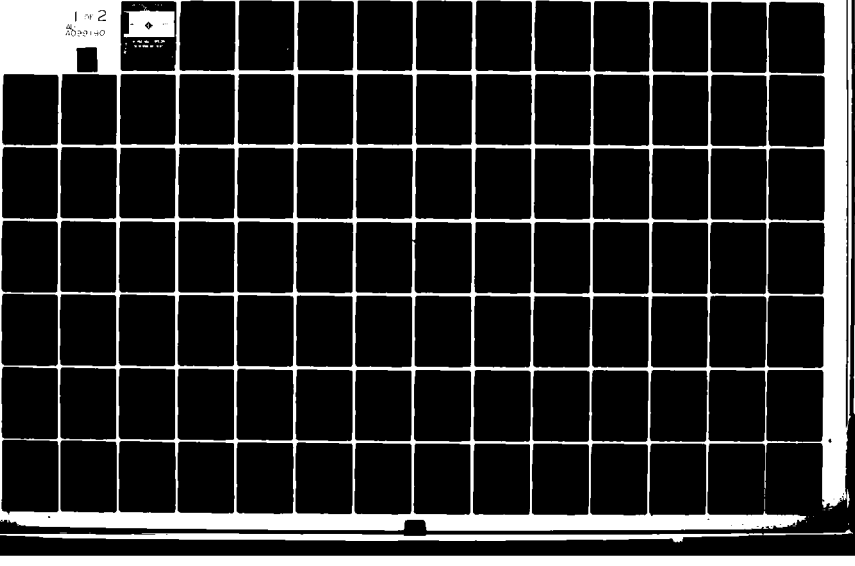
AD-A099 190 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS INC--ETC F/G 9/4
IEEE INTERNATIONAL SYMPOSIUM INFORMATION THEORY, HELD AT SANTA --ETC(U)
1981 I RUBIN, K YAO AFOSR-81-0032

UNCLASSIFIED AFOSR-TR-81-0454 NL



AFOSR-TR-81-0454

ABSTRACTS OF PAPERS

LEVEL II 3

AD A099190

1981

IEEE

DTIC FILE COPY

INTERNATIONAL SYMPOSIUM ON INFORMATION THEORY

AFOSR-81-0032

February 9-12, 1981

Santa Monica
California, USA

DTIC ELECTE MAY 20 1981 S A

SPONSORED BY: IEEE INFORMATION THEORY GROUP

CO-SPONSORED BY: UNION RADIO SCIENTIFIQUE INTERNATIONALE

IEEE Catalog Number 81 CH 1609-7 IT

81 5 20 046

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER AFOSR-TR- 81-0454	2. GOVT ACCESSION NO. AD-A099	3. RECIPIENT'S CATALOG NUMBER 190
4. TITLE (and Subtitle) 1981 IEEE International Symposium on Information Theory		5. TYPE OF REPORT & PERIOD COVERED Final 6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) Professors Izhak Rubin and Kung Yao, Co-Chairmen, Department of System Science, University of California, Los Angeles, CA 90024		8. CONTRACT OR GRANT NUMBER(s) AFOSR-81-0032
9. PERFORMING ORGANIZATION NAME AND ADDRESS IEEE, Inc. 345 East 47th Street New York, NY 10017		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS 61102F 2304/AG
11. CONTROLLING OFFICE NAME AND ADDRESS AFOSR NM Bolling AFB Washington, D.C. 20332		12. REPORT DATE Feb. 9-12, 1981 13. NUMBER OF PAGES 152
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)		15. SECURITY CLASS. (of this report) Unclassified 15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

1981 IEEE International Symposium on Information Theory
February 9-12, 1981, Santa Monica California, USA

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Information Theory, Communications, Stochastic Processes, Communication Networks, Coding, Radar, Cryptography, Pattern Recognition, Image Processing, Speech Compression, Complexity, Estimation, Detection

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

This book contains the abstracts of papers presented at the 1981 IEEE International Symposium on Information Theory, Feb. 9-12, 1981, at Santa Monica, California. Papers encompass the following areas: information theory, communications, stochastic processes, communicaiton networks, coding, radar, cryptography, pattern-recognition, image-processing, speech compression, complexity, estimation, detection.

