, P. H. Siegel, and J. K. Wolf, "Finite-state modulation codes for data storage", *IEEE Journal on Selected Areas in Communication*, vol. 10, no. 1, pp. 5–38, January 1992.

[4] R. G. Gallager, *Low Density Parity Check Codes*, Number 21 in Research monograph series. MIT Press, 1963.

[5] M. C. Davey and D. J. C. MacKay, "Low density parity check codes over GF(q)", in *Proceedings of the 1998 IEEE Information Theory Workshop*. IEEE, June 1998, pp. 70–71.

[6] M. C. Davey and D. J. C. MacKay, "Reliable Communication over Channels with Insertions, Deletions and Substitutions.", Submitted to IEEE Trans. Info. Theory, 1999.

[7] T. Richardson and R. Urbanke, "The capacity of low-density parity check codes under message-passing decoding", Submitted to IEEE Trans. Info. Theory, 1998.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Fast Computation of Roots of Polynomials over Function Fields and Fast List Decoding of Algebraic Geometric Codes[1]

Xin-Wen Wu
ECE, 0407
University of California, San Diego
La Jolla, CA 92093-0407, USA
e-mail: wxw@cwc.ucsd.edu

Paul H. Siegel
ECE, 0407
University of California, San Diego
La Jolla, CA 92093-0407, USA
e-mail: psiegel@ucsd.edu

Abstract — **We present a fast algorithm for finding the roots of polynomials over function fields that can be used to speed up the list decoding of algebraic geometric codes.**

I. Introduction

Suppose C is a $[n,k,d]$ code over a finite field $\mathbf{F}_q$, and let $t < n$ be a positive integer. For any received vector $\mathbf{y} = (y_1, \cdots, y_n) \in \mathbf{F}_q^n$, we refer to any code word $\mathbf{c}$ in C satisfying $d(\mathbf{c}, \mathbf{y}) \leq t$ as a *t-consistent code word.* Let $\tau = \lfloor \frac{d-1}{2} \rfloor$. It is clear that in any Hamming sphere in $\mathbf{F}_q^n$ of radius $\leq \tau$, there exists at most one code word of C. On the other hand, if $t > \tau$ then there may exist several distinct t-consistent code words. We call τ the *error correction bound* of the code. The *classical decodings* only consider the decoding algorithms which can correct τ or fewer errors. A *list decoding* is a decoding algorithm which tries to construct a list of all t-consistent code words, where t can be greater than τ. Thus, a list decoding algorithm makes it possible to recover the information from errors beyond the traditional error correction bound.

In this paper, motivated by Roth and Ruckenstein's work [2], we propose an efficient algorithm for finding the roots of polynomials over function fields. This algorithm can be used to speed up the list decoding of algebraic geometric codes.

II. List Decoding for AG Codes

Recently, Shokrollahi and Wasserman [3] proposed a list decoding algorithm for low-rate algebraic geometric codes, generalizing the results of Sudan [4] for Reed-Solomon codes. Guruswami and Sudan [1] then proposed an improved list decoding algorithm applicable to high rate algebraic geometric codes and Reed-Solomon codes, as well. The list decoding algorithm consists of two main steps. The first step is to find a nonzero univariate polynomial $H(T)$ over the function field $\mathcal{K}$ of the curve. This step can be reduced to the solution of a system of homogeneous linear equations, which can be implemented with low complexity using Gaussian elimination. The second step is to find the roots of the polynomial $H(T)$ in a rational function space $L(G)$. Shokrollahi and Wasserman [3] and Guruswami and Sudan [1] proposed factorization (or root-finding) algorithms to find the roots of $H(T)$. However, the implementation of these algorithms is rather complicated.

In [2], Roth and Ruckenstein presented an efficient list decoding algorithm for low-rate Reed-Solomon codes, based upon [4]. They reduced the complexity of the second step, the codeword reconstruction, by means of an efficient algorithm for finding roots of univariate polynomials over polynomial rings.

[1]This work was supported in part by Grant No. NCR-9612802 from the NSF and by a research grant from the National Storage Industry Consortium.

III. Fast Algorithm

We have extended the efficient root-finder in Roth and Ruckenstein's reconstruction algorithm to the class of univariate polynomials over the function field of any curve in m-dimensional projective space. Using this extension, we obtain an efficient list decoding algorithm for algebraic geometric codes.

Let $H(X;T) = h_0(X) + h_1(X)T + \cdots + h_s(X)T^s$, where $h_j(X) \in L((l - j\rho)P)$. Suppose $f(X) \in L(G) = L(\rho P)$ such that $H(X; f(X)) = 0$. Let $\{\varphi_1, \varphi_2, \cdots, \varphi_k\}$ be a basis of $L(\rho P)$, such that φ_i has a pole only at P and the order of the pole is ρ_i, i.e., $\mathrm{ord}_P(\varphi_i) = -\rho_i$, where ρ_i is the i-th nongap at P. We can assume $f(X) = f_1\varphi_1(X) + f_2\varphi_2(X) + \cdots + f_k\varphi_k(X)$, where $f_i \in \mathbf{F}_q$. We now can find f_k, f_{k-1}, $\cdots$, f_1, by the following procedure.

Set $G_1(X;T) = H_1(X;T) = H(X;T)$ and $\widehat{G}_1(X;T) = G_1(X;\varphi_k T)$. Then, $\widehat{G}_1(X;T) = \sum_{j=0}^{s}(h_j\varphi_k^j)T^j$. Let $-\rho_{r_1} = \min\{\mathrm{ord}_P(h_j\varphi_k^j) \mid j = 0, 1, \cdots, s\}$. Suppose φ_{r_1} is a rational function with $\mathrm{ord}_P(\varphi_{r_1}) = -\rho_{r_1}$. Divide $\widehat{G}_1(X;T)$ by φ_{r_1}, and let $\widetilde{G}_1(X;T) = \widehat{G}_1(X;T)/\varphi_{r_1}$. Then, $\widetilde{G}_1(P;T)$ is a nonzero polynimial in $\mathbf{F}_q[T]$.

On the other hand, by $H(X; f(X)) = 0$, we have

$$\widetilde{G}_1(X; \frac{f(X)}{\varphi_k(X)}) = 0. \tag{1}$$

Since $\mathrm{ord}_P\left(\frac{\varphi_j}{\varphi_k}\right) = \rho_k - \rho_j > 0$, for $j = 1, \cdots, k-1$, we have $\frac{f}{\varphi_k}(P) = f_k$. By (1), we have $\widetilde{G}_1(P; f_k) = 0$. So by solving $\widetilde{G}_1(P;T) = 0$, we can get f_k.

This derivation can be applied inductively to determine the remaining coefficients $f_{k-1}, \ldots, f_1$ of a root $f(X)$ of $H(T) = 0$.

Theorem: *Let $H(T)$ be a nonzero polynomial of degree s in $\mathcal{K}[T]$ that is returned in the first step of the list decoding algorithm. Then the roots of $H(T)$ in $L(G) = L(\rho P)$ can be determined by the root-finding procedure described above. This root-finding procedure requires $O(ks(n^2 + s^2 + \log^2 s \cdot \mathrm{loglog} s \cdot \log q))$ operations over $\mathbf{F}_q$ and $O(ks^2)$ operations over $\mathcal{K}$.*

References

[1] V. Guruswami, M. Sudan, "Improved decoding of Reed-Solomon and algebraic-geometry codes," *IEEE Trans. Inform. Theory*, vol. 45, no. 6, pp. 1757–1767, Sept. 1999.

[2] R. Roth and G. Ruckenstein, "Efficient decoding of Reed-Solomon codes beyond half the minimum distance," *IEEE Trans. Inform. Theory*, vol. 46, no. 1, pp. 246–257, Jan. 2000.

[3] M. Shokrollahi, H. Wasserman, "List decoding of algebraic-geometric codes," *IEEE Trans. Inform. Theory*, vol. 45, no. 2, pp. 432–437, March 1999.

[4] M. Sudan, "Decoding of Reed-Solomon codes beyond the error-correction bound," *Journal of Complexity*, 13, pp. 180-193, 1997.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

A fast interpolation method for list decoding of RS and algebraic-geometric codes

Shojiro Sakata,
Yukio Numakami,
Masaya Fujisawa
Dept. of Inform. & Commun. Eng.
Univ. of Elect.-Comm.
Chofu-shi, Tokyo 182-8585, JAPAN
e-mail: sakata@ice.uec.ac.jp

I. Introduction

Recently Sudan [1] presented a decoding method of RS codes beyond the error-correction bound t, i.e. the half of the minimum distance. This is a list decoding which gives as its output a list of all codewords within a specified distance t' from the received word, where $t' > t$. On one hand this method can be generalized to a list decoding of one-point algebraic-geometric (AG) codes [2], and on the other hand their improved versions for larger rate have been given [3]. Sudan algorithm is composed of two major stages. At the first stage, in case of RS codes, one must find a bivariate polynomial $f(x, y)$ having a prescribed set of zeros and a minimal (multi-)degree with respect to a certain admissible total order over the set of integer vectors Z_0^2 so that its factors of form $y - g(x)$ give the codewords in the required list at the second and last stage of factorization of $f(x, y)$. Though the factorization problem has more complexity in Sudan algorithm, the interpolation problem is significant by its own nature and important as well.

In a general interpolation problem in the bivariate polynomial ring $K[x, y]$ over a finite field K, one is required to find a set of polynomials $f(x, y)$ subject to the condition: $f(\alpha_i, \beta_i) = \gamma_i$, $1 \le i \le n$, for a given set $\{(\alpha_i, \beta_i, \gamma_i) | 1 \le i \le n\} \subset K^3$ along with some additional constraints or prerequisites. Since this problem is equivalent to a nonhomogeneous system of linear equations for unknown coefficients of polynomials $f(x, y)$, its generic solution is given as a sum of a single or special solution of the nonhomogeneous system and the generic solution of the homogeneous system corresponding to the condition: $f(\alpha_i, \beta_i) = 0$, $1 \le i \le n$. Thus, the latter type of interpolation problem, where one is required to find polynomials with preassigned zeros, is substantial. Furthermore, the generic solution of this homogeneous system has a mathematically clear meaning as follows:

For a finite subset $V := \{(\alpha_i, \beta_i) | 1 \le i \le n\} \subset K^2$, the set of polynomials $I(V) := \{f(x, y) \in K[x, y] | f(\alpha_i, \beta_i) = 0, 1 \le i \le n\}$ is an ideal of the ring $K[x, y]$ and any element of $I(V)$ having a minimal degree can be obtained among a Gröbner basis of the ideal $I(V)$ with respect to the specific total order. Though some other efficient algorithms to solve this interpolation problem have been given [4][5], they miss the above crucial observation so that each of them is of its own special and separate form.

In this paper, we present an efficient algorithm to find a Gröbner basis of the ideal $I(V)$ based on Berlekamp-Massey-Sakata (BMS) algorithm [6][7], which gives another efficient method of giving the solution at the first stage of Sudan algorithm. Furthermore, we show that the above interpolation problem can be generalized to find a Gröbner basis of the ideal $I(V; M)$ which consists of polynomials having zeros $(\alpha_i, \beta_i) \in V$ with some multiplicity condition specified by a set M $(\in Z_0^2)$ of integer vectors. This Hermitian type of interpolation problem takes a role in the improved version of Sudan algorithm [3]. A modification [8] of BMS algorithm can be applied to solve this problem. On the other hand, for list decoding of one-point AG codes our method can be adapted to find a Gröbner basis of a relevant ideal.

II. Conclusion

BMS algorithm can be applied efficiently not only for the conventional bounded-distance decoding of one-point AG codes up to the Feng-Rao designed distance but also for list decoding of RS codes and one-point AG codes. As a result of a simple analysis of computational complexity in the improved version of Sudan list decoding of RS codes for the number t' of correctable errors, where $t' \sim n - \sqrt{hkn}$ for a constant $h > 1$, we have the following estimate. Based on our method, the first interpolation stage has complexity $\mathcal{O}(k^{-\frac{1}{2}} n^{\frac{5}{2}} m^5)$ (in comparison with $\mathcal{O}(n^3 m^6)$ based on Gaussian elimination), where m is the required multiplicity of zeros in the improved Sudan algorithm.

References

[1] M. Sudan, "Decoding of RS codes beyond the error-correction bound", *J. Complexity*, vol.13, pp.180–193,1997.

[2] M.A. Shokrollahi, H. Wassermann, "List decoding of algebraic-geometric codes", *IEEE Trans. Inform. Theory*, vol.45, pp.432–437, 1999.

[3] V. Guruswami and M. Sudan, "Improved decoding of RS codes and algebraic-geometric codes", *IEEE Trans. Inform. Theory*, vol.45, pp.1757–1767, 1999.

[4] G.L. Feng, "A generalization of the Welch-Berlekamp algorithm for weighted curve fitting with application to the Sudan decoding procedure", preprint, 1998.

[5] R. Roth, G. Ruckenstein, "Efficient decoding of RS codes beyond half the minimum distance", Proc. of 1998 IEEE Intern. Symp. Inform. Theory, p.56, 1998.

[6] S. Sakata, "Finding a minimal set of linear recurring relations capable of generating a given finite two-dimensional array", *J. Symbol. Comp.*, vol.5, pp.321–337, 1988.

[7] S. Sakata, "Extension of the Berlekamp-Massey algorithm to N dimensions", *Inform. & Comp.*, vol.84, pp.207–239, 1990.

[8] S. Sakata, "N-dimensional Berlekamp-Massey algorithm for multiple arrays and construction of multivariate polynomials with preassigned zeros," in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes: Proc. AAECC-6 (Ed. T. Mora)*, Springer Verlag: Berlin, pp.356–376, 1989.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Bounds on List Decoding of MDS Codes

Jørn Justesen
Department of Telecommunication
Technical University of Denmark,
Bldg. 371
DK-2800 Lyngby, Denmark
e-mail: jju@tele.dtu.dk

Tom Høholdt
Department of Mathematics
Technical University of Denmark,
Bldg.303
DK-2800 Lyngby, Denmark
e-mail: T.Hoeholdt@mat.dtu.dk

Abstract — **We derive upper bounds on the number of errors that can be corrected by list decoding of MDS codes using small lists. We show that the performance of Reed-Solomon codes, for certain parameter values, is limited by worst-case codeword configurations, but that with randomly chosen codes over large alphabets, more errors can be corrected.**

I. Introduction

In most cases, error patterns with slightly more than $\frac{D}{2}$ errors can be corrected by an (N, K) maximum distance separable (MDS) code. However, until the publication of Sudan's algorithm [1], the complexity of the computation increased quickly with the number of additional errors, and in practice only a single additional error could be corrected with an acceptable amount of computation. Sudan's paper not only gives an algorithm which allows more errors to be corrected, it also gives a proof that for a limited number of errors, the correct codeword is always on a very small list of possible transmitted words. In [2] the algorithm was extended to all rates and they obtained a bound for list of j decoding consisting of a sequence of straight lines meeting at the points $(r,t) = (s(s-1)/j(j+1), 1-s/(j+1)), s = 1, 2, \ldots, j+1$ where r is the rate of the code and t is the fractional number of errors that can be corrected. For large j, the fractional number of errors approaches $1-\sqrt{r}$.

The aim of this paper is to study codeword configurations in order to derive bounds on the number of errors that can be corrected with any list decoding algorithm when the size of the list is some fixed number. The bounds coincide with Sudan's bounds indicating that the limitation is not related to any particular decoding algorithm.

II. A general observation

Suppose we have $j+1$ codewords

$$u_i = (u_{i1}, u_{i2} \ldots, u_{iN}) \ , \ i = 1, 2, \ldots, j+1$$

at mutual distance D with the property that in any coordinate the $j+1$ words have the same symbol in s words and different symbols in the remaining $j+1-s$ words.

From such a configuration we can get a balanced incomplete block design by taking the $j+1$ codewords as points and let the N blocks be the codewords that have the same symbol in the first, the second,..., the N th. coordinate.

The parameters of the design are $v = j+1$, $k = s$, $\lambda = N - D$, and $b = N$.

Necessary conditions for the existence of such a design are

$$(s-1) \mid (N-D)j \quad (1)$$

$$s(s-1) \mid (N-D)j(j+1) \quad (2)$$

$$(N-D)j(j+1) = Ns(s-1) \quad (3)$$

If such a configuration of codewords exists and we let w be the word that has the shared symbol as its j th coordinate, the distance between w and all the codewords is $T = N - \frac{Ns}{j+1}$ and the code has rate $\frac{N-D+1}{N} = \frac{s(s-1)}{j(j+1)} + \frac{1}{N}$ and $t = \frac{T}{N} = 1 - \frac{s}{j+1}$. If we let $\lambda = \frac{ls(s-1)}{2}$ and $N = \frac{lj(j+1)}{2}$ the existence of such a block design (for sufficiently large l) follows from a theorem of Wilson [3]. In the special case where $l = 1$ and $j+1$ is relatively prime to $2, 3, \ldots, s-1$ there is a nice direct construction [4].

This gives the following theorem

Theorem 1 *Let j and s be natural numbers $s < j+1$. Then there exists a natural number m such that for $l \geq m$ the Hamming space $\mathbb{F}_q^N$ where $N = \frac{lj(j+1)}{2}$ contains $j+1$ vectors of mutual distance $D = N - \frac{ls(s-1)}{2}$ in a sphere of radius $N - \frac{Ns}{j+1}$.*

Remark 1 *One can prove that if $N = \frac{lj(j+1)}{2}$, then the smallest radius of a sphere containing $j+1$ words of mutual distance at least $N - \frac{ls(s-1)}{2}$ is $N - \frac{Ns}{j+1}$.*

It turns out that using classical designs from points and hyperplanes of $PG(m,q)$ one can actually get the corresponding R-S codewords. This leads to the following:

Theorem 2 *Suppose $j+1 = \frac{q^m-1}{q-1}$, where q is a prime power an m is a natural number. Then there exist Reed-Solomon codes of rates $\frac{q^{m-2}+q-2}{q^m-1}$ and $\frac{q^{m-2}(q-1)^2}{q^m-1}$ such that we can only be sure to have the correct codeword on a list of size j if the fractional number of errors t satisfy $t < 1 - \frac{q^{m-1}-1}{q^m-1}$ and $t < 1 - \frac{q^{m-1}(q-1)}{q^m-1}$ respectively.*

This gives $t < 1 - \sqrt{r}$ for large j.

III. An upper bound for randomly chosen codes

We have also studied list decoding of randomly chosen codes and could prove the following

Theorem 3 *There exists $(q-1, k)$ codes over $\mathbb{F}_q$ such that list of j decoding is possible for any $t < (1-r)j/(j+1)$.*

In a particular case we have that if m is at least 10 , there are codes over $\mathbb{F}_{2^m}$ of rate $1/2$ that allow more than $N/4$ errors to be corrected with list of 2 decoding.

References

[1] M.Sudan Decoding of Reed-Solomon codes beyond the error-correction bound. *J.Compl.*, 13 pp.180-193, 1997

[2] V.Guruswami and M.Sudan Improved decoding of Reed-Solomon and algebraic-geometric codes. *IEEE-Trans.Inform.Theory* vol.45 no.6 pp. 1757-1767 Sep. 1999

[3] Th.Beth,D.Jungnickel,H.Lenz *Design Theory* p.377 B.I.Wissenschaftsverlag, 1985.

[4] Th.Beth,D.Jungnickel,H.Lenz *Design Theory* p.333 B.I.Wissenschaftsverlag, 1985.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

VECTOR SYMBOL DECODING WITH LIST INNER SYMBOL DECISIONS

John J. Metzner

Department of Computer Science and Engineering
Pennsylvania State University
University Park, Pennsylvania 16802
E-Mail: metzner@cse.psu.edu

Abstract Vector symbol decoding is an outer code decoding technique for a concatenated code which works with a (n-k)*r syndrome matrix **S** of n-k linear combinations of r-bit inner code symbol vectors. A Gauss-Jordan reduction provides an error location vector. The zeroes in the error location vector are the apparent error positions, and the number of zeroes should match the rank of **S**. Then the error values can be solved for. Decoding success is related to the linear independence of error vectors. Data scrambling techniques for inner code symbols can make linear independence likely for moderately large r. Any parity check code structure can be used for the combination rules.

The new result is that, if the outer code decoder has available a (possibly ordered) list of two or more alternative decisions for some or all inner symbols, a slightly modified vector symbol decoder automatically reveals most correct alternatives, allowing more powerful and often simpler correction. Moreover, the ability to recognize these alternatives does not require error vector linear independence.

The main idea is to store differences between alternative choices and the first choice as additional rows below the syndrome matrix **S**. Let **x** = first choice, **y** = second choice. If **y** is correct, the stored **x** - **y** = **e**, the true error. When column operations are done on the augmented matrix to transform the n-k rows of **S**, if **y** is correct, **e** will almost always be directly revealed as a member of the row space of **S**. Also, its position is known by construction. A simple theorem shows that **e** is revealed whenever the first-choice error positions do not completely cover any code word of the combination code (because then all the error vectors will be in the row space of **S**, even if the error vectors are linearly dependent). It is found that the probability that the error vectors are not all in the row space of **S** is about **four orders of magnitude lower** than the decoder error probability for an equal-rate maximum distance nonbinary outer code working with a 0.01 - 0.1 vector symbol error probability range, for cases of a (15,4) binary combination code and a (23, 12) Golay binary combination code. Even for a randomly-chosen (255, 223) binary combination code, the probability the errors are not all in the row space of **S** is at least two orders of magnitude lower than the decoder failure probability of a (255,223) Reed-Solomon code correcting up to the guaranteed error probability, in the symbol error probability range 0.02-0.06. For conditional second choice error probability less than about 0.3 and large r, the decoder failure probability closely approximates the probability that the first-choice error positions cover some code word, in the ranges stated.