DD FORM 1 JAN 73 1473

Unclassified

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

1981 IEEE INTERNATIONAL SYMPOSIUM ON INFORMATION THEORY

SANTA MONICA, CALIFORNIA, ~~USA~~
FEBRUARY 9-12, 1981

Sponsored by:
The Institute of Electrical and Electronics Engineers,
Information Theory Group

Co-sponsored by:
Union Radio Scientifique Internationale

Co-Chairmen:
I. Rubin and K. Yao
Vice-Chairman
N.J.A. Sloane

International Advisory Committee:

A. Gersho (Chairman; USA)
R. Ahlswede (West Germany)
S. Arimoto (Japan)
I. Bar David (Israel)
P. Bergmans (Belgium)
E. Biglieri (Italy)
I. Blake (Cananda)
A. Carleial (Brazil)
I. Csiszar (Hungary)
J. Delgado-Penin (Spain)
A. Perez (Czechoslovakia)
B.C. Picinbono (France)
A.N. Protonotarios (Greece)
J.P.M. Schalkwijk (The Netherlands)
B. Tsybakov (USSR)
G. Ungerboeck (Switzerland)
L.H. Zetterberg (Sweden)

Program Committee:

R.A. Scholtz (Chairman)
T.M. Cover
A.A. El Gamal
R.M. Gray
L. Kleinrock
E. Masry
J.K. Omura
I.B. Rhodes
A.J. Viterbi
C.L. Weber
L.R. Welch

Committee Chairmen:

Finance: L. Biederman
Local Arrangements: J.R. Lesh
Publications: L.B. Milstein
Publicity: L.M. Nirenberg
Registration: H.H. Tan

IEEE Catalog Number 81CH 1609-7 IT

Library of Congress No. 72-179437

Approved for public release;
distribution unlimited.

ACKNOWLEDGMENTS

We wish to acknowledge the support of the Air Force Office of Scientific Research.

Copyright © 1981 by the Institute of Electrical and Electronics Engineers, Inc., 345 East 47th Street, New York, New York 10017

Manufactured in the United States of America.

Library of Congress Catalog Card Number: 72-179437

PROGRAM SCHEDULE

SUNDAY, FEBRUARY 8, 1981

5:00 PM - 8:00 PM	Registration
6:00 PM - 7:00 PM	Complimentary Cocktail Party

MONDAY, FEBRUARY 9, 1981

Morning:

9:00 AM	A1: Stochastic Processes I A2: Multi-User Information Theory I A3: Communication Systems I A4: Radar A5: Coding I

Afternoon:

1:30 PM	Plenary Session I
2:30 PM	B1: Quantum Channels B2: Communication Systems II B3: Cryptography B4: Shannon Theory I B5: Coding II

Evening:

8:00 PM	Impromptu Session

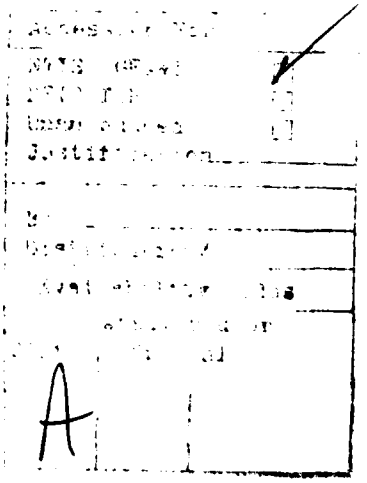
TUESDAY, FEBRUARY 10, 1981

Morning:

9:00 AM	C1: Communication Systems III C2: Communication Networks I C3: Pattern Recognition C4: Shannon Theory II C5: Coding III

Afternoon:

1:30 PM	Plenary Session II
2:30 PM	D1: Stochastic Processes II D2: Image Processing I D3: Communication Networks II D4: Shannon Theory III D5: Coding 1V



WEDNESDAY, FEBRUARY 11, 1981
Morning:

9:00 AM	E1: Complexity
	E2: Stochastic Processes III
	E3: Multi-User Information Theory II
	E4: Speech Compression I
	E5: Coding V

Afternoon:

1:30 PM	Plenary Session III
2:30 PM	F1: Estimation I
	F2: Communication Networks III
	F3: Detection Theory
	F4: Shannon Theory IV
	F5: Image Processing II

Evening:

Cocktail Party

THURSDAY, FEBRUARY 12, 1981
Morning:

9:00 AM	G1: Communication Systems IV
	G2: Estimation II
	G3: Shannon Theory V
	G4: Speech Compression II
	G5: Coding VI