If ρ is the rank of S, there is a probability of about $2^{-(r-\rho)}$ that **x** - **y** is in the row space of S for a false **y**. However, the error location vector acts as added verification whether the position of **y** is one of the apparent error locations. Another theorem shows that the number of false apparent error locations in the error location vector can not exceed the number of combination code words covered by the error vectors in at least all but one position. This number would usually be zero, and rarely > 1.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Selectable Delay Turbo Decoding

Stephen G. Wilson
Dept. of EE, Univ. of Virginia
Charlottesville, VA 22904-4743

Munevver Kaya
Dept. of EE, Univ. of Virginia
Charlottesville, VA 22904-4743

Abstract —

We present a method for selectable delay turbo coding that, using a common serially-concatenated encoding operation with interleavers of growing lengths, allows decoders having differing latency constraints to achieve decoding power commensurate with that delay.

I. Introduction

Concatenated encoding with soft, iterative decoding is known to be capable of achieving operation near the Shannon bound on the AWGN and other channels, provided the interleaving length is sufficiently large (see for example [1]). Other than decoder computational complexity attached to the APP algorithm and subsequent iterative decoding passes, the primary negative aspect of turbo codes is latency (delay) associated with the interleaving and deinterleaving mappings in the decoder. It is now known [2], [3], that concatenated systems with iterative decoders perform nearly as well as any code for a given specified latency. Still, latency is a sensitive issue for many applications, e.g. two-way interactive voice traffic. Also, it is easy to envision applications whose latency allowances vary widely from frame to frame. We thus propose a system which admits decoder choice in latency, while sharing a common transmission framework. We suggest this has applications in multimedia data transmission applications, or in allowing performance/delay tradeoffs.

II. System Description

We will illustrate the concept with the three-level serial concatenation scheme shown in Figure 1. A message $\mathbf{u}$ with length N enters the encoder, and is systematically encoded by a 2-state convolutional encoder with feedback. The sequence $\mathbf{p^1}$ is formed as the running sum of the input to the encoder, i.e. ${p_n}^1 = \sum_{j=1}^{n} w_j$. To maintain

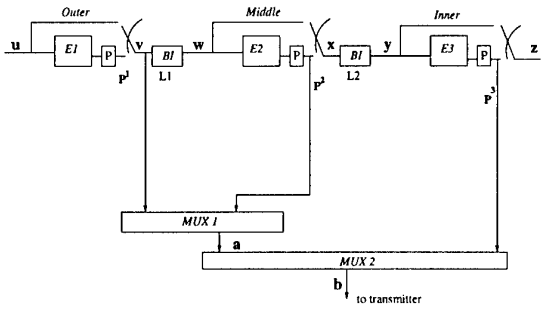


Figure 1: Diagram of three-level encoder

high rate, we puncture much of the parity stream, and for discussion here, preserve every seventh parity bit for transmission. Hence the first component is a rate 7/8, two-state convolutional encoder. The multiplexed bit stream is designated $\mathbf{v}$ and has length $(8/7)N$. As with standard SCCC systems, the sequence $\mathbf{v}$ is bit-interleaved into a permuted sequence $\mathbf{w}$, using an interleaver. Here we suggest interleaver size D_1 in the range of a few hundred bits, ultimately allowing a modest delay iterative decoding.

The pseudo-message $\mathbf{w}$ is presented to another encoder, also here having two states and rate 7/8. The output parity sequence $\mathbf{p^2}$ is again punctured and multiplexed with the input sequence, producing a sequence $\mathbf{x}$ having length $(8/7)^2N$. Finally, $\mathbf{x}$ is interleaved to a sequence $\mathbf{y}$ with an interleaver having size D_2, perhaps 4000 bits. The sequence $\mathbf{y}$ is encoded as above, producing a final sequence $\mathbf{z}$, whose length is $(8/7)^3N$, so that the overall encoding rate is $(7/8)^3$.

Instead of transmitting the sequence $\mathbf{z}$ we propose a reordering so that selectable latency options exist. Specifically, we form the sequence $\mathbf{b}$ as shown in Figure 1, obtained by first multiplexing $\mathbf{v}$ with the punctured version of $\mathbf{p^2}$ to produce $\mathbf{a}$. Note that this sequence retains the proper ordering of the $\mathbf{v}$ sequence, so that "zero-delay" decoding is possible. Then, $\mathbf{b}$ is formed by multiplexing the punctured parity sequence $\mathbf{p^3}$ into $\mathbf{a}$.

Depending on the latency allowed, three decoding architectures are possible. First, a simple Viterbi decoding of the sequence $\mathbf{v}$, with essentially zero delay, is possible merely by deleting unncessary parity bits from the received stream. A moderate delay iterative decoder using two SISO modules can be built to process the noisy reassembled version of $\mathbf{x}$. This decoder's latency is proportional to D_1. Finally a full three-SISO decoder can be fashioned to exploit the entire received stream. Its latency is proportional to D_2.

III. Results

We have simulated the performance of the three decoding options in conjunction with BPSK transmission on a Gaussian noise channel. To illustrate, for a message size 4900 bits, encoded with overall rate $(7/8)^3 = 0.67$, and interleaver sizes $D_1 = 280$ and $D_2 = 6400$, we find that "zero delay" decoding achieves $P_b = 10^{-4}$ at $E_b/N_0 = 8$ dB, consistent with high-rate, low complexity, and penalty of discarded parity. With two-SISO decoding (moderate delay), we achieve a coding improvement of about 3 dB over the zero-delay option at $P_b = 10^{-5}$. Finally, the three-level iterative decoder achieves error probability 10^{-5} at $E_b/N_0 = 2.7$ dB. This is about 1.7 dB short of channel capacity for binary PSK when R=0.67 signaling is employed. In summary, progressively more energy efficiency is gained as the latency constraint is relaxed and more decoder levels are employed. In addition to the gain implied by larger latency, we obtain extra value from not discarding parity symbols. Each of these performances is attainable with a common transmitting framework.

IV. Bibliography

1. Berrou C., Glavieux, A., and Thitimajshima, P, "Near Shannon limit error-correcting coding and decoding: Turbo codes," ICC 1993 Record.
2. Dolinar, S., Divsalar, D., and Pollara, F., "Code Performance as a Function of Block Size," TMO PR 42-133, pp 1-23, May, 1998, Jet Propulsion Laboratory. See also Int'l Symposium on Info. Theory, Cambridge, Mass, 1998.
3. Schlegel, C., and Perez, L., "On Error Bounds and Turbo Codes," IEEE Communication Letters, pp 205-207, July, 1999.

[1]This work was supported by NSF grant NCR-9714646

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Soft Output Viterbi Algorithm (SOVA) for Non-binary Turbo Codes

Jun Tan and Gordon L. Stüber
Electrical and Computer Eng.
Georgia Institute of Technology,
Atlanta, GA 30332-0250, USA

Abstract — **An optimal MAP-equivalent SOVA decoding algorithm and its simplified suboptimal algorithm for non-binary codes are proposed. The implementation of its suboptimal algorithm is simpler, while its performance is very close to the optimal Log-MAP algorithm. The proposed SOVA can be used as a decoder for Turbo trellis coded modulation (TTCM). It is concluded that the proposed SOVA performs very close to the Log-MAP algorithm for both the TTCM and binary Turbo codes, and its performance is better than the conventional SOVA.**

I. Introduction

The MAP and Log-MAP algorithms are optimal in the sense of maximum *a posteriori* sequence probability. The simplified versions of MAP or Log-MAP, such as Max-Log-MAP, SOVA, are suboptimal. The optimality are traded for simplification of implementation. The SOVA is roughly half as complex as the Log-MAP [2] with some performance degradation. As for non-binary codes, the complexity of MAP algorithm becomes overwhelming and the simplified suboptimal algorithms are badly needed, with desirable small performance degradation. In this paper, a different implementation of MAP algorithm is proposed, together with a suboptimal algorithm. It is shown the performance of the suboptimal algorithm for non-binary Turbo codes is near to the performance of optimal MAP.

II. MAP equivalent SOVA

One elegant derivation of the MAP algorithm is presented in [1] by splitting the joint probability $p(s', s, \mathbf{y})$, where $s' \to s$ is the state transition at some epoch k, and $\mathbf{y}$ is the received sequence. Another way to derive the joint probability $p(s', s, \mathbf{y})$ is

$$p(s', s, \mathbf{y}) = P(s'|s, \mathbf{y})P(s|\mathbf{y})p(\mathbf{y}). \tag{1}$$

The probability of s' given s and the received $\mathbf{y}$ is

$$P(s'|s, \mathbf{y}) = \frac{p(\mathbf{s}_k^{(s'\to s)}, \mathbf{y}_{j<k})}{\sum_{s''} p(\mathbf{s}_k^{(s''\to s)}, \mathbf{y}_{j<k})}, \tag{2}$$

where $\mathbf{s}_k^{(s'\to s)}$ is the trellis path containing branch $(s' \to s)$, and $\mathbf{s}_k^{(s''\to s)}$ is the trellis path containing branch $(s'' \to s)$ at epoch k. For each state s at k, the number of trellis branches terminated at s is equal to M for M-ary codes. There are M possible states s'' for state transitions $s'' \to s$. The ratio of probability of a trellis path containing branch $(s' \to s)$ to the sum of probabilities of all possible trellis paths terminated at s is the probability of state s' given s and $\mathbf{y}$, i.e., $P(s'|s, \mathbf{y})$. From the VA, the path metric of path $\mathbf{s}_k$ is $M_k(\mathbf{s}_k) = \log\left(p(\mathbf{s}_k, \mathbf{y}_k)\right)$. Then we have,

$$P(s'|s, \mathbf{y}) = \frac{\exp\left(M_k\left(\mathbf{s}_k^{(s'\to s)}\right)\right)}{\sum_{s''}\exp\left(M_k\left(\mathbf{s}_k^{(s''\to s)}\right)\right)}, \tag{3}$$

where the received symbol sequence $\mathbf{y}_{j>k}$ is independent of the state transition at epoch k. The conditional probability $P(s|\mathbf{y})$ can be yielded through backward recursion, as

$$P(s'|\mathbf{y}) = \sum_{s} P(s'|s, \mathbf{y})P(s|\mathbf{y}). \tag{4}$$

The initial value of the backward recursion is $P(s|\mathbf{y}) = 1$ for terminal state s at epoch $k = N$, and $P(s|\mathbf{y}) = 0$ otherwise.

The soft output should have M possible values for M-ary source symbols. The soft output value of the proposed algorithm in probability form is obtained as,

$$\begin{aligned} P(\hat{u}_k = a|\mathbf{y}) &= \sum_{\substack{(s'\to s)\\ u_k = a}} p(s', s, \mathbf{y})/p(\mathbf{y}) \\ &= \sum_{\substack{(s'\to s)\\ u_k = a}} P(s|\mathbf{y})\frac{\exp\left(M_k\left(\mathbf{s}_k^{(s'\to s)}\right)\right)}{\sum_{s''}\exp\left(M_k\left(\mathbf{s}_k^{(s''\to s)}\right)\right)}. \end{aligned} \tag{5}$$

Using the joint probability in (1) with the *a posteriori* probability definition, we derived the implementation of MAP algorithm. In our discussion, the path metrics are computed with VA. (5) is the *a posteriori* probability, or the soft output definition of VA. So we still can call the proposed MAP implementation as a SOVA. However, the proposed SOVA is different from the SOVA in literature [1, 3, 4]. The proposed SOVA is an optimal MAP algorithm, while the conventional SOVA is a Max-Log-MAP equivalent, which is sub-optimal.

Similar to the MAP algorithm, the proposed SOVA soft output in (5) can be simplified by passing to the log-domain of probability.

[1]This research was supported by the National Science Foundation under grant CCR-9903297.

References

[1] J. Hagenauer, E. Offer and L. Papke, "Iterative decoding of binary block and convolutional codes," *IEEE Trans. Info. Theory*, Vol 42, No. 2, pp. 429–445, March 1996.

[2] P. Robertson, E. Villebrun, and P. Hoeher, "A comparison of optimal and sub-optimal MAP decoding algorithms operating in the log domain," in *IEEE Int. Conf. on Communications*(Seattle, WA, June 1995), pp. 1009–1013.

[3] M. P. C. Fossorier, F. Burkert, S. Lin, and J. Hagenauer, "On the equivalence between SOVA and Max-Log-MAP decodings," *IEEE Comm. Letters*, Vol. 2, No. 5, pp. 137–139, May 1998.

[4] Ling Cong, Wu Xiaofu and Yi Xiaoxin, "On SOVA for nonbinary codes," *IEEE Comm. Letters*, Vol. 3, No. 12, pp. 335–337, Dec. 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Convergence Analysis of Turbo-Decoding of Product Codes

Assaf Sella and Yair Be'ery
Department of Electrical Engineering - Systems
Tel-Aviv University
Tel-Aviv, Israel
e-mail: {asella; ybeery}@eng.tau.ac.il

Abstract — **Geometric interpretation of turbo-decoding has founded an analytical basis, and provided tools for the analysis of this algorithm. Based on this geometric framework, we extend the analytical results for turbo-decoding of product codes, and show how analysis tools can be practically adopted for this case. Specifically, we investigate the algorithm's stability and its convergence rate. We present new results concerning the structure and properties of stability matrices of the algorithm, and develop upper bounds on the algorithm's convergence rate. We prove that for any 2 x 2 (information bits) product codes, there is a unique and stable fixed point. For the general case, we present sufficient conditions for stability. The interpretation of these conditions provides an insight to the behavior of the decoding algorithm.**

I. Introduction

Turbo codes, first introduced in 1993 [1], are considered as one of the most important developments in coding theory in recent years. Although simulation and practical results generally show excellent performance, there is a lack of theoretical basis for explaining the results and providing tools for their analysis. Recently, a new approach [2] of geometric interpretation to the decoding algorithm has managed to reveal interesting features of the decoding process. Based on it, we extend the analytical results, and use simulations to gain a deeper understanding of the turbo-decoding of product codes.

II. Product Codes Turbo-Decoding

A product code (without checks on checks) turbo encoder uses block encoders, and a rows to columns interleaver. The information bits are arranged in k_r rows and k_c columns. The i-th row (x^{r_i}) enters a (n_y, k_c, d_r) block encoder and forms a row code word y^i. The i-th column (x^{c_i}) enters a (n_z, k_r, d_c) block encoder and forms a column code word z^i (where d_r and d_c are the minimal distances of the row and column codes, respectively).

Let P_x, P_y and P_z represent the log-densities corresponding to the posterior densities $p(\widetilde{x}|x), p(\widetilde{y}|x)$ and $p(\widetilde{z}|x)$, respectively. Let Q_y, Q_z denote the extrinsic information from the rows and columns decoders, respectively. In [2] it is shown that the stability of the decoding algorithm is determined by the stability of S:

$$S = S^R S^C = (J_{P_x+P_y+Q_z} - I)(J_{P_x+Q_y+P_z} - I), \quad (1)$$

and the general expression for the Jacobian matrix is given. Using the independence of the decoding of different rows (or columns), we develop an explicit expression for J_P. E.g. for the Jacobian of the rows decoding - $(J^R)_{i,j}$ we get ($P = P_x + P_y + Q_z$):

$$\begin{cases} e^P(x_j = 1|x_i = 1) - e^P(x_j = 1|x_i = 0) & x_i, x_j \in x^{r_a} \\ 0 & x_i \in x^{r_a}, x_j \in x^{r_b} \end{cases} \quad (2)$$

The brute-force calculation complexity of a J^R element is $o(2^{k_c-1})$, also, note that it is a diagonal block matrix, whose i-th block ($J^{R,i}$) is the Jacobian matrix of the i-th row decoding.

We show that for general values of k_r and k_c , S is a block matrix, where each block ($S^{i,j}$) is a k_c x k_c matrix, with an all zeros diagonal. The main diagonal of S is the zero matrix ($S^{i,i} = 0$). For $k_r = k_c = 2$ we get:

$$S = \begin{pmatrix} & & & a_{1,2}b_{2,4} \\ & & a_{2,1}b_{1,3} & \\ & a_{3,4}b_{4,2} & & \\ a_{4,3}b_{3,1} & & & \end{pmatrix}, \quad (3)$$

where $a_{i,j} = (S^R)_{i,j}$ and $b_{i,j} = (S^C)_{i,j}$.

Theorem 1: The fixed point of *any* product code turbo-decoder with $k_r = k_c = 2$ is always stable.

Proof: From (2) we deduce that the absolute value of each element of J^R is less or equal to 1, hence, $|a_{i,j}| < 1$. The same holds for $b_{i,j}$. Therefore, the eigenvalues of S are inside the unit circle, and S is stable (regardless of the SNR or the rows or columns encoders).

For the general case, we develop in [3] an upper bound for the maximal eigenvalue of S (which governs the convergence rate in the vicinity of the fixed point), and sufficient conditions for the stability of the decoding algorithm. The basic component in these conditions is the product of the posterior dependence between two bits in a row, and the sum of the posterior dependencies between one of these bits and all the bits in its column. Hence, small column posterior dependencies (i.e. successful columns decoding) can compensate for a large value of inter-row bit dependence (i.e. unsuccessful row decoding) and vice versa.

In our talk we present simulation results for the stability matrices of Hamming $[(7,4,3)]^2$ and Golay $[(24,12,8)]^2$ product codes. Further analysis of the results is made using distribution histograms of the complete eigenvalues spread, at the algorithm's fixed-point.

References

[1] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: turbo codes," *Proc. of ICC '93* , pp. 1064–1070.

[2] T. Richardson, "The geometry of turbo-decoding dynamics," *IEEE Trans. on Information Theory* , vol. 46, no. 1, pp. 9–23, Jan. 2000.

[3] A. Sella and Y. Be'ery, "Convergence analysis of turbo-decoding of product codes," submitted to *IEEE Trans. on Information Theory*.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Turbo-Decoding as a Numerical Analysis Problem

Pär Moqvist
Ericsson Mobile Data Design AB
S:t Sigfridsg. 89
SE-412 66 Göteborg, Sweden
e-mail: pmoqvist@ce.chalmers.se

Tor M. Aulin
Chalmers University of Technology
Dept. of Computer Engineering
SE-412 96 Göteborg, Sweden
e-mail: tor@ce.chalmers.se

Abstract — **After recognizing classical turbo-decoding as fix-point iteration, alternative numerical methods such as Gauss-Seidel iteration, Jacobi over-relaxation iteration, the damped substitution method, and Newton-type methods are evaluated. None of these methods seem to perform better than fix-point iteration, and it is noticed that not even Newton's method performs better due to the presence of a random interleaver.**

I. Problem Statement

Consider a turbo code [1] with a random interleaver of length N equal to the block size, transmitted over an additive white Gaussian noise channel using a binary antipodal signal set. The iterative receiver employs *a posteriori* probability (APP) algorithms (MAP decoders) for the two constituent codes. In classical turbo-decoding, the MAP decoders simply feed each other after proper interleaving/deinterleaving, and the final decisions are based on the APPs from the last decoder after a number of iterations. Given a block of received samples, a full decoding iteration corresponds to a nonlinear function $\mathbf{g} : \mathbf{R}^N \rightarrow \mathbf{R}^N$, which produces extrinsic log-likelihood ratios (LLR) from the input *a priori* LLRs. Using similar functions $\mathbf{c}_1$, $\mathbf{c}_2$ for the constituent MAP decoders, and denoting the operations of the interleaver/deinterleaver with permutation matrices $\mathbf{P}$ and $\mathbf{P}^{-1} = \mathbf{P}^T$, respectively, $\mathbf{g}(\mathbf{L}^n) \triangleq \mathbf{P}^T\mathbf{c}_2(\mathbf{P}\mathbf{c}_1(\mathbf{L}^n))$ at iteration n. Usually, $\mathbf{L}^0 = \mathbf{0}$.

For every received block, the goal is to find a multidimensional fix-point $\mathbf{L}^*$, in which $\mathbf{L}^* = \mathbf{g}(\mathbf{L}^*)$. This implies convergence of bit decisions based on $\mathbf{L}^*$. Equivalently, we can find a root to $\mathbf{f}(\mathbf{L}^*) = \mathbf{0}$ where $\mathbf{f}(\mathbf{L}) \triangleq \mathbf{g}(\mathbf{L}) - \mathbf{L}$. Clearly, classical turbo-decoding corresponds to fix-point iteration (or the substitution method), $\mathbf{L}^{n+1} = \mathbf{g}(\mathbf{L}^n)$. Of course, fix-points can be found (possibly faster) with several other numerical methods.

II. Overview of Numerical Methods

First, consider a recursion similar to Gauss-Seidel's method for a system of linear equations [2]: $L_k^{n+1} = g_k(L_1^{n+1}, \ldots, L_{k-1}^{n+1}, L_k^n, \ldots, L_N^n)$, $k = 1, \ldots N$. Normally, it converges slightly faster than fix-point iteration. However, using block-mode MAP decoders, $\mathbf{c}_1$ and $\mathbf{c}_2$ are evaluated for all k at the same time, thus not allowing a successive evaluation. Instead, consider a method similar to Jacobi over-relaxation (JOR) iteration for linear equations [3]: $\mathbf{L}^{n+1} = a_n\mathbf{g}(\mathbf{L}^n) + (1 - a_n)\mathbf{L}^n$, $0 < a_n \leq 1$. If it converges, it still solves the fix-point problem. Since the Jacobian of $\mathbf{g}$, $J_{\mathbf{g}}(\mathbf{L})$, is attenuated by a factor a_n, we expect convergence more frequently, but possibly also at a slower rate. As a third alternative, consider the damped substitution (DS) method $\mathbf{L}^{n+1} = \mathbf{g}^{DS}(\mathbf{L}^n) \triangleq a_n\mathbf{g}(\mathbf{L}^n) = a_n\mathbf{P}^T\mathbf{c}_2(\mathbf{P}\mathbf{c}_1(\mathbf{L}^n))$, $a_n > 0$, and where a_n approaches one as n increases. $J_{\mathbf{g}}(\mathbf{L}^*)$ and $J_{\mathbf{g}}^{DS}(\mathbf{L}^*)$ are the same, suggesting convergence equally frequently. The DS method does not differ very much from the modified DS $\mathbf{L}^{n+1} = \mathbf{P}^T\mathbf{c}_2(\sqrt{a_n}\mathbf{P}\mathbf{c}_1(\sqrt{a_n}\mathbf{L}^n))$, originally used in [1].

With Newton's method for solving $\mathbf{f}(\mathbf{L}^*) = \mathbf{0}$, a common approach [4] is to use $\mathbf{L}^{n+1} = \mathbf{L}^n + a_n\mathbf{s}^n$, $0 < a_n \leq 1$, with the Newton direction $\mathbf{s}^n = -J_{\mathbf{f}}^{-1}(\mathbf{L}^n)\mathbf{f}(\mathbf{L}^n)$. a_n is determined at each iteration by performing a backtracking line search, which aims at yielding a sufficient decrease in some function relating to the distance from the solution, e.g. $d(\mathbf{L}) \triangleq \| \mathbf{f}(\mathbf{L}) \|^2$. Requiring a decrease in $d(\mathbf{L})$ is exactly what we would do if we were trying to minimize $d(\mathbf{L})$ over $\mathbf{L}$. However, all its local minima need not be roots of $\mathbf{f}$, a fact which turns out to be a clear drawback in turbo-decoding. (In fact, all gradient methods suffer from the problem of finding false roots.) Furthermore, due to the random interleaver, most of the elements of $J_{\mathbf{g}}(\mathbf{L})$ are close to zero, hence $J_{\mathbf{f}}(\mathbf{L}) \approx J_{\mathbf{f}}^{-1}(\mathbf{L}) \approx -\mathbf{I}$, reducing Newton's method to the JOR iteration. In practice, $J_{\mathbf{g}}(\mathbf{L})$ certainly has some significant elements, but we can still imagine that the strength of Newton's method - to exploit the Jacobian - is of little value for a problem such as turbo-decoding.

III. Simulation Results and Conclusions

The different methods were compared by computer simulations estimating the bit error rate (BER) for a non-punctured turbo code employing two identical rate-1/2 recursive systematic convolutional codes with generating matrix $G(D) = [\ 1,\ (1 + D^2)/(1 + D + D^2)\ ]$, separated by an S-random interleaver with S=19 and N=1024. At E_b/N_0=0.75 dB, BER$\approx 10^{-3}$ after 10 iterations with fix-point iteration. With the JOR, DS, and modified DS iterations, a large number of attenuation coefficient sequences ending with $a_n = 1$ were evaluated. None of these methods were able to converge faster (in terms of BER for a given number of iterations) than fix-point iteration. With Newton's method, the BER flattens out at appr. 10^{-2} even in the absence of noise, obviously because it finds a false root for many blocks. In conclusion, fix-point iteration seems to be the superior choice in most situations.

References

[1] C. Berrou *et al.*, "Near Shannon limit error-correcting coding and decoding: Turbo codes," in *Proc. IEEE ICC'93*, Geneva, May 1993, pp. 1064–1070.

[2] A. Korganoff, *Méthodes de Calcul Numérique, Tome 1*, Paris: Dunod, 1961.

[3] O. Axelsson, *Iterative Solution Methods*, Cambridge: Cambridge Univ. Press, 1994.

[4] J. E. Dennis, Jr. and R. B. Schnabel, *Numerical Methods for Unconstrained Optimization and Nonlinear Equations*, Englewood Cliffs, NJ: Prentice-Hall, 1983.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Efficient Reconstruction at the Output of a Discrete Memoryless Channel

Vladimir I. Levenshtein [1]
Keldysh Inst. Appl. Math., RAS
Miusskaya Sq. 4, 125047 Moscow
e-mail: leven@spp.Keldysh.ru

Abstract — **Asymptotic behaviour of the minimum number of the repeated transmissions of a sequence over a discrete memoryless channel sufficient for its exact (or within a permissible Hammimg distance) reconstruction with a given error probability is found.**

I. Introduction

Traditional problems of theory of information transmission consist in efficient transmission of messages over noisy channels which are described by combinatorial or probabilistic conditions. For solution of these problems it is used a *coding* to introduce a redundancy to messages so that the distance between the encoded messages would be sufficiently large and allows one to correct errors at the output of channels. However, some natural problems, such as analysis of observations, recovering genetic information, require to reconstruct an *arbitrary* sequence using a sufficiently large number N of its erroneous patterns. In these cases we in fact use the repeated transmission, because such patterns can be considered as a result of an N-tuple transmission of the sequence over the same combinatorial or probabilistic channel. This gives rise to new combinatorial and probabilistic problems of finding the minimum number N of erroneous patterns sufficient to reconstruct an unknown sequence with a given accuracy. The precise setting of the problems and solutions to a number of them can be found in [2], [3]. Below we present some results for a discrete memoryless channel C with a matrix $(p_{i,j})$ of transition probabilities of the set $F_q = \{0, 1, ..., q\}$ into F_r, $q \geq 2, r \geq 2$.

II. Optimal and Reducible N-Recontructors

We deal with *non-degenerate* channels C for which the transition matrix $(p_{i,j})$ does not have two identical rows and contains a column with at least two nonzero probabilities. For any $i, k \in F_q$, denote by $C(i,k)$ the subset (which may be empty) consisting of all $j \in F_r$ such that $p_{i,j}p_{k,j} > 0$. For any s, $0 \leq s \leq 1$, let $\alpha_{i,k}(s) = \sum_{j \in C(i,k)} p_{i,j}^{1-s} p_{k,j}^{s}$ and $\alpha(C) = \max_{i,k \in F_q,\ i \neq k} \min_{0 \leq s \leq 1} \alpha_{i,k}(s)$. One can show that $0 < \alpha(C) < 1$ if and only if C is non-generate channel. For any $x = (x_1, ..., x_n) \in F_q^n$ and $Y = (y_1, ..., y_N)$, where $y_j = (y_{1,j}, ..., y_{n,j}) \in F_r^n$, $j = 1, ..., N$, we set $P_C(Y|x) = \prod_{j=1}^{N} \prod_{k=1}^{n} p_{x_k, y_{k,j}}$. We consider Y as the matrix $(y_{i,j})$ of the size $n \times N$ over F_r and denote by $Y_{n,N}$ the set of all r^{nN} such matrices. Let M_N be the set of all mappings $f : Y_{n,N} \to F_q^n$, $n = 1, 2, ...$, which are referred to as *N-reconstructors*. Given an integer-valued function $d = d(n)$, $0 \leq d < n$, and $f \in M_N$, one can calculate the error probability $P_C(f, x, d, N) = \sum_{Y \in Y_{n,N},\ d_H(f(Y), x) > d} P_C(Y|x)$ of reconstructing $x \in F_q^n$ with at most d wrong letters (here $d_H(z, x)$ is the Hamming distance). Note that the case $d = 0$ corresponds to the exact reconstruction. We set

$$P_C(n, d, N) = \min_{f \in M_N} \max_{x \in F_q^n} P_C(f, x, d, N) \qquad (1)$$

and call an N-reconstructor f *optimal* if it gives the minimum in (1) for all n (optimal N-reconstructors exist for any function $d = d(n)$). An N-reconstructor f for a memoryless channel C is called *reducible*, if there exists a memoryless channel C_N such that for any n ($n = 1, 2, ...$) and $x, z \in F_q^n$, $\sum_{Y \in Y_{n,N},\ f(Y) = z} P_C(Y|x) = P_{C_N}(z|x)$. Thus, the action of a reducible N-reconstructor reduces N-tuple transmission of a message over C to its *single* transmission over another "improved" memoryless channel C_N. Reducible N-reconstructors are in general not optimal, but we use them and the classical work [1] to obtain the following estimates.

Theorem 1 *For any non-degenerate discrete memoryless channel C, $P_C(n, d, N) = \sum_{i=d+1}^{n} \binom{n}{i} P^i (1-P)^{n-i}$, where $(2q)^{-1} (\alpha(C))^N e^{-\beta(C)\sqrt{N}} \leq P \leq (q-1)(\alpha(C))^N$, and $\beta(C) = \sqrt{2} \min \max_{j \in C(i,k)} |\ln p_{i,j}/p_{k,j}|$ with the minimum being taken over all $i, k \in F_q$ such that $\alpha(C) = \min_{0 \leq s \leq 1} \alpha_{i,k}(s)$.*

III. The Minimum Number of Repetitions

Denote by $N_C(n, d, \varepsilon)$ the minimum integer N such that $P_C(n, d, N) \leq \varepsilon$, $0 < \varepsilon < 1/2$. Thus, $N_C(n, d, \varepsilon)$ is the minimum number of repeated transmissions that allow one to reconstruct any sequence of length n with accuracy up to d letters with the error probability at most ε.

Theorem 2 *Let $\varepsilon = \varepsilon(n) > 0$ and $d = d(n) \geq 0$ be functions such that $\varepsilon \to 0$ and $d/n \to 0$ as $n \to \infty$. Then for any non-degenerate discrete memoryless channel C,*

$$N_C(n, d, \varepsilon) \sim (\ln \frac{n}{d+1} + \frac{1}{d+1} \ln \frac{1}{\varepsilon}) / \ln \frac{1}{\alpha(C)}.$$

In particular, by Theorem 2 $N_C(n, d, \varepsilon)$ grows linearly with length n when the permissible error probability ε of reconstruction of a sequence with a fixed number d or less wrong letters decreases exponentially with n. On the other hand, one can prove that if $d \geq \delta n$, where $0 < \delta \leq 1$, and $\varepsilon \geq 2^{-cn}$, $c > 0$, then $N_C(n, d, \varepsilon)$ is restricted above by a constant. For instance, in the case of the symmetric binary channel with $p = 0.02$, we get that for $\delta = 0.01$, and $c = 0.1$ five repetitions are sufficient independently of length n.

References

[1] C. Shannon, R.G. Gallager and E.R. Berlekamp, "Lower bounds to error probability for coding on discrete memoryless channels", *Inf. and Control*, vol. 10, pp. 65–103 and 522–552, 1967.

[2] V.I. Levenshtein, "Reconstruction of objects from a minimum number of distorted patterns", *Doklady Mathematics*, vol. 55, no. 3, pp. 417–420, 1997.

[3] V.I. Levenshtein, "Efficient reconstruction of sequences", Submitted to *IEEE Trans. on IT*.

[1] This work was supported by the RFBR Grant 99-01-00941

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Multi-Resolution Channel Codes

Hanying Feng[1] Michelle Effros
Dept. of Electrical Eng. (136-93)
California Institute of Technology
Pasadena, CA91125, USA
email: {fhy, effros}@z.caltech.edu

Abstract — **In this paper, we present a new approach for channel coding on unknown or time-varying channels. Given a family of possible channel characteristics, we define a multi-resolution channel code as a single channel coding codebook from which a collection of codes of increasing rates are extracted by choosing larger and larger nested subsets of the original set of codewords. We give an achievable rate region and a tight converse.**

I. Introduction

Consider the problem of channel coding for an unknown or time-varying channel. Given a family of possible channel characteristics, in theory we could design a different channel code for each channel in our collection. Assuming knowledge (at both the transmitter and the receiver) of the channel in operation at communication time, both encoder and decoder could choose among the family of codes. The resulting strategy would theoretically achieve the capacity of any channel in the collection (e.g., [1], [2] and [3]). Unfortunately, this approach requires an uncountably infinite collection of channel codes when Ω is uncountably infinite. We define a multi-resolution channel code (MRCC) as a single channel coding codebook from which a collection of codes of increasing rates are extracted by choosing larger and larger nested subsets of the original set of codewords. Given a collection Ω of channels and a fixed set of $2^{nR_{\max}}$ channel codewords, the MRCC uses the first $2^{nr(\theta)}$ codewords to code at rate $r(\theta) \leq R_{\max}$ across channel $\theta \in \Omega$. We here consider the set of rate functions $r(\cdot)$ achievable on a fixed class Ω of channels. MRCCs are similar in application to punctured channel codes (e.g., [4]).

II. Preliminaries

Consider a class Ω of memoryless channels with common input alphabet A and output alphabet B. For each $\theta \in \Omega$, let $C(\theta)$ and ν_θ denote the capacity and conditional distribution of channel θ, respectively. Given Ω, a positive constant $R_{\max}$, and a rate function $r : \Omega \to [0, R_{\max}]$ that is measurable with respect to the Borel σ-algebra of open subsets on Ω, a MRCC $\mathcal{C}_n = (\mathcal{F}_n, f_n, g_n, r)$ on Ω is a single channel code defined by a codebook $\mathcal{F}_n$, a measurable encoder f_n, and a measurable decoder g_n. The channel codebook $\mathcal{F}_n$ contains $\lfloor 2^{nR_{\max}} \rfloor$ blocklength-n codewords. The codewords are ordered and denoted by $\mathcal{F}_n = \{a^n(1), \ldots, a^n(\lfloor 2^{nR_{\max}} \rfloor)\}$. The channel $\theta \in \Omega$ in operation is assumed to be fixed and known to the channel code's encoder and decoder during any single channel use. The channel may vary from channel use to channel use. For any $\theta \in \Omega$, the code is used at rate $r(\theta)$ on channel θ. The collection $U_n^{(\theta)}$ of allowable messages on θ is defined as $U_n^{(\theta)} = \{1, \ldots, \lfloor 2^{nr(\theta)} \rfloor\}$. For any $\theta \in \Omega$, the encoder is defined as $f_n(\theta, u) = a^n(u)$ for all $u \in U_n^{(\theta)}$; the corresponding decoder $g_n(\theta, \cdot)$ maps the channel output space B^n back to the set $U_n^{(\theta)}$ of allowable messages. For any $\theta \in \Omega$ and $u \in U_n^{(\theta)}$, let $\Gamma_u^{(\theta)} = \{y^n \in B^n : g_n(\theta, y^n) = u\}$ represent the decoding cells associated with u and θ. Then for any class Ω of channels and MRCC $\mathcal{C}_n = (\mathcal{F}_n, f_n, g_n, r_n)$, we define the average probability of error of $\mathcal{C}_n$ on Ω with respect to β as

$$P_{e,\beta}^{(n)}(\mathcal{C}_n, \Omega) = \int_\Omega \left[\frac{1}{\lfloor 2^{nr(\theta)} \rfloor} \sum_{u \in U_n^{(\theta)}} \nu_\theta^n((\Gamma_u^{(\theta)})^c | a^n(u)) \right] d\beta(\theta),$$

where β is an arbitrary distribution on Ω.

A $(\lfloor 2^{nR_{\max}} \rfloor, n, r(\cdot), \epsilon)$-*block MRCC* for (Ω, β) is defined as a MRCC $\mathcal{C}_n = (\mathcal{F}_n, f_n, g_n, r)$ with $P_{e,\beta}^{(n)}(\mathcal{C}_n, \Omega) \leq \epsilon$. For any $R_{\max} < \infty$, we call the rate function $r : \Omega \to [0, R_{\max}]$ *achievable* on Ω if for *any* distribution β there exists a sequence of $(\lfloor 2^{nR_{\max}} \rfloor, n, r_n(\cdot), \epsilon_n)$-block MRCCs with respect to β on Ω such that $\lim_{n\to\infty} r_n(\theta) = r(\theta)$ for each $\theta \in \Omega$ and $\lim_{n\to\infty} \epsilon_n = 0$.

III. Results

Theorem 1 *If Ω is a collection of stationary, memoryless channels such that $\max_{\theta\in\Omega} C(\theta) < \infty$, then*

$$r(\theta) = C(\theta) \quad \forall \theta \in \Omega$$

is achievable if one of the following holds: (1) Ω is finite; (2) the channel input alphabet is finite; (3) the optimal input distribution for each $\theta \in \Omega$, has a bounded derivative and power.

Theorem 2 *If Ω is a collection of stationary, memoryless channels such that $\max_{\theta\in\Omega} C(\theta) < \infty$ and the power budget is $P(\theta)$ for any $\theta \in \Omega$, then*

$$r(\theta) = C(\theta) \quad \forall \theta \in \Omega$$

is achievable if one of the following holds: (1) Ω is finite; (2) the channel input alphabet is finite; (3) for each $\theta \in \Omega$, $\mu_\theta(x)$, the optimal input distribution for channel θ has a bounded derivative and for any $\epsilon > 0$, there exists an S_a such that $\int_{|x|>S_a} x^2 \mu_\theta(x) dx < \epsilon$.

[1]This work was supported by NSF MIP-9501977 and CCR-9909026 and grants from the Lee Center for Advanced Networking and the Powell Foundation.

References

[1] A. J. Goldsmith and M. Médard, Capacity of Time-Varying Channels with Causal Channel Side Information, Preprint.

[2] G. Caire and S. Shamai, On the capacity of some channels with channel state information, *IEEE Trans. Inform. Theory*, vol. 45, pp. 2007-2019, Sep., 1999.

[3] J. Wolfowitz, *Coding Theorems of Information Theory*, Springer-Verlag, 3rd edition, 1978.

[4] S. B. Wicker, *Error Control Systems for Digital Communication and storage*, Prentice-Hall, Englewood Cliffs, NJ, 1995.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Transmission of a Slowly Varying Markov Signal over Memoryless Channels[1]

Mark S. Pinsker
Institute for Information Transmission Problems of the Russian Acad. Sci., 19 Bol'shoi Karetnyi, 101447 Moscow, Russia
pinsker@iitp.ru

Viacheslav V. Prelov
Institute for Information Transmission Problems of the Russian Acad. Sci., 19 Bol'shoi Karetnyi, 101447 Moscow, Russia
prelov@iitp.ru

Edward C. van der Meulen
Department of Mathematics Katholieke Universiteit Leuven, Celestijnenlaan 200B, 3001 Heverlee, Belgium
prof@gauss.wis.kuleuven.ac.be

Abstract — **Information rates in certain discrete-time, memoryless, stationary channels with additive non-Gaussian noise and slowly varying input signal are investigated. Under the assumption that the input signal is a stationary Markov chain with rare transitions, it is shown that the information rate is asymptotically equivalent to the entropy of the chain and, therefore, the main term of its asymptotics does not depend on the channel noise.**

I. Introduction

Consider a stationary channel whose output signal $Y = \{Y_j\}$ is equal to the sum

$$Y_j = X_j + Z_j, \quad j = 0, \pm 1, \ldots, \tag{1}$$

where the input signal $X = \{X_j\}$ and the noise $Z = \{Z_j\}$ are independent, discrete-time, stationary processes. The problem of explicit calculation of the information rate $\overline{I}(X;Y)$ (i.e., the mutual information per unit time) in such a channel is, except for a number of special cases, rather hard. Therefore, it is important to obtain good upper and lower bounds and investigate the asymptotic behavior of $\overline{I}(X;Y)$ under different assumptions on the behavior of the parameters which characterize the input and noise processes.

In most previous papers dealing with this subject such an asymptotic behavior of $\overline{I}(X;Y)$ has been analyzed for the case where the input signal is weak, i.e., the noise is large. Here, we do not assume that the power of the input signal or the noise goes to zero or infinity, respectively, but we consider the case where the input signal $\{X_j\}$, depending on a parameter ϵ, is a slowly time varying stationary Markov chain with a finite number of states (i.e., the transition probabilities of it tend to 0 or 1 as $\epsilon \to 0$). Thus, the model (1) can be considered as a special case of the well-known simple hidden Markov model. In [1], for such kind of model the asymptotics of the mean-square error for the optimal estimates of X_n from the observations $Y_{-\infty}^n = \{Y_j, j \le n\}$ was found. We use the result of [1] to derive the asymptotics of the information rate as $\epsilon \to 0$ for the channel model considered.

In this connection, it should be noted that some relations between the mutual information and a causal mean-square filtering error were observed many years ago. But most results in this area were obtained for continuous-time models with additive white Gaussian noise.

[1]This work was supported in part by the Russian Fundamental Research Foundation under Grant 99-01-00828 and in part by INTAS under Grant 94-469.

II. Main Result

As already mentioned in the introduction, we consider a stationary channel whose input signal $X^\epsilon = \{X_j^\epsilon\}$ (and, therefore, the output signal $Y^\epsilon = \{Y_j^\epsilon\}$) depends on a parameter $\epsilon > 0$ and

$$Y_j^\epsilon = X_j^\epsilon + Z_j, \quad j = 0, \pm 1, \ldots. \tag{2}$$

It is assumed that X^ϵ is a stationary, aperiodic, and irreducible Markov chain with a finite number of states $\{x_1, \ldots, x_m,\ x_i \in \mathbf{R},\ i = 1, \ldots, m\}$ and transition probabilities

$$\Lambda_{ij} = \mathbf{P}\{X_{n+1}^\epsilon = x_j | X_n^\epsilon = x_i\} = \begin{cases} \epsilon\lambda_{ij}, & i \ne j, \\ 1 - \epsilon\lambda_{ii}, & i = j, \end{cases} \tag{3}$$

where $\lambda_{ii} = \sum_{j \ne i} \lambda_{ij}$. We will also assume that $Z = \{Z_j\}$ is a sequence of real valued i.i.d. random variables independent of X^ϵ.