Afternoon:

1:30 PM	Plenary Session IV
2:30 PM	Shannon Lecture

TECHNICAL PROGRAM AND TABLE OF CONTENTS

MONDAY MORNING, FEBRUARY 9, 9:00

SESSION A1
STOCHASTIC PROCESSES I

Chairman: F. Beutler, University of Michigan

"Partial Balance, Innovations Gains, and the Intensity Filtering Method of Flow Analysis in Markovian Systems," P. Bremaud (France). 20

"A Fourth-Order Homogeneous Random Field in Oceanography," T.T. Kadota and F.M. LaBianca (USA). 20

"Some Comments on Conditionally Markov and Reciprocal Gaussian Processes," J. Abrahams and J.B. Thomas (USA) 20

"Pseudo Innovations Pepresentations for Alpha-Stationary Processes," M. Morf and J.M. Delosme (USA) 21

"Expectation of a Multiplicative Functional of a Linear Ito Process," J.L. Hibley (USA). 22

"Alpha-Stationary Distortion Measures via Ladder Forms," D.T.L. Lee and M. Morf (USA) 22

SESSION A2
MULTI-USER INFORMATION THEORY I

Chairman: T. Berger, Cornell University

* "On Source Coding with Side Information via a Multiple-Access Channel and Related Problems," T.S. Han (Japan) and R. Ahlswede (Germany). 24

"Information Theory of Multiple Descriptions," A.A. El Gamal and T. Cover (USA) 24

"A New Achievable Rate Region for the Interference Channel," T.S. Han and K. Kobayashi (Japan). 25

"The Wiretap Channel with Feedback," R. Khan (USA) 25

"Feedback and Semi-Feedback Investigations for Multi-User Channels," F.M.J. Willems, E.C. Van der Meulen (Belgium) and J.P.M. Schalkwijk (The Netherlands). 26

"Coding of Correlated Sources with Prescribed Distortion by Separated Encoders," J. Wolfowitz (USA) . . . . . .

"On the Capacity of an n-Receiver Broadcast Channel with Partial Feedback," C. Leung (Canada) 27

* Denotes Long Paper

SESSION A3
COMMUNICATION SYSTEMS I

Chairman: J. Holmes, Holmes Associates

"Adaptive Equalizer for Carrier Modulated Data Transmission," N.C. Mohanty (USA) 28

"Embedded Pilot Signals for Adaptive Signal Extraction in Multi-Channel Environments," B.G. Agee and W.A. Gardner (USA). . . . 28

"Adaptive Channel Encoding for Multiplex Transmission over Discrete Channels Having Very Variable Error Rate," A. Bernardini and G.M. Poscetti (Italy). 28

"Diffusion Approximations for the Analysis of Digital Phase Locked Loops," H.J. Kushner and H. Huang (USA) 29

"Phase Sequence Estimation in the Presence of Rayleigh Fading," S.R. Robinson and D.E. Meer (USA). 29

"Entropy and Absolute Phase Demodulation," R.S. Bucy (USA), J.M.F. Moura (Portugal) and A.J. Malinckrodt (USA) 30

SESSION A4
RADAR

Chairman: E. Mendelovicz, Hughes Aircraft Company

"Maximum Likelihood Estimation in Detection of Radar Signals," R.N. Madan and J.M. Guild (USA). 31

"The Apparent Disparity between the Responses of a Monopulse Receiver to Jammers and to Passive Targets," I. Kanter (USA) 31

"A Doppler Estimation Circuit for an Adaptive MTI in the Presence of a Coded Waveform in a Tracking Radar," T. Bucciarelli and G. Picardi (Italy). 31

"The Effect of Thresholding in Reducing Glint from Extended Targets," I. Kanter (USA). 32

"Linear vs. Logarithmic Frame-Integration for Coherent Laser Radars," J.H. Shapiro (USA). 32

Implementation and Performance of NAR-AGC Adaptive Detection Systems," B. Picinbono and A. Ouamri (France). 33

SESSION A5
CODING I

Chairman: S. Lin, University of Hawaii

"Graph Theoretic Approaches to the Code Construction for the Two-User Multiple-Access Binary Adder Channel," T. Kasami (Japan), S. Lin, V.K. Wei (USA) and S. Yamamura (Japan) 34