Theorem. *If* $\mathbf{E}|Z_0|^\beta < \infty$ *for some* $\beta > 4$, *then*

$$\overline{I}(X^\epsilon; Y^\epsilon) = \overline{H}(X^\epsilon)(1 + o(1)), \quad \epsilon \to 0,$$

where

$$\overline{H}(X^\epsilon) = \left(\sum_{i=1}^m \sum_{j \ne i} q_i \lambda_{ij} \right) \epsilon \left(\log \frac{1}{\epsilon} \right) (1 + o(1)), \quad \epsilon \to 0,$$

is the entropy of the Markov chain X^ϵ, *and* $\{q_k = \lim_{n \to \infty} \mathbf{P}\{X_n^\epsilon = x_k\},\ k = 1, \ldots, m\}$ *is the stationary distribution of it (which does not depend on* ϵ*).*

The proof of this theorem can be found in [2]. There, we also compare the asymptotic behavior of the information rates $\overline{I}(X^\epsilon; X^\epsilon + Z)$ for the channel model (2) under the assumptions that: 1) X^ϵ is a stationary Markov chain with two states $x_1,\ x_2 \in \mathbf{R}$ and transition probabilities (3) where $\lambda_{12} = \lambda,\ \lambda_{21} = \mu$, 2) X^ϵ is a stationary Gauss–Markov process with the same covariance function as the Markov chain above. It is also assumed that the noise $Z = \{Z_j\}$ in both cases is a sequence of i.i.d. Gaussian random variables.

References

[1] G. K. Golubev ,"On filtering for a hidden Markov chain under mean-square quality criterion," to appear in *Probl. Peredachi Inf.*

[2] M. S. Pinsker, V. V. Prelov, and E. C. van der Meulen, "Information rate in memoryless channels for a slowly varying Markov signal," to appear in *Probl. Peredachi Inf.*

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Splitting the Scheduling Headache[1]

Kevin Foltz
Caltech 136-93
Pasadena, CA 91125, USA
e-mail:
kfoltz@paradise.caltech.edu

Jehoshua Bruck
Caltech 136-93
Pasadena, CA 91125, USA
e-mail:
bruck@paradise.caltech.edu

Abstract — **The broadcast disk provides an effective way to transmit information from a server to many clients. Information is broadcast cyclically and clients pick the information they need out of the broadcast. An example of such a system is a wireless web service where web servers broadcast to browsing clients. Work has been done to schedule the information broadcast so as to minimize the expected waiting time of the clients. This work has treated the information as indivisible blocks that are transmitted in their entirety. We propose a new way to schedule the broadcast of information, which involves splitting items into smaller sub-items, which need not be broadcast consecutively. This relaxes the restrictions on scheduling and allows for better schedules. We look at the case of two items of the same length, each split into two halves, and show that we can achieve optimal performance by choosing the appropriate schedule from a small set of schedules.**

I. Model and Problem

The broadcast disk is a way to send information to many clients at the same time over a broadcast medium. The broadcast disk is a central server that acts as a common cache for many clients. Data at the server is made available cyclically to the clients, according to the broadcast schedule. The goal is to schedule the broadcast information in a way that minimzes the expected waiting time of the clients.

Vaidya and Hammeed [1] worked out the optimal broadcast frequencies of items within a schedule as a function of their demand probabilities, p_i, and lengths, l_i. They showed that to minimize expected waiting time, the frequencies of broadcast, f_i, should be proportional to $\sqrt{\frac{p_i}{l_i}}$. This led to an algorithm that attempted to achieve these relative frequencies. This algorithm is good because it is computationally fairly simple and works for an arbitrary number of broadcast items with arbitrary lengths and demand probabilities. However, they make some assumptions about spacing of items that do not hold in most cases.

We look at a new way to schedule the items, which allows us to achieve better expected waiting times. We consider the case of two items of the same length, and we split each item into two halves. We then schedule these pieces of the items for broadcast. We find the optimal schedule under these conditions based on the demand probabilities.

We represent a schedule by a sequence of numbers. Each number represents a piece of an item. For example, 1122 means we broadcast two pieces of item 1 followed by two pieces of item 2. To determine which piece of an item to send, we look at which piece of that item was sent last and send the other piece.

Our metric for evaluating schedules is the following:

Definition 1 *EWT(S, p_1) is the expected waiting time using schedule S with demand probabilities p_1 and $p_2 = 1 - p_1$, assuming two items, each of length one unit, split into two halves.*

By "expected waiting time", we mean the total amount of time that a client spends listening to the broadcast channel, not including the time spent obtaining the desired data. We assume that clients start listening at random times uniformly distributed over the broadcast cycle.

II. Summary of Results

The main result is the following:

Theorem 1 *For two items of the same length, each split into two halves, the broadcast schedule that minimizes expected waiting time is:*

1122, *if* $p_1 \in \left(\frac{5}{16}, \frac{1}{2}\right]$

11222, *if* $p_1 \in \left(\frac{5}{21}, \frac{5}{16}\right]$

112222, *if* $p_1 \in \left(\frac{1}{5}, \frac{5}{21}\right]$

$122122\overbrace{2\ldots2}^{n}, n = Max\left(0, \left\lfloor \frac{-13+\sqrt{-103+\frac{32}{p_1}}}{2} \right\rfloor\right)$, *if* $p_1 \in \left(0, \frac{1}{5}\right]$

For a more detailed discussion of this result, refer to [2]. This theorem tells us that with two items of equal length, the optimal schedule is a simple function of the demand probability p_1. To prove this result, we first prove some lemmas about comparing the waiting times of different schedules. Then, we use these lemmas to narrow the set of schedules to a small set of schedules. From this set, we numerically compare the schedules to find which is best and for what value of p_1.

Is is surprising that the optimal schedule is such a simple function of p_1. The set of possible schedules is uncountably infinite. Using certain rules of manipulation, we can reduce this uncountable set to a countable set, which is essentially 25 types of schedules, each parameterized by length. From these, we see that only the small set of schedules in the theorem are optimal.

References

[1] N. H. Vaidya, S. Hameed, "Data Broadcast in Asymmetric Wireless Environments", First International Workshop on Satellite-based Information Services (WOSBIS), Rye, NY, November 1996.

[2] K. Foltz, J. Bruck, "Splitting the Scheduling Headache", Electronic Technical Report 030, Paradise Lab, Caltech, April 1999. http://www.paradise.caltech.edu/papers/etr030.ps

[1]This research was partially supported by the Lee Center for Advanced Networking at Caltech

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Information Projections Revisited*

Imre Csiszár
A. Rényi Institute of Mathematics
Hungarian Academy of Sciences
P.O.Box 127, H-1364 Budapest, Hungary
e-mail: csiszar@math-inst.hu

František Matúš
Institute of Information Theory and Autom.
Academy of Sciences of the Czech Republic
Pod vod. věží 4, 182 08 Prague, Czech Rep.
e-mail: matus@utia.cas.cz

Abstract — **The goal of this paper is to complete results about I-projections and reverse I-projections, and to correct some errors in the literature. A new tool is the concept of convex support of a probability measure, better suited for our purposes than the familiar closed convex support.**

I. Preliminaries

For probability measures (pm's) on the same measurable space, $D(P\|Q)$ denotes information divergence (relative entropy). Its infimum for P or Q in a set $\mathcal{S}$ of pm's is denoted by $D(\mathcal{S}\|Q)$ and $D(P\|\mathcal{S})$, respectively. If here a unique minimizer exists, it is called the I-projection of Q to $\mathcal{S}$ or the reverse I-projection (rI-projection) of P to $\mathcal{S}$. Such projections, particularly to linear, respectively exponential families of pm's occur in various problems of probability and statistics. Previous works studying these projections include Čencov [1], Csiszár [2], [3], Topsoe [5], etc.

We will consider linear families $\mathcal{L}_a = \{P : \int x\, dP = a\}$ for $a \in \mathbb{R}^d$, and exponential families of pm's on $\mathbb{R}^d$

$$\mathcal{E}_Q = \{Q_\vartheta : \frac{dQ_\vartheta}{dQ}(x) = \exp[\langle \vartheta, x\rangle - \Lambda_Q(\vartheta)]\,,\ \vartheta \in \operatorname{dom}\Lambda_Q\},$$

where

$$\Lambda_Q(\vartheta) = \log \int \exp\langle \vartheta, x\rangle\, dQ\,, \quad \operatorname{dom}\Lambda_Q = \{\vartheta : \Lambda_Q(\vartheta) < \infty\}\,;$$

more general situations can be easily reduced to this [3].

We define the convex support $\operatorname{cs}(Q)$ of a pm Q on $\mathbb{R}^d$ as the intersection of all convex sets of Q measure 1.

Theorem 1. *$D(\mathcal{L}_a\|Q)$ is finite iff $a \in cs(Q)$.*

We also introduce the extended exponential family

$$\operatorname{ext}(\mathcal{E}_Q) = \bigcup \{\mathcal{E}_{Q_F} : F \text{ non-empty face of } \operatorname{cs}(Q)\}$$

(see [4] for the definition of and basic facts about faces) where Q_F denotes the conditional distribution determined by Q conditioned on $\overline{F}$, the closure of F. Note that $\mathcal{E}_Q \subseteq \operatorname{ext}(\mathcal{E}_Q)$ with equality iff $\operatorname{cs}(Q)$ is open.

A similar construction appears in [1], using closed convex support (equal to $\overline{\operatorname{cs}(Q)}$) rather than $\operatorname{cs}(Q)$, but several assertions there are false. The 'right' extension concept permits us to correct those.

Example. Let Q be the normalized sum of the Lebesque measure on the unit square and the point masses δ_b, δ_c at $b = (\frac{1}{3}, 0)$, $c = (\frac{2}{3}, 0)$. Then δ_b and δ_c belong to $\operatorname{ext}(\mathcal{E}_Q)$ but not to the union of $\mathcal{E}_Q$ with its 'boundary at infinity' in the sense of [1]; they have no rI-projection to that union, contradicting Theorem 23.3 of [1].

II. Main results

Let $\{R : D(\mathcal{S}\|R) = 0\}$ be the *I-closure* $cl_I(\mathcal{S})$ and $\{R : D(R\|\mathcal{S}) = 0\}$ the *reverse I-closure* $cl_{rI}(\mathcal{S})$ of a set $\mathcal{S}$ of pm's.

Theorem 2. *For every exp. family $\mathcal{E} = \mathcal{E}_Q$ and $a \in cs(Q)$ there exists a unique pm $Q^*_{a,\mathcal{E}}$ in $cl_I(\mathcal{L}_a) \cap \operatorname{ext}(\mathcal{E})$. It satisfies*

$$D(P\|R) = D(P\|Q^*_{a,\mathcal{E}}) + D(\mathcal{L}_a\|R)\,, \quad P \in \mathcal{L}_a\,,\ R \in \operatorname{ext}(\mathcal{E})\,.$$

The pm $Q^*_{a,\mathcal{E}}$ belongs to $\mathcal{E}_{Q_F}$ where F denotes the unique face of $cs(Q)$ whose relative interior contains a.

Corollary 1. For a pm Q and $a \in \operatorname{cs}(Q)$ the I-projection of Q on $\mathcal{L}_a$ exists iff $\mathcal{L}_a$ intersects $\operatorname{ext}(\mathcal{E}_Q)$. A sufficient condition for the latter is $\operatorname{dom}\Lambda_Q = \mathbb{R}^d$.

Corollary 2. If $\mathcal{E}$ is an exponential family and P is a pm with mean a such that $D(P\|\operatorname{ext}(\mathcal{E}))$ is finite then the reverse I-projection of P to $\operatorname{ext}(\mathcal{E})$ exists and equals $Q^*_{a,\mathcal{E}}$.

Theorem 3. *For every exp. family $\mathcal{E} = \mathcal{E}_Q$ and $a \in cs(Q)$ there exists a unique $P^*_{a,\mathcal{E}}$ in $cl_{rI}(\mathcal{E})$ such that*

$$D(P\|P^*_{a,\mathcal{E}}) = D(P\|\mathcal{E}) = D(P\|cl_{rI}(\mathcal{E}))\,, \quad P \in \mathcal{L}_a\,.$$

This $P^*_{a,\mathcal{E}}$ has a mean a^*, and satisfies

$$D(P\|R) \geq D(P\|\mathcal{E}) + D(P^*_{a,\mathcal{E}}\|R)\,, \quad P \in \mathcal{L}_a\,,\ R \in cl_{rI}(\mathcal{E})\,.$$

Corollary 3. If $\mathcal{E}$ is an exponential family and P is a pm with mean a such that $D(P\|\mathcal{E})$ is finite then the rI-projection of P to $cl_{rI}(\mathcal{E})$ exists and equals $P^*_{a,\mathcal{E}}$. The rI-projection of P to $\mathcal{E}$ exists iff $P^*_{a,\mathcal{E}} \in \mathcal{E}$.

Corollary 4. The following assertions are equivalent

1. $D(\mathcal{L}_a\|\mathcal{E}) = 0$
2. $P^*_{a,\mathcal{E}} = Q^*_{a,\mathcal{E}}$
3. $cl_I(\mathcal{L}_a) \cap cl_{rI}(\mathcal{E})$ is nonempty.

Theorem 4. *$\operatorname{ext}(\mathcal{E}_Q)$ is variation closed. A sufficient condition for the equality in $cl_{rI}(\mathcal{E}_Q) \subseteq \operatorname{ext}(\mathcal{E}_Q)$ is $\operatorname{dom}\Lambda_Q = \mathbb{R}^d$.*

References

[1] N.N. Čencov, *Statistical Decision Rules and Optimal Inference.* Amer. Math. Soc. 1982 (Russian original: Nauka, Moscow 1972).

[2] I. Csiszár, I-divergence geometry of probability distributions and minimization problems, *Ann. Probab.* **3**, pp. 146–158, 1975.

[3] I. Csiszár, Sanov property, generalized I-projections, and a conditional limit theeorem, *Ann. Probab.* **12**, pp. 768–793, 1984.

[4] R.T. Rockaffellar, *Convex Analysis.* Princeton Univ. Press 1970.

[5] F. Topsoe, Information theoretical optimization techniques, *Kybernetika* **15**, pp. 7–17, 1979.

*This work was supported by the HSSS programme of ESF, by the Hungarian National Foundation for Scientific Research, Grant T 26041 and by Grant Agency of Academy of Sciences of the Czech Republic, Grant A 1075801.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Properties of the Information Value Decomposition

Joseph A. O'Sullivan
Electronic Systems and Signals Research Laboratory
Department of Electrical Engineering
Washington University, St. Louis, MO 63130
jao@ee.wustl.edu

Abstract — **The information value decomposition approximates a positive-valued matrix by a sequence of reduced rank matrices. A rank K approximating matrix is closest to the original matrix in the sense of minimizing the discrimination between the original matrix and the approximation, over rank K matrices. The information value decomposition is analogous to the singular value decomposition with discrimination used for the discrepancy measure instead of squared error. Several properties of the information value decomposition correspond to properties of the singular value decomposition. These properties are discussed.**

I. Introduction

The singular value decomposition is arguably the most important tool in numerical linear algebra and is used widely in virtually all areas of science and engineering. The singular value decomposition computes the real-valued, rank K approximation to a real-valued matrix that is closest to that matrix, where the closeness or discrepancy is measured using squared error. The information value decomposition computes the closest positive-valued, rank K approximation to a positive-valued matrix, where discrimination (or I-divergence)

$$I(\mathbf{A}||\mathbf{B}) = \sum_i \sum_j a_{ij} \ln \frac{a_{ij}}{b_{ij}} - a_{ij} + b_{ij} \tag{1}$$

is the discrepancy measure.

The information value decomposition is useful for problems where the data are naturally positive-valued, including problems in optical and hyperspectral imaging, and in approximations of joint probabilities.

Several properties of the information value decomposition result from properties of discrimination (see the work of Csiszár [1, 2, 3]). Two properties are equivalent to the successive projection property of squared error. Let $\mathcal{L}$ be any nonempty linear set

$$\mathcal{L} = \{\mathbf{p} \in \mathbf{R}_+^n : \mathbf{Qp} = \mathbf{q}\}. \tag{2}$$

Then for any $\mathbf{p} \in \mathcal{L}$,

$$I(\mathbf{p}||\mathbf{r}) = I(\mathbf{p}||\mathbf{p}^*) + I(\mathbf{p}^*||\mathbf{r}), \tag{3}$$

where $\mathbf{p}^* = \text{argmin}_{\mathbf{p}\in\mathcal{L}} I(\mathbf{p}||\mathbf{r})$. Let $\mathcal{E}$ be any nonempty exponential set

$$\mathcal{E} = \{\mathbf{r} \in \mathbf{R}_+^n : r_i = \pi_i \exp(\sum_j P_{ij}\mu_j), \text{ for some } \mu\}. \tag{4}$$

Then, for any $\mathbf{r} \in \mathcal{E}$,

$$I(\mathbf{p}||\mathbf{r}) = I(\mathbf{p}||\mathbf{r}^*) + I(\mathbf{r}^*||\mathbf{r}), \tag{5}$$

where $\mathbf{r}^* = \text{argmin}_{\mathbf{r}\in\mathcal{E}} I(\mathbf{p}||\mathbf{r})$. These two successive projection properties are central to the analysis of the information value decomposition.

Many alternating minimization algorithms [3, 4] can be rewritten as minimizing the first variable over a linear set and minimizing the second variable over an exponential set

$$\min_{\mathbf{r}\in\mathcal{E}} \min_{\mathbf{p}\in\mathcal{L}} I(\mathbf{p}||\mathbf{r}). \tag{6}$$

The computation of the information value decomposition may be written in this form, yielding an iterative algorithm for a rank K approximation. Write the approximating matrix in terms of factors as $\mathbf{B} = \mathbf{XV}^T$, where $\mathbf{X}$ and $\mathbf{V}$ are nonnegative-valued matrices with K columns, and the columns of $\mathbf{V}$ sum to 1. Denote the set of all such rank K matrices as $P(K, m, n)$. The optimal rank K matrix is found as $\mathbf{B}^{(K)} = \mathbf{X}^{(K)}\mathbf{V}^{(K)T}$ and achieves

$$\hat{\mathbf{B}}^{(K)} = \underset{\mathbf{B}\in P(K,m,n)}{\text{argmin}} \; I(\mathbf{A}||\mathbf{B}). \tag{7}$$

The rank one solution is given by the normalized marginals on the columns and rows of $\mathbf{A}$. If the entries of $\mathbf{A}$ sum to 1, the resulting discrimination equals the mutual information between two random variables whose joint distribution is $\mathbf{A}$. If the entries do not sum to 1, the discrimination is proportional to such a mutual information, with proportionality constant equal to the total sum of the entries of $\mathbf{A}$.

The successive approximation properties yield expressions for the improvement going from rank K to rank $K+1$ approximations.

References

[1] I. Csiszár, "I-Divergence Geometry of Probability Distributions and Minimization Problems," *Ann.Prob.*, vol. 3, no. 1, pp. 146-158, 1975.

[2] I. Csiszár, "Why Least Squares and Maximum Entropy? An Axiomatic Approach to Inference for Linear Inverse Problems," *Ann. Stat.*, vol. 19, pp. 2032-2066, 1991.

[3] I. Csiszár and G. Tusnady, "Information Geometry and Alternating Decisions," *Statistical Decisions*, Suppl. issue #1, pp. 205-207, 1984.

[4] Joseph A. O'Sullivan, "Alternating Minimization Algorithms: From Blahut-Arimoto to Expectation-Maximization," in A. Vardy, Ed., *Codes, Surves, and Signals, Common Threads in Communications*, Kluwer Academic, Boston, pp. 173-192, 1998.

[1]Supported by grant DAAH04-95-1-0494.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

A Group-theoretic Approach to Information Inequalities

Ho-leung Chan
Dept. of Information Engineering
The Chinese Univ. of Hong Kong
Shatin, N.T., Hong Kong
China
e-mail: hlchan6@ie.cuhk.edu.hk

Raymond W. Yeung
Dept. of Information Engineering
The Chinese Univ. of Hong Kong
Shatin, N.T., Hong Kong
China
e-mail: whyeung@ie.cuhk.edu.hk

Abstract — **In this paper, the one-to-one correspondence between group-theoretic inequalities and information-theoretic inequalities are established. The consequence is that we can prove an information-theoretic inequality by proving its corresponding group-theoretic inequality and vice versa. Finally, a new non-trivial group-theoretic inequality is found using this approach. The meaning of this inequality is yet to be understood.**

I. Group-theoretic inequalities

Definition I.1 *Let G be a finite group and $G_1, G_2, \cdots, G_n$ be subgroups of G. A group-theoretic inequality is an inequality that involves only additions or subtractions of terms of the form $\log \frac{|G|}{|G_\alpha|}$, where $|G|$ is the order of the group G and $|G_\alpha|$ is the order of the subgroup $\bigcap_{i\in\alpha} G_i$.*

A group-theoretic inequality is valid if and only if it is satisfied by all finite groups. For example, $\log \frac{|G|}{|G_1\cap G_3|} + \log \frac{|G|}{|G_2\cap G_3|} \geq \log \frac{|G|}{|G_1\cap G_2\cap G_3|} + \log \frac{|G|}{|G_3|}$ is a valid group-theoretic inequality.

II. A One-to-one correspondence

For any information inequality, we can establish a group-theoretic inequality through the following transformation. For any entropy term in the information inequality, say $H(X_\alpha)$, the entropy of the joint random variable $(X_i : i \in \alpha)$, we change it to $\log \frac{|G|}{|G_\alpha|}$. Then the inequality obtained is a group-theoreitc inequality. For example, given the information inequality, $H(X_1, X_3) + H(X_2, X_3) \geq H(X_1, X_2, X_3) + H(X_3)$, after transformation, we obtain the group-theoretic inequality $\log \frac{|G|}{|G_1\cap G_3|} + \log \frac{|G|}{|G_2\cap G_3|} \geq \log \frac{|G|}{|G_1\cap G_2\cap G_3|} + \log \frac{|G|}{|G_3|}$. It can be seen easily that the transformation is reversible, that is, given any group-theoretic inequality, we can find its corresponding information inequality.

The main result of this work is the following theorem.

Theorem II.1 *A linear information inequality is valid if and only if its corresponding group-theoretic inequality is valid.*

This theorem establishes an intriguing relation between entropy and group in the form of inequalities. A trivial implication of the theorem is that if we can also prove an information inequality, then we also prove the corresponding group-theoretic inequality, and vice versa.