"Coding for T-User Binary Symmetric Broadcast Channels," S.C. Chang (USA). 34

"Group Codes for the M-Receiver Gaussian Broadcast Channel," C. Downey and J. Karlof (USA). 34

"On the Combinational and Delay Complexity of Asymptotically Good Codes," Y. Imber and J.E. Savage (USA). 35

"Bilinear Cyclic Convolution Algorithms over Finite Fields," S.D. Morgera and M.D. Wagh (Canada). 35

* * * * * *

MONDAY AFTERNOON, FEBRUARY 9, 1:30

PLENARY SESSION I

Invited Lecture:

"In Search of a Non-Probabilistic Information Theory", J. Ziv, Technion, Israel Institute of Technology (Israel). . . .

* * * * * *

MONDAY AFTERNOON, FEBRUARY 9, 2:30

SESSION B1
QUANTUM CHANNELS

Chairman: C. Helstrom, University of California, San Diego

"Noncommutative Probability Models in Quantum Communication and Multi-Agent Stochastic Control," J.S. Baras (USA). 37

"Optimal Point Process Estimators for Gaussian Optical Field Intensities," F. Davidson and Y.C. Park (USA). 37

"Variable Structure Nonlinear Quantum Mechanical Filter for a Vector-Valued System Process with Semi-Martingale Decomposition," D. Ilic (USA). 38

"Optimal Coding and Decoding of a Random Telegraph Wave for Transmission through a Poisson Type Channel," A.A. Lazar and S.C. Schwartz (USA). 38

"Performance of Quantum Signals in Unimodal and Bimodal Optical Communications," C.W. Helstrom (USA) 39

"Direct and Indirect Quantum Measurements Yield Equal Maximum Information," L.B. Levitin (Germany) 39

"The Cutoff Rate Region for Multiple Access Optical Communication Systems," P. Narayan and D.L. Snyder (USA). 40

"On the Capacities and Error Performance of the Free-Space Optical Channel, "H.P. Yuen (USA). 40

SESSION B2
COMMUNICATION SYSTEMS II

Chairman: G.K. Huth, Axiomatix, Inc.

*"Time Slot Assignment in an SS/TDMA System with Minimum Switchings," K.S. Natarajan and S.B. Calo (USA). 41

"Narrowband Interference Suppression in Pseudo-Noise Spread Spectrum Systems," J.G. Proakis and J.W. Ketchum (USA) 41

"Hard-Decision versus Soft-Decision Decoding for Frequency-Hopping Multiple-Access Systems in a Rayleigh Fading Environment," O.C. Yue (USA). 41

"A Method of Signal Design for Spread Spectrum Systems," K.V. Cai and G.R. Cooper (USA) 42

"Spectra of Linearly Coded Digital Signals," J. Bezerra and D.S. Arantes (Brazil). 42

"Spectral Analysis of the Powers of a PAM Digital Signal," S. Pupolin and G. Bilardi (Italy). 43

SESSION B3
CRYPTOGRAPHY

Chairman: L. Adleman, University of Southern California

"A Cryptosystem Making Use of the Correlation between Message and Key," S.C. Lu (China). 44

"Maximum Likelihood Estimation Applied to Cryptanalysis," D. Andelman (USA). 44

"Knapsacks which are not Partly Solvable after Multiplication Modulo q," I. Ingemarsson (Sweden). 45

"Cryptanalysis of the Data Encryption Standard by Formal Coding," I. Bichl, J. Biermeier, D. Gollmann and F. Pichler (Austria). 45

"On Traitor-Secure Public-Key Systems," D. Dolev and A. Yao (USA) 46

"Bounds on Message Equivocation for Simple Substitution Ciphers," J.G. Dunham (USA). 46

"On Computing Algorithms over GF(2^p) or an Attempt to Swindle MITRE Corporation," T. Herlestam and R. Johannesson (Sweden) 47

* Denotes Long Paper

"On Secret Sharing Systems," E. Krasniansky, D. Greene, W. Jonathan and M.E. Hellman (USA) 47

"On Factoring and Random Graphs," J. Reyneri and M.E. Hellman (USA) 48

SESSION B4
SHANNON THEORY I

Chairman: M. Pursley, University of Illinois

* "The Ergodic and Entropy Theorems Revisited," P.C. Shields (USA) 49

"The Asymptotic Redundancy of Huffman Coding," R.J. McEliece (USA) 49

"Algorithms for Sliding Block Codes (An application of symbolic dynamics to information theory)," M. Hassner and R.L. Adler (USA) 50