III. Group-theoretic Approach

Suppose we want to prove a linear information inequality. We can prove it in two steps.

step 1: Transform the information inequality to its corresponding group-theoretic inequality.

step 2: Prove that the group-theoretic inequality is true for all groups.

Example III.1 *Suppose we want to prove $H(X_1) + H(X_2) - H(X_{1,2}) \geq 0$. It suffices to show that $\log \frac{|G|}{|G_1|} + \log \frac{|G|}{|G_2|} - \log \frac{|G|}{|G_{1,2}|} \geq 0$, or equivalently, $|G_1||G_2| \leq |G||G_1\cap G_2|$ is satisfied by all groups and their subgroups. But it is a trivial result in group theory that $|G_1||G_2| \leq |G||G_1\cap G_2|$. Hence, the result follows.*

All commonly known information inequalities can be proved by using this group-theoretic approach. Moreover, all the tools developed in group theory can be used to prove information inequalities. This approach enlarges our set of tools for proving information inequalities.

IV. Information-theoretic approach

As in the previous section, we can use an information-theoretic approach for proving group-theoretic inequalities. The procedure is similar, and we omit the details here. But an interesting result obtained by using this approach deserves mentioning. A new information inequality has recently been proved by Zhang and Yeung in [2]. This information inequality is highly non-trivial that it cannot be deduced from the commonly known information inequalities. This inequality, in terms of joint entropies, is as follows:

$$\begin{array}{l} H(X_1) + H(X_2) + 2H(X_{1,2}) \\ +4H(X_3) + 4H(X_4) \\ +5H(X_{1,3,4}) + 5H(X_{2,3,4}) \end{array} \leq \begin{array}{l} 6H(X_{3,4}) + 4H(X_{1,3}) \\ +4H(X_{1,4}) + 4H(X_{2,3}) \\ +4H(X_{2,4}) \end{array}$$

The corresponding group theoretic inequality,

$$\begin{array}{l} |G_3\cap G_4|^6|G_1\cap G_3|^4 \\ |G_1\cap G_4|^4|G_2\cap G_3|^4 \\ |G_2\cap G_4|^4 \end{array} \leq \begin{array}{l} |G_1||G_2||G_3|^4 \\ |G_4|^4|G_1\cap G_2|^2 \\ |G_1\cap G_3\cap G_4|^5|G_2\cap G_3\cap G_4|^5 \end{array}$$

appears to be new in group theory, but its meaning is yet to be understood.

References

[1] H.L. Chan and R.W. Yeung, "New Approaches to Information Inequalities Part II: Algebraic Analysis of Entropy Functions," submitted to IEEE Transactions of Information Theory.

[2] Z. Zhang and R. W. Yeung, " On the characterization of entropy function via information inequalities," IEEE Trans. on Information Theory, Vol. 44, pp.1440-1452, Jul 1998.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Toward a Theory of Information Processing

Sinan Sinanović* and Don H. Johnson*
Department of Electrical and Computer Engineering
Rice University
Houston, Texas 77251–1892
e-mail: sinan@rice.edu, dhj@rice.edu

Abstract — **Information processing is performed when a system preserves aspects of the information encoded in the input and removes other aspects. We describe an approach to quantify such information processing based on applying controlled changes to the input and observing the corresponding outputs. Information-theoretic distance measures–those that reflect the data processing theorem–are calculated on the input and output separately and compared. Properties of the resulting information transfer ratio are used to quantify the system's fundamental information processing properties.**

I. Introduction

In general, processing is performed when a system enhances certain aspects of its input as it supresses others. While some systems only re-represent the input signal without loss, such as an ideal amplifier or the Fourier transform, others do have a loss and act as "information filters." To develop a measure that would characterize a system's information processing capability, we need to compare input(s) and output(s) somehow. In linear systems, one uses the transfer function or cross-correlation. However, in quantifying the processing of more complex systems, non-linearities and non-Gaussian effects cause classical methods to fail to capture all a system does. Furthermore, in the case of the mixed input and output (e.g. continuous input, discrete output), it is difficult to find joint distribution of the input and output. We induce controlled changes of the information represented by a system's input and compare distances between inputs and between outputs using the Kullback-Leibler distance. By considering distance changes thus induced, we essentially specify what information is conveyed and processed. Finally, by measuring the difference between two inputs before and after the change and comparing this difference to the corresponding output difference, we quantify how a system processes relevant information.

II. Quantifying Information Processing

We represent information by a collection of parameters coalesced into the vector $\boldsymbol{\theta}$. Let $\mathbf{X}$ represent a system's input signal and $\mathbf{Y}$ its output. According to the data processing theorem [2], if $\boldsymbol{\theta} \mapsto \mathbf{X} \mapsto \mathbf{Y}$ ($\boldsymbol{\theta}$, $\mathbf{X}$, and $\mathbf{Y}$ form Markov chain), then $I(\boldsymbol{\theta};\mathbf{X}) \geq I(\boldsymbol{\theta};\mathbf{Y})$. Let $\mathbf{X}(\boldsymbol{\theta}_0)$, $\mathbf{X}(\boldsymbol{\theta}_1)$ represent input signals having different information content with $\mathbf{Y}(\boldsymbol{\theta}_0)$, $\mathbf{Y}(\boldsymbol{\theta}_1)$ representing the corresponding outputs. Many distance measures, which we generically write as $d(\cdot,\cdot)$, also satisfy the data processing theorem in the sense that

$$\gamma_{\mathbf{X},\mathbf{Y}}(\boldsymbol{\theta}_0,\boldsymbol{\theta}_1) \equiv \frac{d(\mathbf{Y}(\boldsymbol{\theta}_0),\mathbf{Y}(\boldsymbol{\theta}_1))}{d(\mathbf{X}(\boldsymbol{\theta}_0),\mathbf{X}(\boldsymbol{\theta}_1))} \leq 1$$

All Ali-Silvey distances [1], satisfy the data processing theorem by construction. We use one particular Ali-Silvey distance—the Kullback-Leibler (KL) distance—extensively because of its convenience and importance. We explore the quantity $\gamma_{\mathbf{X},\mathbf{Y}}$, the *information transfer ratio*, defined as the ratio of the distance between the two output distributions and the distance between the corresponding input distributions. This ratio is always between zero and one: zero means none of the information change $\boldsymbol{\theta}_0 \to \boldsymbol{\theta}_1$ is represented by the output and one means perfect reproduction of the input information change.

III. A System Theory of Information Processing

If two systems are in cascade, the overall information transfer ratio is the product of the component ratios: if $\boldsymbol{\theta} \mapsto \mathbf{X} \mapsto \mathbf{Y} \mapsto \mathbf{Z}$ form a Markov chain, $\gamma_{\mathbf{X},\mathbf{Z}} = \gamma_{\mathbf{X},\mathbf{Y}} \cdot \gamma_{\mathbf{Y},\mathbf{Z}}$ regardless of the distance measure used.

The special case wherein the information parameter is perturbed ($\boldsymbol{\theta}_1 = \boldsymbol{\theta}_0 + \delta\boldsymbol{\theta}$) yields interesting result. When the distance measure is in the Ali-Silvey class, we can explicitly write the information transfer ratio, under very general assumptions, as $\gamma_{\mathbf{X},\mathbf{Y}}(\boldsymbol{\theta}_0,\boldsymbol{\theta}_0+\delta\boldsymbol{\theta}) = \dfrac{\delta\boldsymbol{\theta}'\mathbf{F}_{\mathbf{Y}}(\boldsymbol{\theta}_0)\delta\boldsymbol{\theta}}{\delta\boldsymbol{\theta}'\mathbf{F}_{\mathbf{X}}(\boldsymbol{\theta}_0)\delta\boldsymbol{\theta}}$, where $\mathbf{F}$ is the Fisher information matrix. We refer to this result as the *local invariance property*: the information transfer ratio for perturbational changes is invariant to the choice of distance measure.

Notice that two previous results hold for any Ali-Silvey distance used in the information transfer ratio. However, the KL distance is especially convenient since it is related to *both* detection (Stein's lemma) and estimation theory (Fisher information matrix). The following results are derived using the KL distance.

When the input consists of several statistically independent components, the overall information transfer ratio is related to individual transfer ratios by an expression identical to the parallel resistor formula: $\dfrac{1}{\gamma_{\mathbf{X},\mathbf{Y}}(\boldsymbol{\theta}_0,\boldsymbol{\theta}_1)} = \sum_i \dfrac{1}{\gamma_{X_i,\mathbf{Y}}(\boldsymbol{\theta}_0,\boldsymbol{\theta}_1)}$.

Finally, consider the system with one input and N outputs that are *conditionally* independent given the input (N parallel systems is one example). We calculated how the information transfer ratio changes as more outputs are added for two special cases. In both cases as $N \to \infty$, $\gamma_{\mathbf{X},\mathbf{Y}}(\boldsymbol{\theta}_0,\boldsymbol{\theta}_1) \to 1$, and the asymptotic differential increase in γ is proportional to $1/N^2$ We believe this result applies more generally.

*Work supported by NSF Grant CCR-9628236.

References

[1] S.M. Ali and D. Silvey, "A general class of coefficients of divergence of one distribution from another," *J. Roy. Stat. Soc.* B, Vol 28, No. 1, 1966, pp.131-142.

[2] T.M. Cover and J.A. Thomas, *Elements of Information Theory*, John Wiley and Sons, Inc., 1991.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Minimizing Transmit Power for Fading Multiple-Access Channels

Michael Mecking
Institute for Communications Engineering
Munich University of Technology
D-80290 Munich, Germany
e-mail: Michael.Mecking@EI.TUM.de

Abstract — **The problem of minimizing sum transmit power for a fading multiple-access channel is considered. While for non-fading channels with equal user attenuations wideband multi-access with cooperative (joint) decoding and orthogonal access are both optimal, wideband access is superior in case of unequal attenuations or fading channels. Losses due to fading are negligible for wideband access as a result of low rate coding, and near AWGN perfomance is achievable. On the other hand, orthogonal access suffers from losses of high rate codes under fading conditions. Wideband access with non-cooperative decoding is clearly suboptimal in any case and only useful for low transmission rates.**

I. Introduction

A multiple-access channel is considered where K users are accessing the channel at information rates $R_k = R, k \in \mathcal{K} = \{1, \ldots, K\}$. Each transmission signal X_k is attenuated in power by a constant $1/\mu_k$ due to path losses and randomly attenuated by H_k due to multipath propagation assumed to result in flat fading. The fading is perfectly known at the base station for all signals individually but unknown at the transmitters. The transmitters merely have access to the average attenuations $1/\mu_k$ via a low-rate feedback link, which is used to control the powers.

The problem of minimizing sum transmit power is discussed for wideband accessing of all users with optimal cooperative (joint) decoding (WB-CD) and independent, non-cooperative decoding (WB-NCD), respectively, as well as orthogonal accessing techniques (OA).

II. Results

For WB-CD, the set $\mathcal{P}^{\mathrm{CD}}$ of required powers for equal rate transmission is given implicitely by [1] [2] [1]

$$\mathcal{P}^{\mathrm{CD}} = \left\{ \mathbf{P} \in \mathbb{R}_+^K : |S|\, R \le E\left\{ C\left(\sum_{k \in S} H_k P_k, \sigma^2 \right) \right\}, \forall S \subseteq \mathcal{K} \right\} \quad (1)$$

The problem of finding the minimum sum transmit power P_T to support reliable transmission at rates R may thus be formulated as

$$P_T = \min_{\mathbf{P} \in \mathcal{P}^{\mathrm{CD}}} \sum_{k \in \mathcal{K}} \mu_k P_k. \quad (2)$$

The region $\mathcal{P}^{\mathrm{CD}}$ is proved to be convex and thus, the minimum can be found using Kuhn-Tucker multipliers. However, $\mathcal{P}^{\mathrm{CD}}$ does not form a contra-polymatroid, and the optimum point $\mathbf{P}^*$ minimizing sum transmit power need not be a vertex. The vertices of $\mathcal{P}^{\mathrm{CD}}$ posses the outstanding property of being achievable by low complexity stripping [3]. By focusing on the best vertex a practically attractive solution is obtained which usually is close or equal to the optimum.

With WB-NCD, all users are decoded individually and in parallel considering all other users as noise. The optimum receive power P^* per user is given implicitely by [1]

$$R = \frac{e^{\frac{\sigma^2}{P^*}}}{2 \ln 2\, (K-2)!} \int_0^\infty t^{K-2} E_1\left(\frac{\sigma^2}{P^*} + t \right) dt. \quad (3)$$

For OA, the optimum receive power P^* is given by

$$R = \frac{1}{2\, K \ln 2}\, e^{\frac{\sigma^2}{K P^*}}\, E_1\left(\frac{\sigma^2}{K P^*} \right). \quad (4)$$

Both non-cooperative decoding and orthogonal access eliminate inter-user trade-offs and result in a minimum sum transmit power given by

$$P_T^{OA} = P^* \sum_{k \in \mathcal{K}} \mu_k, \quad (5)$$

which is stricly greater than the best achievable with WB-CD even for equal attenuations. WB-NCD suffers from suboptimal decoding and OA from suboptimal accessing as well as losses of high rate codes under fading conditions.

By using adaptive resource sharing, the minimum sum transmit power for OA could be reduced at the cost of a more complex encoder/decoder pair supporting variable rates.

If the users are located uniformly within a cell and the attenuations grow with the distance r_k to the receiver as $\mu_k = r_k^\rho$, expressions for the long-term average transmission power per user are found for WB accessing with stripping, WB-NCD, and OA.

References

[1] D. N. C. Tse and S. V. Hanly, "Multiaccess Fading Channels - Part I: Polymatroidal Structure, Optimal Resource Allocation and Throughput Capacities," *IEEE Trans. Inform. Theory*, vol. 44, pp. 2796–2815, 1998.

[2] S. Shamai (Shitz) and A. D. Wyner, "Information-Theoretic Considerations for Symmetric, Cellular, Multiple-Access Fading Channels - Part I," *IEEE Trans. Inform. Theory*, vol. 43, pp. 1877–1894, 1997.

[3] B. Rimoldi and R. Urbanke, "A rate-splitting approach to the Gaussian multiple-access channel," *IEEE Trans. Inform. Theory*, vol. 42, pp. 364–375, 1996.

[1] $C(P, \sigma^2) = \frac{1}{2} \log_2 \left(1 + \frac{P}{\sigma^2}\right)$ and $E_1(x) = \int_x^\infty \frac{e^{-t}}{t}\, dt$.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On Multi-Antenna Receiver Principles for Correlated Rayleigh Fading Channels

Anders Hansson[1] and Tor M. Aulin
Chalmers University of Technology
Dept. of Computer Engineering
SE-412 96 Göteborg, Sweden
{ahansson, tor}@ce.chalmers.se

Abstract — **An exact error probability analysis clearly demonstrates that adaptive antenna arrays are unable to fully exploit the implicit diversity effect of Rayleigh fading channels. Instead, a class of array receivers that yields close-to-optimal performance is proposed.**

I. System Description

Binary signaling is treated, and the channel comprises D diversity links, represented by means of D receiver antenna elements. In each link the transmitted waveform is perturbed by two time-varying random processes: one is the multiplicative fading, and the other is the additive noise. The modulator waveforms, the noise, and the fading are assumed to be statistically independent. Further, suppose that the noise processes in the different diversity links are equally strong, independent, and white stationary Gaussian. The statistical properties of the fading, which is assumed to be frequency-flat, is described in detail in [1]; the correlation function depends on the Doppler frequency shift, the direction of arrival (DOA), the angle spread (AS), and the antenna geometry.

II. Optimum and Suboptimum Reception

Optimum one-shot detection of binary signals on Rayleigh fading channels requires the continuous-time received signal to pass through a time-varying filter whose impulse response in general cannot be found on closed form [2]. In order to avoid such complex operations on the received signal, the suboptimum approach suggested in [3] will be followed here. First, the received process is projected onto a finite dimensional basis to obtain a finite set of N observation variables. Karhunen-Loève expansion (KLE) is known to be optimal, since it leads to uncorrelated observables. The basis is thus found as the solution to a vector-valued homogeneous Fredholm equation of the second kind. Here, time-orthogonal modulator waveforms are employed to make the kernel of the Fredholm equation independent of the hypotheses. Secondly, given this finite set of observables, the optimum one-shot detector performs a binary likelihood ratio test. However, the KLE is far too complex for practical implementation; recall that the no closed-form expression for the basis exists, and note that the detector has to (numerically) resolve for the basis whenever the kernel changes, i.e., whenever the Doppler shift, the DOA, or the AS changes. For a single-antenna system, a simple set of time orthonormal basefunctions (ON set) has proved to give performance comparable to that of the KLE [3]. Our proposal is then to employ the very same ON basis in each antenna.

[1]This work was supported by Grant PCC-9706-01.

Further, the concept of adaptive antenna arrays suggests a weighted sum of the antenna signals to be formed. Much research has been devoted to derive antenna weights, but the underlying models are mostly free from fading—an ideal assumption hardly met in real systems. Two weighting principles are treated: least mean square (LMS) and maximum likelihood (ML). The LMS algorithm operates by aligning the phases of the antenna signals, erroneously assuming zero AS, while the ML weights minimize the error probability. Once a continuous-time sum has been formed, the KLE still constitutes an optimum projection.

III. Calculation Results and Conclusions

Merely for brevity, both the first and second order channel statistics are assumed to be perfectly estimated. An exact expression for the probability of error has been calculated by means of the method given in [4]. Figure 1 shows that adaptive antenna arrays are suboptimal regarding error performance on Rayleigh fading channels. The error rates were calculated for a 2-element array with antenna separation=0.5 wavelength, DOA=45°, AS=90°, and Doppler frequency shift=0.1 symbol rate. The antenna patterns, DOA=60° and AS=180°, reveal a fundamental discrepancy between LMS and ML weights.

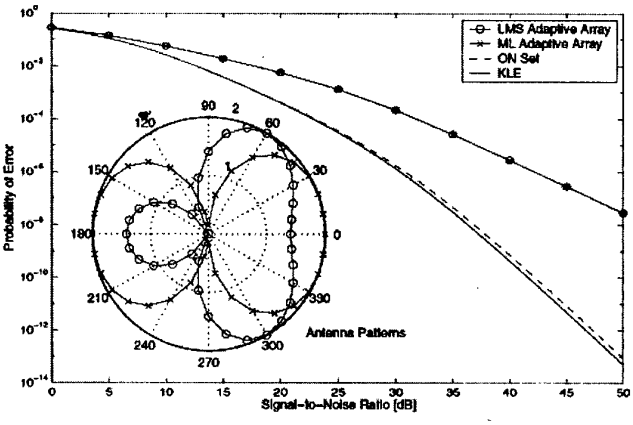


Fig. 1: Error probabilities and antenna patterns.

References

[1] A. F. Naguib, *Adaptive Antennas for CDMA Wireless Networks*, Ph.D. dissertation, Stanford University, Aug. 1996.

[2] T. T. Kadota, "Optimum reception of binary Gaussian signals", *Bell Syst. Tech. J.*, Vol. 43, pp. 2767–2810, Nov. 1964.

[3] U. Hansson and T. Aulin, "Aspects on single symbol signaling on the frequency flat Rayleigh fading channel", *IEEE Trans. Comm.*, Vol. 47, No. 6, pp. 874–883, June 1999.

[4] M. J. Barrett, "Error probability for optimal and suboptimal quadratic receivers in rapid Rayleigh fading channels", *IEEE J. Select. Areas Comm.*, Vol. 5, No. 2, pp. 302–304, Feb. 1987.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Achievable rate region for spatial multiplexing systems using the MMSE criterion

Hemanth Sampath
Information Systems Lab
Stanford University, CA-94305
hemanth1@leland.stanford.edu

Arogyaswami Paulraj[1]
Information Systems Lab
Stanford University, CA-94305
paulraj@rascals.stanford.edu

Abstract — **We address the problem of designing jointly optimum precoder and equalizer for a MIMO spatial multiplexing system using the MMSE criterion. Next, we compare the optimum power allocation policy and the achievable rate region for such a system to the well-known rate maximizing precoder and decoder design.**

I. Introduction

It is well-known that the optimum precoder and decoder that maximizes the information rate decouples the MIMO channel into parallel sub-channels and allocates bits and power on the sub-channels according to the well-known *water-pouring* strategy. This requires a variable coding and modulation scheme across sub-channels which is difficult to implement in practice for a changing MIMO channel. For fixed modulation and coded systems, the optimum design should equalize the MIMO channel. The MMSE design [1][2][3] optimally trades off noise enhancement and channel equalization at both the transmitter and receiver.

II. System Model

Spatial multiplexing involves transmitting (and receiving) independent data streams on separate antennas, through a MIMO wireless channel to achieve unparalled data-rates. Consider the following MIMO system equation:

$$X = GHFS + GN \tag{1}$$

where H is an $m \times n$ MIMO channel whose (i,j)-th entry denotes the channel gain from the j-th transmit antenna to i-th receive antenna; X is the $b \times 1$ received vector and S is the $b \times 1$ transmitted vector, where $b = rank(H) \leq min(m,n)$ is the number of independent data streams that is to be transmitted; N is the $m \times 1$ noise vector; finally, G is the $b \times m$ decoder matrix and F is the $n \times b$ precoder matrix. Assume

$$E(SS^*) = I;\ \ E(NN^*) = R_{NN};\ \ E(SN^*) = 0. \tag{2}$$

where the superscript $*$ denotes the conjugate transpose. Define the eigen-value decomposition (EVD) :

$$H^* R_{NN}^{-1} H = V \Lambda V^* = (V\ \ V_{n-b}) \begin{pmatrix} \Lambda & 0 \\ 0 & \Lambda_{n-b} \end{pmatrix} (V\ \ V_{n-b})^* \tag{3}$$

where V is an $n \times b$ orthogonal matrix which is the projector onto the range space of $H^* R_{NN}^{-1} H$ and Λ is a diagonal matrix containing the b non-zero eigen values, arranged in a decreasing order from top-left to bottom-right.

[1]On part-time leave at Gigabit Wireless Inc.

The optimum precoder and equalizer that minimizes the *total output symbol estimation errors* using the MMSE criterion, was shown to diagonalize the MIMO channel [1][3]. The optimum transmitter power allocation policy across the sub-channels is given by [1][2][3]:

$$\Phi_f^2 = (\mu^{-1/2} \Lambda^{-1/2} - \Lambda^{-1})_+ \tag{4}$$

where Φ_f^2 is a diagonal matrix of transmitter powers across sub-channels and μ is computed so that the total power constraint $tr(\Phi_f^2) = P_0$ is satisfied. This is compared to the well-known *water-pouring policy* given as:

$$\Phi_f^2 = (\mu^{-1/2} I - \Lambda^{-1})_+ \tag{5}$$

The maximum data rate for the i-th sub-channel (for both the designs) is given by:

$$C_i = log\ |1 + \Lambda_i \Phi_{f,i}^2| \tag{6}$$

where Φ_f^2 is obtained from (4) or (5).

III. Results

The MMSE design, like the rate-maximizing design, allocates non-zero power on sub-channels with highest SNRs. However, among the above chosen sub-channels, power is allocated inversely proportional to sub-channel SNRs, unlike the rate-maximizing design. This subtle, yet important difference leads to a loss in data rate which we now quantify. The capacity hit suffered by the MMSE design (under high SNRs) is given by: $\delta C = log\ |\eta^{-1}|$, where $\eta = b \frac{\Lambda^{-1/2}}{\sum_{i=1}^{b} \Lambda_i^{-1/2}}$. When H is an orthogonal matrix ($\Lambda \rightarrow I$), the capacity hit is zero i.e., $\delta C = 0$. For an iid channel matrix, the capacity hit suffered by MMSE design is minimal, while a more trivial channel inversion strategy at the transmitter suffers a great hit in capacity due to noise enhancement.

The MMSE policy ensures similar sub-channel SNRs (when compared to the water-pouring policy) and hence favors identical but lower data rate transmission across sub-channels.

References

[1] Scaglione. A, Giannakis. G.B and Barbarossa. S. "Redundant Filterbank Precoders and Equalizers Part I: Unification and Optimal Designs" *IEEE Trans. on Signal Processing*, vol 47, No.7, July 1999.

[2] Yang. J and Roy. S. "On Joint Transmitter and Receiver Optimization for Multiple-Input Multiple-Output (MIMO) Transmission Systems". *IEEE Trans. on Communications*, vol 42, No.12, December, 1994.

[3] Sampath. H and Paulraj. A. "Joint transmit and receive optimization for high data rate wireless communications using multiple antennas" *Proceedings of the Asilomar conference on signals, systems and computers*, Asilomar, CA, November, 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Error Control Coding Schemes for Multiple Channels

Ahmed Mokhtar & Amer Hassan
Teledesic, 1445 120th Ave NE
Bellevue, WA 98005 USA
{ahmed,amer}@teledesic.com

Abstract — **This paper addresses a problem in error control coding when a user has access to either one of two identical channels or may have access to both channels simultaneously. In particular, puncturing sequences *matched* to this type of scenario are identified for select convolutional codes.**

I. INTRODUCTION

Communications networks are usually designed to handle a specified peak capacity that may occur during busy hours or in highly populated regions. It is, therefore, not uncommon that such networks have excess idle capacity a good percentage of the time. The network can use this excess capacity to enhance the performance of other users accessing the network during off-peak times. This scenario was particularly motivated by global satellite systems [1]. In such systems most latitude bands provide for double coverage; that is, one user can see two satellites most of the time. When satellite capacity is under-utilized, each user can access two radio channels between a user and two distinct satellites. The simplest (and common) error control coding strategy is to use repetition coding when two channels are available: transmit the same code twice, once over each channel. The receiver can then use any soft combining method it desires when it receives both channels. In this case, a practical coding gain provides an extra 2.5 dB. The next section describes a strategy that takes better advantage of the availability of the two channels.

II. DUAL PUNCTURED CODES

Consider a digital communications system having access to two channels: channel-1 and channel-2. Each channel is bandwidth restricted such that only a rate-k/n code can be used. The intended receiver can receive the information from channel-1 only, or channel-2 only, or both channel-1 and channel-2 simultaneously. A good error control coding strategy is the following.

- Use or construct the optimal (or best known) convolutional code C with rate $k/2n$.
- Find a dual-puncturing scheme that divides C into the two codes C_1 and C_2, each with rate-k/n. Dual refers to a puncturing sequence and its 2-s compliment. The dual-puncturing scheme is such that the free distance of C_1 and C_2 are the same, *and* are as good as the best known punctured codes.
- Transmit C_1 over channel-1.
- Transmit C_2 over channel-2 when available.
- If the receiver receives channel-1 or channel-2 only, it can decode a rate-k/n punctured code using the rate-$k/2n$ code decoder.
- If the receiver receives both channel-1 and channel-2, it decodes a rate-$k/2n$ code with the same rate-$k/2n$ decoder as above.

III. SEARCH RESULTS

(A) Rate-1/3, $K = 3$ Convolutional Code

The first example is demonstrated starting with a rate-1/3, constraint length $K = 3$ (4 states) convolutional code. The octal form of the code generator is $G = (5, 7, 7)$. Using an exhaustive search, the best punctured rate-1/3 code to rate-2/3 code is derived from a puncturing sequence which is a periodic repetition of the following puncturing vector of length 6:

$$P = (1 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1)$$

to obtain C_1, with a dual puncturing vector given by

$$\overline{P} = (0 \quad 1 \quad 1 \quad 1 \quad 0 \quad 0)$$

to obtain C_2. Moreover, $d_{\text{free}}(C_1) = d_{\text{free}}(C_2) = 4$.

A commonly used puncturing sequence is a periodic sequence

$$P = (1 \quad 0 \quad 1 \quad 0 \quad 1 \quad 0 \ldots)$$

with a resulting dual puncturing vector

$$\overline{P} = (0 \quad 1 \quad 0 \quad 1 \quad 0 \quad 1 \ldots)$$

However, in this case, $d_{\text{free}}(C_1) = 4$, but $d_{\text{free}}(C_2) = 3$.

In comparison, the best known rate-2/3, $K = 3$ code has $d_{\text{free}} = 5$.

(B) Rate-1/3, $K = 4$, $G = (13, 15, 17)$

The best puncturing vector of length 12 and its dual are given by

$$P = (1 \quad 0 \quad 0 \quad 1 \quad 0 \quad 1 \quad 1 \quad 0 \quad 1 \quad 0 \quad 1 \quad 0)$$

$$\overline{P} = (0 \quad 1 \quad 1 \quad 0 \quad 1 \quad 0 \quad 0 \quad 1 \quad 0 \quad 1 \quad 0 \quad 1)$$

resulting in rate-2/3 codes such that $d_{\text{free}}(C_1) = d_{\text{free}}(C_2) = 5$. The best known rate-2/3, $K = 4$ code has $d_{\text{free}} = 7$.

(C) Rate-1/3, $K = 5$, $G = (25, 33, 37)$

The best puncturing vector of length 12 is given by

$$P = (1 \quad 1 \quad 1 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0 \quad 0)$$

resulting in rate-2/3 codes with $d_{\text{free}}(C_1) = d_{\text{free}}(C_2) = 6$. The best known rate-2/3, $K = 5$ code has $d_{\text{free}} = 8$.

REFERENCES

[1] A. A. Hassan, B. D. Molnar, and Y-P E. Wang, "Coding and modulation for mobile satellite systems," *Proceedings of the Vehicular Technology Conference*, 1997, pp. 1997-2001.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On the Linear Structure of Self-Similar Processes[1]

Carl J. Nuzman H. Vincent Poor
Dept. of Electrical Engineering
Princeton University
Princeton, NJ 08540 USA
e-mail: {cjnuzman,poor}@ee.princeton.edu

Abstract — **Self-similar processes have a rich linear structure, based on scale invariance, which is analogous to the shift-invariant structure of stationary processes. The analogy is made explicit via Lamperti's transformation. This transformation is used here to characterize the reproducing kernel Hilbert space (RKHS) associated with self-similar processes and hence to solve problems of prediction, whitening, and Gaussian signal detection. Some specific results for the fractional Brownian motion illustrate the general concepts.**

I. Self-Similar Processes

An *H-self-similar* (or H-ss) stochastic process is one whose distributions are essentially invariant to scaling of the time axis. More precisely, scaling by a factor $a > 0$ has the same effect as multiplying the process by a factor a^H:

$$\{Y(at)\} \stackrel{\mathcal{D}}{=} \{a^H Y(t)\}, \quad a > 0,$$

where the notation $\stackrel{\mathcal{D}}{=}$ indicates that the two processes have the same probability law, and where H is referred to as the *self-similarity parameter* of the process. In recent decades self-similar processes have found application in diverse fields including hydrology, medicine, finance, physics, and electrical engineering.

As noted in [1], *Lamperti's transformation* L_H given by

$$(L_H Y)(t) = e^{-Ht} Y(e^t)$$

invertibly maps an H-ss process Y on $\mathbb{R}^+$ to a stationary process $L_H Y$ on $\mathbb{R}$. The process $L_H Y$ is the *stationary generator* of Y. Recent applications of Lamperti's transformation can be found in [2], [3], [4], and [5].

II. RKHS Structure of Self-Similar Processes

The reproducing kernel Hilbert space (RKHS) formalism can be used to describe the linear space of a random process, and to describe the solutions to linear problems such as Gaussian signal detection, prediction, and whitening [6], [7]. Given a random process $Y(t)$ on an index set I, there is an isomorphism J which maps random variables in the linear space $L^2(Y, I)$ of Y to functions in a specially-structured Hilbert space $S(Y, I)$ (an RKHS). The solutions to many problems of interest are known once we have answered the following questions: Which functions belong to $S(Y, I)$? For $f, g \in S(Y, I)$, how can the inner product $\langle f, g \rangle$ be computed? For $f \in S(Y, I)$, how can the random variable $J^{-1}(f)$ be expressed?

[1]Research supported in part by the Office of Naval Research under Grant N00014-00-1-0141, in part by the National Science Foundation under Grant CCR-9979361, and in part by the U.S. Department of Defense NDSEG Fellowship Program.

The result below demonstrates that if these questions can be answered for the stationary generator of an H-ss process, then they can easily be answered for the H-ss process itself.

Theorem 1 *Suppose that Y is a H-ss process on $I \subset \mathbb{R}^+$, and that $X = L_H Y$ is its stationary generator. Denote by $J_Y : L^2(Y, I) \to S(Y, I)$ and $J_X : L^2(X, \ln I) \to S(X, \ln I)$ the RKHS isomorphisms associated with each process. Then $L^2(Y) = L^2(X)$ and for each $g \in S(Y, I)$, $J_X(J_Y^{-1}(g)) = L_H g$.*

The RKHS's associated with stationary processes on semi-infinite index sets can be characterized using spectral factorization and linear time-invariant systems. Applying Theorem 1, we can describe the RKHS's associated with H-ss processes on a variety of index sets, using linear *self-similar* systems.

III. Application to Fractional Brownian Motion

Specializing the general results of the previous section, we characterize the RKHS associated with fractional Brownian motion (fBm) on various index sets, extending results in [8] and [9]. We also give conditions for non-singular discrimination of the usual fBm from the Barnes-Allan fBm.

References

[1] J. Lamperti, "Semi-stable stochastic processes," *Trans. of the AMS*, vol. 104, pp. 62-78, 1962.

[2] G. Wornell, *Synthesis, Analysis, and Processing of Fractal Signals*, Ph.D. thesis, MIT, Cambridge, Mass., October 1991.

[3] B. Yazici and R. L. Kashyap, "A class of second-order stationary self-similar processes for 1/f phenomena," *IEEE Trans. on Sig. Proc.*, vol. 45, pp. 396-410, 1997.

[4] C. J. Nuzman and H. V. Poor, "Linear estimation of self-similar processes via Lamperti's transformation," *J. App. Prob.*, vol. 37, 2000.

[5] C. J. Nuzman and H. V. Poor, "Reproducing Kernel Hilbert Space Methods for Self-Similar Processes," submitted for publication, Nov. 1999.

[6] T. Kailath and H. V. Poor, "Detection of stochastic processes," *IEEE Trans. Inform. Theory*, vol. IT-44, pp. 2230-59, 1998.

[7] E. Parzen, "Statistical inference on time series by RKHS methods," In *12th Biennial Sem. Canadian Math. Cong. Proc.*, pp. 1-37, ed. R. Pyke, Montreal, 1970.

[8] R. J. Barton and H. V. Poor, "Signal detection in fractional Gaussian noise," *IEEE Trans. Inform. Theory*, vol. IT-34, pp. 943-59, 1988.

[9] L. Decreusefond and A. S. Üstünel, "Stochastic analysis of the fractional Brownian motion", *Potential Analysis*, vol. 10, pp. 177-214, 1999.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Analytic Variations on the Redundancy Rate of Renewal Processes

Philippe Flajolet
Project ALGO
INRIA-Rocquencort
F-78153 Le Chesany
FRANCE
Philippe.Flajolet@inria.fr

Wojciech Szpankowski[1]
Department of Computer Science
Purdue University
W. Lafayette, IN 47907
U.S.A.
spa@cs.purdue.edu

The redundancy-rate problem of universal fixed-to-variable length coding for a class of sources consists in determining by how much the actual code length exceeds the optimal (ideal) code length. In a minimax scenario one finds the additional "price" on top of entropy incurred (at least) by any code in order to be able to cope with *all* sources. While Shields [5] proved that there is no function $o(n)$ which is a rate bound on the redundancy for the class of *all ergodic* processes, it has been known for some time (cf. [3]) that, for certain parametric families of sources (e.g., memoryless and Markov sources), the redundancy can be as small as $\Theta(\log n)$ where n is the block length. There was no interesting bound for a class of sources that lies between $\Theta(\log n)$ and general $o(n)$ until recently, when Csiszár and Shields [1] designed a renewal class of sources that yields a $\Theta(\sqrt{n})$ bound. In this paper, we provide a precise asymptotic expansion of the redundancy for renewal sources up to the constant term.

Given a probabilistic source model, we let $P(x_1^n)$ be the probability of the message $x_1^n \in \mathcal{A}^n$. For a given code C_n, we denote by $L(C_n, x_1^n)$ the code length for x_1^n. The *pointwise redundancy* $R_n(C_n, P)$ is defined as $R_n(C_n, P; x_1^n) = L(C_n, x_1^n) + \lg P(x_1^n)$. The (asymptotic) *strong redundancy-rate problem* consists in determining for a class $\mathcal{S}$ of source models the rate of growth of the minimax quantities

$$R_n^*(\mathcal{S}) = \min_{C_n} \sup_{P \in \mathcal{S}} \{\max_{x_1^n} \{R_n(C_n, P; x_1^n)\}\}$$

where supremum is taken over all distributions P.

A substantial literature is available on the redundancy problem. The following results are known:

- If $\mathcal{M}$ is i.i.d. or the class of Markov chains, or more generally the process belongs to a finitely parameterizable class of dimension K, then it was established that $\bar{R}_n(\mathcal{M}) \sim R_n^*(\mathcal{M}) \sim \frac{K}{2} \log n$ (cf. Rissanen [3]).
- Csiszàr and Shields [1] have studied order r Markov renewal sequences in which a 1 is inserted every $T_0, T_1, \ldots$ of 0's, where $\{T_i\}$ is either an i.i.d. or Markov renewal or r-order Markov renewal process. We denote such sources as $\mathcal{R}_r$. The authors of [1] proved that $\bar{R}_n(\mathcal{R}_r) = R^*(\mathcal{R}_r) = \Theta(n^{(r+1)/(r+2)})$ for $r = 1, 2, \ldots$ which specializes to $\Theta(\sqrt{n})$ when $r = 0$.
- Shields [5] proved that there is no function $\rho(n) = o(n)$ which is a weak-rate bound for the class of all ergodic processes.
- Louchard and Szpankowski [2], Savari [4], and Wyner [7] proved that the Lempel-Ziv codes in the class of i.i.d. and Markov processes have either rate $\Theta(n/\log n)$ (for LZ'78) or $\Theta(n \log\log n/\log n)$ (for LZ'77 code).

[1]This work was supported in part by NSF Grants NCR-9415491 and C-CR-9804760, and Purdue Grant GIFG-9919.

We now present our main result and start with a precise definition of the class $\mathcal{R}_0$ of renewal process and its associated sources. Let $T_1, T_2 \ldots$ be a sequence of i.i.d. positive-valued random variables with distribution $Q(j) = \Pr\{T_1 = j\}$. An independent random variable T_0 is introduced with distribution $\Pr\{T_0 = i\} = \mathbf{E}[T_1]^{-1} \sum_{j \geq i} Q(j)$ provided $\mathbf{E}[T_1] < \infty$. The quantities $\{T_i\}_{i=1}^{\infty}$ are the interarrival times, while T_0 is the initial waiting time. The process $T_0, T_0 + T_1, T_0 + T_1 + T_2, \ldots$ is then called a renewal process and it is stationary whenever T_0 has the distribution above. With such a renewal process there is associated a *binary renewal sequence* that is a 0,1-sequence in which the 1's occur exactly at the renewal epochs T_0, $T_0 + T_1$, $T_0 + T_1 + T_2$, etc.

Shtarkov's maximum-likelihood technique [6] implies

$$\log_2 \left(\sum_{x_1^n} \sup_Q P(x_1^n) \right) \leq R_n^*(\mathcal{R}_0) \leq \log_2 \left(\sum_{x_1^n} \sup_Q P(x_1^n) \right) + 1$$

where supremum is taken over all distributions Q. We use this bound to prove our main result.

Theorem 1 *Consider the class $\mathcal{R}_0$ of renewal sources. The the minimax redundancy R_n^* of the renewal process satisfies*

$$R_n^*(\mathcal{R}_0) = \frac{2}{\log 2} \sqrt{\left(\frac{\pi^2}{6} - 1\right) n} - \frac{5}{8} \log_2 n + \frac{1}{2} \log_2 \log n + O(1).$$

for large n.

This result is proved by complex-analytic methods that include generating functions, Mellin transforms, singularity analysis and saddle point estimates. Thus, this work places itself within the framework of analytic information theory.

References

[1] I. Csiszár and P. Shields, Redundancy Rates for Renewal and Other Processes, *IEEE Trans. Information Theory*, 42, 2065–2072, 1996.

[2] G. Louchard and W. Szpankowski, On the Average Redundancy Rate of the Lempel-Ziv Code, *IEEE Trans. Information Theory*, 43, 2–8, 1997.

[3] J. Rissanen, Complexity of Strings in the Class of Markov Sources, *IEEE Trans. Information Theory*, 30, 526–532, 1984

[4] S. Savari, Redundancy of the Lempel-Ziv Incremental Parsing Rule, *IEEE Trans. Information Theory*, 43, 9–21 (1997).

[5] P. Shields, Universal Redundancy Rates Do Not Exist, *IEEE Trans. Information Theory*, 39, 520-524, 1993.

[6] Y. Shtarkov, Universal Sequential Coding of Single Messages, *Problems of Information Transmission*, 23, 175–186, 1987.

[7] A. J. Wyner, The Redundancy and Distribution of the Phrase Lengths of the Fixed-Database Lempel-Ziv Algorithm, *IEEE Trans. Information Theory*, 43, 1439–1465, 1997.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

"Any-time" Capacity and A Separation Theorem For Tracking Unstable Processes

Anant Sahai[1]
MIT LIDS
Cambridge, Massachusetts, 02139
email: sahai@lids.mit.edu

Abstract — **The problem of tracking an exponentially unstable scalar source process across a noisy channel is considered. We introduce the a new parametric notion of capacity that we call "any-time capacity" $C_{\mathbf{at}}(\alpha)$. It is a twist on the familiar concept of error-exponents and is always between the classical Shannon Capacity and the zero-error capacity. A separation theorem is given which shows that $C_{\mathbf{at}}(\alpha)$ characterizes the properties of a channel needed for finite expected distortion.**

I. Introduction

In a sense, the justification of Shannon capacity is the classical source-channel separation theorem and its modern refinements[9]. These tell us that for a wide class of sources, channels, and distortion measures, two-part encodings suffice as long as we are willing to tolerate delays.

Traditional rate-distortion theory[1] has focused almost exclusively on stationary processes. While a broad class, it excludes exponentially unstable processes which are important in practice, especially in control applications[5]. Recently, there has been some work showing how to extend source coding to such processes.([7], [3]) But these have implicitly considered only noiseless channels. For noisy channels, the situation was unclear since the traditional source-channel separation theorem need not (and in fact, does not) apply.

II. Why Classical Separation Fails

Consider the simplest of all unstable processes:

$$X_{t+1} = AX_t + W_t, \quad t \geq 0, A > 1 \tag{1}$$

where $\{X_t\}$ is an $\mathbb{R}$-valued state process and $\{W_t\}$ is a bounded noise process s.t. $\|W_t\| \leq \frac{w}{2}$. Assume $X_0 = 0$ for convenience. This process is non-stationary and has infinite variance as t goes to ∞. Our per-letter distortion measure is the usual $d(X, \hat{X}) = (X - \hat{X})^2$.

$\forall \delta > 0$, sequential rate distortion theory([8], [7]) gives encoders which can track this process with finite expected distortion using $(\log_2 A + \delta)$ bits per sample. They quantize $(X_t - A\hat{X}_{t-1})$ at each time and recursively track the source.

If we attempt to apply the usual separation results, we would pick an $\epsilon > 0$ which $\exists(N, \mathcal{E}_N, \mathcal{D}_N)$ for which $P_e(\mathcal{E}_N, \mathcal{D}_N) < \epsilon$ across a noisy channel. For Shannon Capacity, while this per-bit probability of error can be made arbitrarily small, it can not be made exactly zero. Eventually, a mistake will be made. The effect will be compounded at every subsequent time step since it will get repeatedly multiplied by $A > 1$ in the source decoder's recursion. The expected per-letter distortion will thus tend to infinity with probability one, regardless of how small an ϵ we choose in our channel code!

[1]Work under Prof. Sanjoy Mitter and supported by U.S. Army Grant PAAL03-92-G-0115.

III. "Any-time" Capacity

Definition III.1 *The α-any-time capacity $C_{at}(\alpha)$ of a channel is the maximal rate at which the channel can be used to transmit data with a probability of error that decays to zero with delay at least exponentially at a rate α.*

$$C_{at}(\alpha) = \sup\{R | \exists(\mathcal{E}^R, K), \forall N > 0, \exists \mathcal{D}_N^R, P_e(\mathcal{E}^R, \mathcal{D}_N^R) < K2^{-\alpha N}$$

The above definition is very close to the definition of the reliability function $E(R)$ of a channel given in [2]. The crucial difference is that while we require the encoder to be fixed, in the standard definition of error exponents both the encoder and decoder vary with delay N.

Theorem III.1 *[6] For the AWGN channel with noiseless feedback, $C_{at}(\alpha) = C$ regardless of the value for α.*

Theorem III.2 *[5] For the binary erasure channel with noiseless feedback and probability of erasure e:*

$$C_{at}(\eta - \log_2(1 + (2^\eta - 1)e)) = 1 - \frac{1}{\eta}\log_2(1 + (2^\eta - 1)e)$$

if you let η range over $(0, \infty)$.

Amazingly, [6] shows that α-any-time capacity is also non-zero for these channels even without any feedback!

IV. Separation For Unstable Processes

Theorem IV.1 *The source in (1) can be tracked with finite MSE across a noisy channel iff there is an $\epsilon > 0$ for which $C_{at}(2\log_2 A + \epsilon) > \log_2 A$ for the channel.*

References

[1] T. Berger, *Rate Distortion Theory.* Englewood Cliffs, NJ: Prentice-Hall, 1971.

[2] R. Gallager, *Information Theory and Reliable Communication.* New York, NY: John Wiley and Sons, 1971.

[3] G. Nair and R. Evans, "State Estimation with a Finite Data Rate." Unpublished Report, 1998

[4] A. Sahai, S. Tatikonda, S. Mitter, "Control of LQG Systems Under Communication Constraints." Proceedings of the American Control Conference, 1999.

[5] A. Sahai, "Evaluating Channels for Control: Capacity Reconsidered." Proceedings of the American Control Conference, 2000.

[6] A. Sahai, "Any-time Information Theory." PhD Dissertation in progress.

[7] S. Tatikonda, "Control Under Communication Constraints." PhD Dissertation in progress.

[8] S. Tatikonda, A. Sahai, S. Mitter, "Control of LQG Systems Under Communication Constraints." Proceedings of the 37th IEEE Conference on Decision and Control, 1998.

[9] S. Vembu, S. Verdu, Y. Steinberg, "The Source-Channel Separation Theorem Revisited." IEEE Transactions on Information Theory, Vol. 41, No. 1, pp. 44-54, Jan 1995.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

On an Identification Algorithm of a Markov Chain

Tohru Kohda and Hiroshi Fujisaki
Department of Computer Science
and Communication Engineering,
Kyushu University, Fukuoka 812-8581, Japan
e-mail: kohda@csce.kyushu-u.ac.jp

Abstract **We discuss how to identify a Markov information source with transition matrix P by only observing a sequence of symbols generated by the source.**

I. Introduction

Markov information sources play an important role in modelling subjects to be studied as a stochastic process, for example, blockcipher, speech recognition, recognition of human genes in DNA and so on. Suppose what we can do is only observing a sequence of symbols generated by a Markov source. To identify an N-state simple Markov source with transition matrix P which takes symbols in $\mathcal{S} \in \{1, 2, \cdots, N\}$, it is natural to estimate directly all the elements p_{ij}, $(i, j = 1, 2, \cdots, N)$ in P by using N^2 histograms of possible strings of length 2. However, this method requires too many histograms if the number of states, N becomes large. Since statistics of sequences generated by the Markov source are primarily governed by eigenvalues of P, one of simple ways to identify the source is to estimate eigenvalues of P. In this case, the number of eigenvalues in question is $N-1$. Hence we discuss how to estimate a characteristic polynomial of P by using histograms whose number is in the order of N.

II. Algorithm

The characteristic polynomials of P is expressed as

$$\varphi(P) = (x-1)(x^{N-1} + a_1 x^{N-2} + \cdots + a_{N-1}). \quad (1)$$

Denote an arbitrary string of length m by

$$U = U_0 U_1 \cdots U_{m-1}, \quad U_k \in \mathcal{S}, \quad (k = 0, 1, \cdots, m-1). \quad (2)$$

Next, let

$$u^{(r)} = u_0^{(r)} u_1^{(r)} \cdots u_{m-1}^{(r)} \quad (r = 0, 1, \cdots, N^m - 1) \quad (3)$$

be the r-th string with elements $u_k^{(r)} \in \mathcal{S}$, $(k = 0, 1, \cdots, m-1)$.

Let $\{X_n\}_{n=1}^{\infty}$ $(X_n \in \mathcal{S})$ be a sequence generated by a Markov source. We introduce a binary random variable,

$$Y_n(u^{(r)}) = \begin{cases} 1 & (X_n X_{n+1} \cdots X_{n+m-1} = u^{(r)}) \\ 0 & (X_n X_{n+1} \cdots X_{n+m-1} \neq u^{(r)}) \end{cases} \quad (4)$$

Let

$$M_T(u^{(r)}) = \sum_{n=0}^{T-1} Y_n(u^{(r)}). \quad (5)$$

First choose strings with symmetry such that

$$u_0^{(r)} = u_{m-1}^{(r)}, u_1^{(r)} = u_{m-2}^{(r)}, \cdots, \quad (6)$$

and

$$\forall i \neq j, \quad (i, j = 0, 1, \cdots, \left[\frac{m}{2}\right]) \quad u_i^{(r)} \neq u_j^{(r)}. \quad (7)$$

Next select strings of length m of which all the first symbol u_0 $(u_0 \in \mathcal{S})$ is the same. We denote elements of a class of this specific strings by $u^{(u_0,m)}$. We investigate $2N-2$ histograms of random variables $\frac{1}{L} M_L(u^{(u_0,m)})$, $(m = 1, 2, \cdots, 2N-2)$. Note that p_{u_0} is to be estimated when $m = 1$.

Thus we obtain a nonsymmetric Toeplitz system of equations

$$\begin{bmatrix} A(N-1) & A(N-2) & \cdots & A(1) \\ A(N) & A(N-1) & \cdots & A(2) \\ \vdots & & & \vdots \\ A(2N-3) & A(2N-4) & \cdots & A(N-1) \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_{N-1} \end{bmatrix} = -\begin{bmatrix} A(N) \\ A(N+1) \\ \vdots \\ A(2N-2) \end{bmatrix}, \quad (8)$$

where $A(m)$'s are constants determined by means and variances of $2N-2$ histograms of $\frac{1}{L} M_L(u^{(u_0,m)})$. Note that (8) is like the Wiener-Hopf equation [1]. We remark here that unknown parameters are a_i and eigenvalues of P, $\lambda_i \neq 1$ $(i = 1, 2, \cdots, N-1)$ and hence the number of these is equal to that of different strings of symbols. This implies the above method is based on the minimum number of histograms.

III. Concluding Remarks

Computer simulations are carried out for 2-state Markov chains. Unfortunately experimental estimations of $A(2)$ are not in accordance with theoretical ones because estimating variances of histograms of $\frac{1}{L} M_L(u^{(u_0,2)})$ are not successful.

If we do not use the variances of histograms, the algorithm is to be modified as follows. Denote any strings of length m with $u_0^{(r)} = u_{m-1}^{(r)}$ by $\widehat{u}^{(u_0,m)}$. Means of $2N-2$ histograms of random variables $\frac{1}{L} M_L(\widehat{u}^{(u_0,m)})$ $(m = 1, 2, \cdots, 2N-2)$ give coefficients $\widehat{A}(m)$'s of another Toeplitz system of equations. Computer simulations based on this algorithm are also carried out for 2-state and 3-state Markov chains. The identification of 2-state Markov chains are successful. However , experimental estimations of $\widehat{A}(4)$ are not in accordance with theoretical ones on identification of 3-state Markov chains. Further investigation is needed and problems remain on the algorithm based on the minimum number of histograms.

References

[1] B. Widrow and S. D. Stearns, *Adaptive Signal Processing*, Prentice-Hall, Inc., 1985.

0-7803-5857-0/00/$10.00 ©2000 IEEE.

Author Index

A

Abdel-Ghaffar, K.A.S. 395
Agrawal, Dakshi 365
Agrawal, Dakshi 316
Agrell, Erik 391
Aguila, Raquel 110
Agustini, Edson 58
Ahlswede, Rudolf 390
Ahmed, Mohiuddin 436
Ahmed, Walid K.M. 306
Al-Askary, Omar 87
Alajaji, F. 165
Alajaji, Fady 403
Alajaji, Fady 157
Alatan, Aydin 405
Aleshnikov, I. 168
Alexander, Paul D. 171
Alexander, Paul D. 335
Alouini, Mohamed-Slim 304
Amrani, Ofer 85
Anantharam, Venkat 130
Anantharam, Venkat 466
Anderson, John B. 400
Anderson, John B. 340
Anderson, John B. 343
Andrew, Richard 226
Antonini, Marc 204
Arikan, Erdal 27
Ariyoshi, Masayuki 174
Arnold, Dieter 433
Ashikhmin, A. 458
Ashikhmin, Alexei 275
Atkin, Olivier 140
Aulin, Tor M. 103
Aulin, Tor M. 485
Aulin, Tor M. 90
Aulin, Tor M. 495
Aydinian, H. 390

B

Baccarelli, Enzo 73
Badri, Sabah 101
Baechler, Brice 292
Baicheva, Tsonka 392
Bakin, Maxim 20
Balakirsky, Vladimir 376
Baldini Filho, Renato 259
Baliga, Asha 114
Banerjee, Adrish 188
Barbulescu, Sorin Adrian 123
Barg, Alexander 458
Barg, Alexander 275
Barg, Alexander 1
Barron, Andrew R. 25
Barton, Richard J. 358
Baruch, Anelia 99
Battail, Gérard 202
Bauer, Rainer 238
Bazzi, L. 203
Be'ery, Yair 85
Be'ery, Yair 484
Beaulieu, N.C. 165
Begusic, Dinko 92
Bejjani, Elie 160
Belfiore, Jean-Claude 404
Belfiore, Jean-Claude 362
Belzer, Benjamin J. 222
Benedetto, Sergio 65
Benedetto, Sergio 287
Berger, Tierry P. 195
Berger, Toby 127
Berger, Toby 344
Berry, Randall 409
Bertsekas, Dimitri P. 417
Betsumiya, Koichi 141
Bettesh, Ido 303
Beyer, Gerd 139
Biglieri, Ezio 438
Biglieri, Ezio 379
Biglieri, Ezio 288
Blackmore, Tim 170
Blahut, Richard E. 380
Blinovsky, Volodia 473
Blundo, Carlo 270
Bocharova, Irina E. 341
Bogdanova, Galina T. 142
Bohman, Tom 179
Borah, Deva K. 272
Bose, Bella 190
Bossert, Martin 96
Bossert, Martin 30
Bossert, Martin 94
Bossert, Martin 283
Bossert, Martin 284
Bossert, Martin 95
Bossert, Martin 93
Boutros, Joseph 160
Boutros, Joseph 150
Boyarinov, I. 394
Boyarinov, Igor M. 397
Breiling, Marco 451
Bresler, Yoram 445
Briffa, Johann A. 450
Brink, B. 260
Bross, Shraga I. 38
Bross, Shraga I. 261
Brower, Andreis E. 142
Brown, D.R. 334
Bruck, Jehoshua 489
Buckley, M. Eoin 66
Burnashev, Marat V. 38
Burnashev, Marat V. 442
Burshtein, David 290
Buttigieg, Victor 450
Buzzi, Stefano 355
Buzzi, Stefano 357
Byrne, Eimear 448
Bystrom, Maja 440

C

Cabral, Hermano 230
Cadez, Igor V. 323
Caire, Giuseppe 438
Caire, Giuseppe 406
Cancellieri, Giovanni 65
Canteaut, Anne 213
Canteaut, Anne 183
Cao, Jin 79
Cardinal, Christian 187
Carlach, Jean-Claude 476
Carlet, Claude 183
Cedergren, Andreas 103
Cernuschi-Frías, Bruno 374
Cesa-Bianchi, Nicolò 98
Chamberland, J.-F. 468
Chan, Ho-leung 492
Chande, Vinay 239
Chao, Chi-chao 35
Charpin, Pascale 183
Chen, Brian 46
Chen, C.L. 475
Chen, Chi-Chung 379
Chen, Hongyuan 429
Chen, Houshou 119
Chen, Jia-Pyn 421
Chen, Po-Ning 157
Chen, Po-Ning 227
Chen, Rong 273
Chen, Rong 271
Chen, Rong-Rong 469
Chen, Zhi 197
Chiani, Marco 34
Chiu, Mao-Ching 262
Chkeif, Ammar 362
Chong, Edwin K.P. 382
Chou, Philip A. 43
Chou, Philip A. 176
Chu, Li-chung 336
Chuang, Isaac L. 278
Chung, Habong 299
Chung, Sae-Young 318
Cicalese, Ferdinando 377
Cideciyan, Roy 256

Cioffi, John M. 431
Clarke, W.A. 260
Coffey, John T. 119
Cohen, Aaron 48
Cohen, Gérard 242
Cohen, Gérard 11
Colavolpe, Guilio 322
Collins, Oliver M. 172
Conan, Jean 182
Concha, Julio I. 276
Conte, Ernesto 84
Conti, A. 34
Cozzo, Carmela 338
Costa, Sueli I.R. 58
Costello Jr., Daniel J. 122
Costello Jr., Daniel J. 172
Costello Jr., Daniel J. 188
Costello Jr., Daniel J. 326
Costello Jr., Daniel J. 230
Costello Jr., Daniel J. 220
Cover, Tom 232
Cox, R.V. 266
Csibi, Sándor 105
Csiszár, Imre 490
Csiszár, Imre 26

D

da Rocha Jr., Valdemar C. 241
D'Arco, Paolo 270
Damen, Oussama 362
Danev, Danyo 198
Danon, Tamar 261
Das, Arnab 349
Das, Arnab 432
Das, Deepak 247
Datta, Suparna 146
Davey, Matthew C. 477
Davis, Drew 79
De Bonis, Annalisa 49
de Lind van Wijngaarden 40
De Maio, Antonio 84
Deolalikar, V. 168
Derakhtian, Mostafa 388
Desmedt, Yvo 464
Dholakia, Ajay 293
Di Blasio, G. 73
Dieterich, Hans 93
Diggavi, Suhas 52
Dinh, The Cuong 251
Dinis, Rui 216
Divsalar, Dariush 410
Divsalar, Dariush 459
Divsalar, Dariush 288
Divsalar, Dariush 194
Dobbertin, Hans 329
Dolinar, Sam 410
Dolinar, Sam 459
Dolinar, Sam 428
Dolinar, Sam 194
Duel-Hallen, Alexandra 159
Duman, Tolga M. 258
Dumer, Ilya 63
Dumer, Ilya 89
Dumer, Ilya 252
Durand, Céline 160
D'yachkov, Arkadii 330

E

Effros, Michelle 208
Effros, Michelle 487
Egner, Sebastian 368
Ekstrand, Nicklas 72
El Gamal, Hesham 319
El Gamal, Hesham 339
Eleftheriadis, Alexandros 206
Eleftheriou, Evangelos 256
Elwalid, Anwar 78
Engdahl, K. 201
Engdahl, Karin 139
Eppstein, David 148
Eriksson, Svante 90
Etzion, Tuvi 311
Evans, Jamie S. 441

F

Fabre, Eric 10
Fagnani, Fabio 33
Fain, Eric A. 416
Fair, Ivan J. 381
Farrell, P.G. 29
Farvardin, Nariman 239
Fasano, A. 73
Feder, Meir 126
Feder, Meir 81
Feder, Meir 23
Fedotov, Alexey 13
Feng, Gui-Liang 32
Feng, Hanying 487
Ferrari, Gianluigi 322
Ferreira, H.C. 6
Ferreira, H.C. 260
Fierens, Pablo 80
Fine, Terrence L. 80
Finesso, Lorenzo 111
Fingscheidt, T. 266
Fionov, Andrei 354
Fisher, R.F.H. 136
Fitz, Michael P. 336
Fitz, Michael P. 314
Fitzi, Matthias 267
Fitzpatrick, Patrick 448
Fitzpatrick, Patrick 196
Flajolet, Philippe 499
Flajolet, Philippe 296
Fleming, Michael 208
Fleury, Gilles 443
Foltz, Kevin 489
Fontaine, Caroline 183
Forchhammer, Soren 282
Forney Jr., G. David 9
Fossorier, Marc P.C. 200
Fossorier, Marc P.C. 248
Fossorier, Marc P.C. 367
Fossorier, Marc P.C. 342
Fossorier, Marc P.C. 64
Fossorier, Marc P.C. 214
Foster, Dean 325
Freudenberger, J. 94
Freudenberger, Jürgen 95
Frey, Brendan J. 249
Frey, Brendan J. 121
Fu, Fang-Wei 209
Fuja, Thomas E. 264
Fuja, Thomas E. 188
Fujisaki, Hiroshi 501
Fujisawa, Masaya 479
Fujiwara, Chikato 399
Fujiwara, Eiji 8
Fujiwara, Eiji 429
Fujiwara, Toru 463
Fujiwara, Toru 225

G

Gabidulin, Ernst M. 115
Gabidulin, Ernst M. 283
Gabidulin, Ernst M. 284
Gaborit, Philippe 140
Gagnon, François 187
Gagnon, François 292
Gallager, Robert G. 22
Gallager, Robert G. 461
Gallager, Robert G. 409
Galli, Stefano 82
Gameiro, A. 134
Ganesan, Ashwin 161
García Fernández, E.M. 259
Garcia-Frias, Javier 67
Garello, Roberto 65
Garello, Roberto 287
Gastpar, Michael 236
Gastpar, Michael 445
Ge, Xian-ping 148
Geng, Jifeng 336
Georghiades, Costas N. 315
Georghiades, Costas N. 55
Ghazaryan, A.R. 211
Giles, James R. 51
Gill, John 372
Giraud, Xavier 404
Gluesing-Luerssen, Heide 294
Gober, Peter 39
Goldsmith, Andrea J. 193
Goldsmith, Andrea J. 407
Goldsmith, Andrea J. 305
Golin, Mordecai J. 280

Golomb, Solomon W. 300
Gong, Guang 300
Gong, Xiaohong 246
Gorokhov, Alexei 411
Görtz, Norbert 173
Goyal, Vivek K. 207
Grant, Alex J. 171
Grassl, Markus 253
Grossglauser, Matthias 52
Guess, Tommy 102
Guidi, Andrew 123
Gulliver, T. Aaron 141
Gulliver, T. Aaron 88
Guo, Dongning 332
Gupta, P. 434
Gusmão, António 216
Guyader, Arnaud 10
Györfi, Lászlò 28

H

Haccoun, David 187
Haccoun, David 292
Hadjicostis, Christoforos 444
Haering, Juergen 137
Hagenauer, Joachim 238
Hagenauer, Joachim 425
Hagenauer, Joachim 228
Hagenauer, Joachim 422
Hagenauer, Joachim 66
Hajek, Bruce 51
Hallen, Hans 159
Hamada, Mitsuru 189
Hamasuna, Yuuichi 59
Hamkins, J. 410
Hammons Jr., A. Roger 319
Hammons Jr., A. Roger 339
Han, Te Sun 42
Han, Te Sun 454
Han, Yunghsiang S. 227
Handlery, Marc 340
Hanly, Stephen V. 467
Hansson, Anders 495
Harada, Masaaki 141
Haroutunian, E.A. 211
Haroutunian, Evgueni 205
Harutyunyan, A.N. 211
Harutyunyan, Ashot N. 205
Hashimoto, Takeshi 229
Hashimoto, Takeshi 210
Hashimoto, Takeshi 251
Haslach, Christoph 149
Hassan, Amer 497
Hassan, Amer 268
Hassibi, Babak 337
Hassibi, Babak 313
Hata, Masayasu 59
Hatano, Atsushi 401
Heegard, Chris 131
Heinen, Stefan 265
Helleseth, Tor 299
Helleseth, Tor 328
Helleseth, Tor 329
Hermoso-Carazo, Aurora 110
Hero, Alfred O. 363
Hero, Alfred O. 414
Hindelang, Thomas 266
Hirano, Norimichi 309
Hirasawa, Shigeichi 231
Hirasawa, Shigeichi 155
Hirasawa, Shigeichi 44
Hirota, O. 277
Hochwald, Bertrand 337
Hochwald, Bertrand 313
Hoeher, Peter 415
Hoeher, Peter 101
Hoeholdt, Tom 480
Holevo, A.S. 277
Honary, B. 394
Honary, Bahram 115
Hong, Dae-Sik 192
Honig, Michael H. 385
Honig, Michael L. 335
Honkala, Iiro 393
Honkala, Iiro 11
Honkala, Iiro 254
Hons, Erik S. 249
Horadam, K.J. 31
Hoshi, Mamoru 15
Höst, Stefan 96
Hu, Shengquan 159
Hu, Zhengming 301
Huang, G. 315
Huang, Howard 286
Huang, Jianguo 233
Huang, Jianyi 407
Huber, Johannes B. 451
Huber, Johannes B. 136
Hughes, Brian L. 383
Hughes, Brian L. 285
Hughes, Brian L. 338

I

Imai, Hideki 462
Imai, Hideki 219
Imai, Hideki 138
Imai, Hideki 214
Immink, K.A. Schouhamer 144
Immink, K.A. Schouhamer 352
Isaka, Motohiko 138
Ito, Hisashi 281
Iwata, Ken-ichi 156
Izzo, Luciano 361

J

Jacquet, Philippe 181
Janssen, Augustus J.E.M. 144
Ji, Chuanyi 78
Jia, Yunwei 16
Jin, Hui 120
Jin, Hui 459
Johannesson, Rolf 343
Johannesson, Rolf 341
Johannesson, Rolf 96
Johannesson, Rolf 398
Johansson, Thomas 212
Johansson, Thomas 184
Johnson, Don H. 493
Johnson Jr., C.R. 334
Joly, Véronique 181
Jones, Douglas L. 166
Jönsson, Frederik 212
Jordan, Ralph 96
Jordan, Ralph 95
Julian, David 232
Justesen, Jørn 289
Justesen, Jørn 480

K

Kabatianski, Gregory 375
Kaji, Yuichi 424
Kaltchenko, A. 298
Kamabe, Hiroshi 308
Kanaya, Fumio 457
Kaneko, Haruhiko 8
Kang, Chang-Eon 192
Kapralov, Stoian N. 142
Karakos, Damianos 47
Karlof, John 57
Kasami, Tadao 424
Kasami, Tadao 396
Kashyap, Navin 427
Katayama, Yasunao 449
Kato, Akiko 279
Kato, Akiko 281
Kavcic, Aleksandar 433
Kawabata, Tsutomu 152
Kawasaki, Shuhji 470
Kawasaki, Zenshiro 401
Kaya, Munevver 482
Kazakov, Peter S. 224
Khachatrian, L. 390
Khandani, Amir K. 249
Khandani, Amir K. 86
Khosravifard, S.M. 345
Kieffer, John C. 295
Kieffer, John C. 296
Kieffer, John C. 298
Kiely, Aaron 428
Kim, Hyun Cheol 369
Kim, Saejoon 12
Kim, Sungill 402
Kim, Woong-Gon 192
Kitakami, Masoto 429
Klapper, Andrew 393
Klein, Thierry 461

Klimesh, Matthew 428
Knill, Emanuel 275
Ko, Young-Chai 304
Kobayashi, Kingo 15
Koga, Hiroki 158
Koga, Hiroki 346
Kogo, Naoto 309
Kohda, Tohru 501
Kohno, Ryuji 309
Koorapaty, Havish 268
Koppelaar, Arie 368
Korjik, Valeri 20
Kötter, Ralf 433
Kötter, Ralf 76
Kötter, Ralf 61
Kötter, Ralf 100
Kötter, Ralf 178
Kou, Yu 200
Koulgi, Prashant 177
Koumoto, Takuya 396
Kramer, Gerhard 40
Kramer, Gerhard 350
Krichevskiy, Rafail 89
Krishnamachari, Bhaskar 66
Krzyzak, Adam 360
Ku, Bon-Jin 192
Kuai, H. 165
Kudryashov, Boris D. 341
Kuh, Anthony 246
Kuijper, Margreet 418
Kukorelly, Zsolt 14
Kulkarni, S. 53
Kulkarni, S.R. 321
Kumar, P. Vijay 168
Kumar, P. Vijay 328
Kumar, P. Vijay 329
Kumar, P.R. 434
Kurosawa, Kaoru 464
Kurtas, Erozan 258
Kutoyants, Yury 442
Kwok, Henry K. 166

L

Lahalle, Élisabeth 443
Lahtonen, Jyrki 446
Laihonen, Tero 254
Lally, Kristine 196
Lampe, Alexander 333
Lampe, Lutz H.-J. 136
Land, Ingmar 415
Langevin, Philippe 167
Lapidoth, Amos 48
Lapidoth, Amos 460
Lastras, Luis 127
Lau, Francis C.M. 162
Laybourn, Loren E. 380
Le Ruyet, Didier 452
Lebedev, V.S. 375
Leduc, Jean-Pierre 108
Lee, Jung-Do 299
Lee, Moon Ho 471
Lee, Pil Joong 369
Lee, Tzong-Yow 227
Lee, Wee Sun 41
Lentmaier, M. 201
Levenshtein, Vladimir I. 486
Li, Lifang 305
Li, Xiaodong 286
Li, Xin 301
Li, Xin 113
Li, Youjian 315
Liang, Cheng-Po 191
Lim, Jongtae 237
Lim, Teng Joon 387
Lin, Shu 117
Lin, Shu 200
Lin, Shu 248
Lin, Shu 367
Lin, Shu 342
Lin, Shu 64
Linarez-Pérez, Josefa 110
Linder, Tamás 125
Linder, Tamás 151
Litsyn, Simon 458
Litsyn, Simon 275
Litsyn, Simon 242
Liu, Guodong 57
Liu, Juan 54
Liu, Jun S. 271
Liu, Ye 367
Liu, Youjian 314
Lobstein, Antoine 11
Loeliger, H.-A. 433
Loidreau, Pierre 186
Lops, Marco 355
Lops, Marco 357
Loyer, P. 204
Lu, Chung-Chin 421
Lugosi, Gábor 125
Lugosi, Gábor 98
Lund, David 115
Lusina, Paul 283
Lusina, Paul 284

M

MacKay, David J.C. 477
MacKay, David J.C. 121
Macula, Antony J. 3
Madhow, Upamanyu 312
Madhow, Upamanyu 76
Madhow, Upamanyu 469
Maeda, Masaya 225
Mallik, Ranjan K. 412
Mallik, Ranjan K. 56
Malyutov, M.B. 386
Marcus, Brian H. 147
Martin, I. 394
Martinsen, H. Movik 328
Martinsen, H. Movik 329
Marzetta, Thomas L. 363
Marzetta, Thomas L. 129
Marzetta, Thomas L. 313
Massey, James L. 398
Massey, James L. 241
Massey, Peter 122
Masucci, Barbara 49
Matache, Adina 428
Matsushima, Toshiyasu 155
Matsushima, Toshiyasu 44
Matsushima, Toshiyasu 231
Matús, Frantisek 490
Maucher, J. 30
Maurer, Ueli 18
Maurer, Ueli 267
Maurer, Ueli 243
McCloud, Michael L. 356
McCloud, Michael L. 163
McEliece, Robert J. 120
McEliece, Robert J. 459
McEwen, Peter 291
McLane, Peter J. 306
McLaughlin, Steven W. 146
Mecking, Michael 494
Médard, Muriel 413
Médard, Muriel 407
Mehrotra, Sanjeev 176
Merhav, Neri 97
Merhav, Neri 99
Merhav, Neri 70
Merhav, Neri 45
Metzner, John J. 481
Mevel, Laurent 111
Meyn, Sean P. 77
Meyn, Sean P. 407
Micciancio, Daniele 252
Michel, Olivier J.J. 414
Middleton, David 104
Mihaljevic, Miodrag J. 214
Miller, Gadi 290
Ming, Michael Yip 162
Miri, S.A. 86
Mitra, Urbashi 336
Mittal, Udar 24
Mittelholzer, Thomas 116
Miyoshino, Kenji 59
Modestino, J.W. 440
Modha, Dharmendra S. 278
Modha, Dharmendra S. 147
Moision, Bruce E. 145
Mokhtar, Ahmed 497
Monico, Chris 215
Montorsi, Guido 65
Montorsi, Guido 287
Moqvist, Pr 485
Morelos-Zaragoza, R.H. 138
Morelos-Zaragoza, R.H. 218
Morioka, Sumio 449

Morita, Hiroyoshi 347
Morita, Hiroyoshi 456
Morita, Hiroyoshi 15
Morita, Hiroyoshi 470
Morvai, G. 28
Mörz, Matthias 425
Motani, M. 334
Motani, Mehul 131
Motwani, Ravi 368
Moulin, Pierre 19
Moulin, Pierre 54
Moureaux, J.M. 204
Müller, Ralf R. 439
Mundici, Daniele 377
Munemasa, Akihiro 141
Muniz, Marcelo 58
Murad, Ahsun H. 264
Muramatsu, Jun 327

N

Nagy, Zsigmond 180
Nagy, Zsigmond 281
Napolitano, Antonio 361
Narayan, Prakash 349
Nasiri-Kenari, M. 345
Navarro-Moreno, Jesùs 389
Nayebi, Mohammad M. 388
Nebe, G. 453
Nekritch, Yakov 371
Neuhoff, David L. 427
Neuhoff, David L. 402
Neuhoff, David L. 237
Neves Barroso, Victor 244
Nguyen, Ha Hoang 378
Ni, Jian-Jun 358
Nielsen, Rasmus R. 112
Niinomi, Toshihiro 231
Nikov, Ventsislav 60
Nikova, Svetla 60
Nishiara, Mikihiko 347
No, Jong-Seon 299
No, Jong-Seon 472
Nomura, Ryo 44
Norton, Graham 170
Numakami, Yukio 479
Nuzman, Carl J. 498

O

O'Sullivan, Joseph A. 320
O'Sullivan, Joseph A. 19
O'Sullivan, Joseph A. 491
Ochiai, Hideki 219
Offer, Elke 425
Offer, Elke 423
Oka, Ikuo 399
Oksman, Jacques 443
Olsson, Jonas 198
Oohama, Yasutada 455
Ordentlich, Erik 70
Ordentlich, Erik 297
Orlitsky, Alon 154
Orlitsky, Alon 145
Östergard, Patric 142
Otmani, Ayoub 476
Oya, Antonia 389

P

Palazzo Jr., Reginaldo 58
Papadias, C.B. 245
Papadopoulos, H. C. 435
Papamarcou, Adrian 47
Parker, Matthew G. 302
Parkvall, Stefan 74
Pasalic, Enes 184
Patapoutian, Ara 291
Paterson, Kenneth G. 217
Paulraj, Arogyaswami 496
Pavlouchkov, Viktor 95
Pawlak, Miroslav 360
Peeters, Stein 451
Pellenz, Marcello E. 221
Peng, Xiao-Hong 29
Petropulu, Athina 104
Phamdo, Nam 403
Phamdo, Nam 24
Phamdo, Nam 68
Pierleoni, Paola 287
Pietrobon, Steven S. 123
Pimentel, Cecilio 36
Pinsker, M.S. 359
Pinsker, M.S. 488
Pless, Vera 140
Pollara, F. 410
Pollara, F. 194
Ponnampalam, Vishakan 62
Poor, H. Vincent 276
Poor, H. Vincent 498
Poor, H. Vincent 384
Poor, H. Vincent 334
Portugheis, Jaime 221
Pottie, Gregory 436
Pradhan, S. Sandeep 351
Pradhan, S. Sandeep 178
Prelov, V.V. 488
Prelov, Vyacheslav V. 359
Pursley, Michael B. 109

R

Rafajlowicz, Ewaryst 360
Raheli, Ricardo 322
Rajan, B. Sundar 75
Rajan, B. Sundar 118
Ramchandran, Kannan 351
Ramchandran, Kannan 178
Rankin, D. 88
Ranto, Kalle 447
Rao, T.R.N. 32
Rapajic, Predrag 272
Rasmussen, Lars K. 332
Rasmussen, Lars K. 387
Ratasuk, Rapeepat 385
Reddy, V. Umapathi 75
Regunathan, Shankar L. 177
Rhee, Dojun 7
Rhee, Dojun 218
Ricci, Giuseppe 84
Ricci, Giuseppe 357
Richardson, Tom J. 317
Richardson, Tom J. 199
Richardson, Tom J. 318
Richardson, Tom J. 203
Richardson, Tom J. 365
Rimoldi, Bixio 236
Risley, Allen 222
Rissanen, Jorma 324
Rodriguez-Guisantes, J. 404
Roessing, Cornelia 331
Rose, Kenneth 234
Rose, Kenneth 177
Rosenthal, Joachim 294
Rosenthal, Joachim 215
Roth, Ron M. 307
Rozic, Nikola 92
Ruiz-Molina, Juan Carlos 389
Ruszinkó, Miklós 179
Ryabko, Boris 240
Ryabko, Boris 13
Ryabko, Boris 71

S

Sadjadpour, Hamid R. 453
Sahai, Anant 500
Sakaniwa, Kohichi 169
Sakata, Shojiro 479
Salehi, M. 453
Sampath, Hemanth 496
Sandilya, Sathyakarma 321
Saowapa, Kiattichai 8
Sarkar, Sandip 133
Sarkar, Saswati 107
Sarwate, Dilip V. 419
Sarwate, Dilip V. 132
Sasase, Iwao 174
Sayeed, Akbar M. 161
Sayir, Jossy 235
Schaathun, Hans Georg 255
Schaefer, Andrew 422
Scharf, Louis L. 356
Schein, Brett 22
Schlegel, Christian 274
Schmid, Natalia A. 320
Schnug, Walter 96
Schnug, Walter 93
Sella, Assaf 484

Seroussi, Gadiel 70
Seroussi, Gadiel 297
Servetto, Sergio 175
Seshadri, N. 266
Shabunov, Kirill 63
Shalmon, Michael 106
Shamai (Shitz), Shlomo 38
Shamai (Shitz), Shlomo 128
Shamai (Shitz), Shlomo 129
Shamai (Shitz), Shlomo 303
Shamir, Gil 326
Shanbhag, Naresh R. 419
Shao, Rose Y. 117
Shao, Rose Y. 342
Shashidhar, V. 75
Shavgulidze, S. 94
Shavgulidze, Sergo 93
Shea, John M. 109
Shen, Ba-Zhong 291
Shen, Jia-Pei 372
Sheng, Li 280
Shi, Wei 437
Shibuya, Ryujiro 424
Shibuya, Tomoharu 169
Shields, Paul C. 26
Shokrollahi, Amin 5
Shokrollahi, Amin 337
Shokrollahi, Amin 199
Shokrollahi, Amin 215
Shulman, Nadav 23
Shum, K. 168
Shwedyk, E. 378
Sidel'nikov, Vladimir 164
Sidorenko, Vladimir 30
Siegel, Paul H. 307
Siegel, Paul H. 478
Siegel, Paul H. 145
Simon, Marvin K. 304
Sinanovic, Sinan 493
Singer, Andrew C. 81
Singer, Andrew C. 100
Skoglund, Mikael 403
Skoglund, Mikael 74
Sloane, N.J.A. 453
Sloane, N.J.A. 175
Smarandache, Roxana 294
Smeets, Ben 72
Smyth, Padhraic 323
Smyth, Padhraic 148
Soljanin, Emina 423
Soljanin, Emina 257
Solé, Patrick 140
Solé, Patrick 167
Song, Hong-Yeop 472
Song, Hong-Yeop 299
Song, Lihua 21
Song, Young Joon 353
Sorger, Ulrich 415
Sow, Daby 206
Spasojević, Predrag 55
Srikant, R. 413
Stahl, Per 343
Stahl, Per 341
Stahl, Per 398
Stark, Wayne E. 191
Steinberg, Yossef 45
Stichtenoth, H. 168
Stine, Robert 325
Stites, Ross 295
Stockhammer, Thomas 228
Stojanović, Diana 248
Storn, Rainer 5
Stüber, Gordon L. 483
Sudan, Madhu 252
Sun, Hong 452
Sun, Thomas W. 437
Sun, Wei 301
Sun, Wei 113
Sundaresan, Rajesh 50
Svanström, Mattias 143
Swart, T.G. 6
Sweldens, Wim 337
Szpankowski, Wojciech 499
Szpankowski, Wojciech 370

T

Tajima, Masato 401
Takahara, Glen 165
Takeshita, Oscar Y. 122
Takeshita, Oscar Y. 172
Takeshita, Oscar Y. 314
Takida, Keiji 401
Takumi, Ichi 59
Tallini, Luca 190
Tamm, Ulrich 4
Tan, Jun 483
Tan, Peng Hui 387
Tanda, Mario 384
Tang, Heng 367
Tarannikov, Yuriy 185
Taricco, Giorgio 438
Tarokh, Vahid 217
Tassiulas, Leandros 107
Telatar, Emre 460
Thien, Han Vu 452
Thoma, Lubos 179
Thorpe, J. 375
Tilborg, Henk van 269
Tjalkens, Tjalling 373
Tokushige, Hitoshi 396
Tolhuizen, Ludo 37
Topsoe, Flemming 71
Torney, David 330
Trabbia, Michaël 213
Tralli, V. 34
Truhachev, D.V. 201
Tse, David N.C. 364
Tse, David N.C. 467
Tse, David N.C. 466
Tse, David N.C. 382
Tsitovich, I.I. 386
Tüchler, Michael 100
Tulino, Antonia Maria 355
Tuncel, Ertem 234
Tuninetti, Daniela 406
Tyczka, Piotr 223

U

Uchida, Osamu 42
Uchida, Osamu 454
Udaya, Parampalli 420
Udaya, Parampalli 420
Urbanke, Rüdiger 317
Urbanke, Rüdiger 199
Urbanke, Rüdiger 318
Urbanke, Rüdiger 203
Urbanke, Rüdiger 365
Uyematsu, Tomohiko 457

V

Vaccaro, Ugo 377
Vaishampayan, Vinay A. 175
Vajda, Igor 28
Valembois, Antoine 91
van der Meulen, E.C. 488
van der Meulen, E.C. 211
van Dijk, Marten 368
Vander Wiel, Scott 79
Varanasi, Mahesh K. 416
Varanasi, Mahesh K. 163
Varanasi, Mahesh K. 247
Varanasi, Mahesh K. 102
Vardy, Alexander 391
Vardy, Alexander 61
Vardy, Alexander 316
Vardy, Alexander 311
Vary, Peter 265
Vasil'eva, Anastasia Yu. 474
Veeravalli, Venugopal V. 468
Veeravalli, Venugopal V. 131
Verdù, Sergio 439
Verdù, Sergio 53
Verghese, G.C. 444
Vervoux, Cyril 476
Vetterli, Martin 236
Vialle, Sandrine 150
Vijayakumar, Rajiv 408
Vilenkin, Pavel A. 330
Vilenkin, Pavel A. 3
Villasenor, John D. 67
Vinck, A.J. Han 149
Vinck, A.J. Han 137
Vinck, Han 263
Vishwanath, Sriram 193
Visotsky, Eugene 312
Viswanath, G. 118

Viswanath, Pramod 130
Viswanath, Pramod 466
Viswanathan, Harish 286
Viswanathan, Harish 153
Visweswariah, K. 53
Viterbi, Andrew J. 366
Viterbi, Audrey M. 366
Viterbo, Emanuele 438
Vontobel, Pascal O. 433
Voronov, German 126
Vrdoljak, M. 92
Vucetic, Branka 62

W

Wadayama, Tadashi 263
Wadayama, Tadashi 137
Wan, Zhe-Xian 2
Wang, Chung-Hsuan 35
Wang, Heng-Shun 421
Wang, Qi 250
Wang, Xiaodong 273
Wang, Xiaodong 271
Warrier, Dilip 76
Wasserman, Kimberly M. 408
Watanabe, Yyuji 462
Weber, Jos 395
Weeks IV, William 310
Wei, Lei 250
Weinberger, Marcelo J. 70
Weinberger, Marcelo J. 297
Weiss, Christian 228
Weiss, Christian 422
Weissman, Tsachy 97
Wesel, Richard 437
White, Gregory S. 220
White, P. Scott 330
Whiting, Philip A. 430
Wicker, Stephen B. 66
Wicker, Stephen B. 12
Willems, Frans M.J. 348
Wilson, Stephen G. 482
Wilson, Stephen G. 223
Wilson, Wang Yong Hong 352
Win, Moe Z. 412
Wintzell, Ola 135
Wolf, Jack K. 307
Wolf, Stefan 18
Wolf, Stefan 17
Wolf, Stefan 465
Woods, John W. 405
Woodward, Graeme 335
Wornell, Gregory W. 46
Wu, Xiaolin 43
Wu, Xin-Wen 32
Wu, Xin-Wen 478
Wyner, Abraham 325

X

Xavier, João 244
Xin, Yan 381
Xu, Sheng-bo 269
Xue, Xiaohui 43

Y

Yamaguchi, Eisaku 59
Yamaguchi, Naoto 346
Yamamoto, Hirosuke 346
Yan, Ying-On 344
Yan, Zhiyuan 132
Yang, En-Hui 296
Yang, En-Hui 295
Yang, En-Hui 16
Yang, En-Hui 298
Yang, Ha-Young 192
Yang, Kyeongcheol 299
Yang, Xueshi 104
Yang, Yixian 301
Yang, Yixian 113
Yao, K. 379
Ye, Chunxuan 426
Ye, Zhongxing 233
Yeh, Edmund 430
Yeung, Raymond W. 21
Yeung, Raymond W. 492
Yeung, Raymond W. 426
Yeung, Raymond W. 209
Yong, Xuerong 280
Yoshida, Maki 463
Yoshida, Takahiro 155
Yoshida, Takuya 464
Yoshikawa, Hideki 399
Yousefi, Shahram 249
Yu, Bin 79
Yu, Wei 431

Z

Zamir, Ram 124
Zamir, Ram 153
Zampieri, Sandro 33
Zeevi, Assaf J. 83
Zeger, Kenneth 391
Zeger, Kenneth 279
Zeger, Kenneth 180
Zeger, Kenneth 281
Zémor, Gilles 11
Zémor, Gilles 242
Zhang, Jianqiu 68
Zhang, Junshan 382
Zhang, Yuanping 280
Zhang, Zhengtao 301
Zhang, Zhengtao 113
Zheng, Lizhong 364
Zheng, Yuliang 462
Zhu, Yathian 222
Zigangirov, Dimitri K. 135
Zigangirov, Kamil Sh. 139
Zigangirov, Kamil Sh. 201
Zigangirov, Kamil Sh. 135
Ziv, Jacob 69
Zucchi, A. 73
Zyablov, Viktor 96
Zyablov, Viktor 94
Zyablov, Viktor 95