"A Sliding-Block Code for Small User Alphabets with Performance near the Rate-Distortion Limit," W.A. Pearlman (USA) 50

"Source Coding with Respect to a Multidimensional Fidelity Criterion," J.E. Stjernvall (Sweden) 50

"Information Rates of Time-Discrete Stationary Gaussian Sources," D. Wolf, H.P. Weber and T. Denker (Germany) 52

"The Rate-Distortion Function on Classes of Sources Determined by Spectral Capacities," V.H. Poor (USA) 52

SESSION B5
CODING II

Chairman: L. Welch, University of Southern Califronia

"A Quick-Look Decoder with Isolated Error Correction and Node Synchronization," C.A. Greenhall, R.L. Miller and S.A. Butman (USA) 54

"Sequential Decoding for Burst Error Channels," L. Bahl, J. Cocke, C.D. Cullum and J. Hagenaur (USA) 54

"Stack and Input Buffers Overflow of Stack Decoding Algorithms," D. Haccoun and M. Dufour (Canada) 55

"On the Class $L_{2,\nu,\ell}$ of Convolutional Codes," A.J. Vinck (The Netherlands) 56

"Binary Convolutional Codes Derived from Cyclic Codes over $GF(2^n)$," G. Séguin (Canada) 56

"Non-Synchronizing Sequences in Convolutional Codes," P. Godlewski (France) 56

* Denotes Long Paper

"On the Complexity of Sequential Decoders," J.P.M. Schalkwijk and J.A.M. de Brouwer (The Netherlands). 57

"New Bounds on the Performance of Binary Convolutional Codes Using Viterbi Decoding on a Binary Symmetric Channel," K.A. Post (The Netherlands). 57

* * * * * *

MONDAY EVENING, FEBRUARY 9, 8:00,

IMPROMPTU SESSION

Chairman: J. Dunham, Washington University, St. Louis (USA)

* * * * * *

TUESDAY MORNING, FEBRUARY 10, 9:00

SESSION C1
COMMUNICATION SYSTEMS III

Chairman: L.B. Milstein, University of California, San Diego

"The Computation Cut-Off Rate R_{comp} for an Optical Channel with Multilevel AM Signaling and Direct Detection Receivers," V.W.S. Chan (USA). 58

"Capacity,Cut-Off Rate, and Coding for a Direct-Detection Optical Channel," J.L. Massey (Switzerland). 58

"Effects of ISI on Viterbi Decoding," D. Divsalar and J.K. Omura (USA) 58

"Cut-Off Rate Evaluation for Diversity Transmission with Rayleigh Fading,"J.J. Komo and A. Aridgides (USA). 59

"The Computational Cutoff Rate of Channels Having Memory," E. Biglieri (Italy). 59

"Power-Bandwidth Performance of Smoothed Phase Modulation," J.B. Anderson (Canada), C. E. Sundberg, T. Aulin and N. Rydbeck (Sweden) 59

"Minimum Distance and Bandwidth of M-ary Multi-h Continuous Phase Modulated Signals," T. Aulin and C.E. Sundberg (Sweden). . . . 60

SESSION C2
COMMUNICATION NETWORKS I

Chairman: I. Rubin, University of California Los Angeles

"Packet Waiting Time for Multiple Access Channels," A. Ephremides and T. Saadawi (USA) 61

"Channel Sharing Among Many Bursty Sources," J.F. Hayes (Canada) 62

"A Class of Hybrid TDMA/Tree-Random-Access Schemes for Multi-Access Communication Channels," I. Rubin and M. Louie (USA) 62

"A Teletraffic Performance Analysis of a Computer Data Communication Link," B.W. Stuck (USA) 62

"Modeling and Analysis of an Integrated Voice-Data Multiplexer," K. Sriram, P.K. Varshney and J.G. Shanthikumar (USA) . . . 63

"Performance Analysis of Hybrid-Switched Link," A. Leon-Garcia (Canada) 63

"Applications of Combinatorial Sets in Satellite Communications," W.W. Wu (USA) 64

"Effect of Channel Errors on the Capetanakis and Related Random-Access Algorithms," J.L. Massey (Switzerland) 65

SESSION C3
PATTERN RECOGNITION

Chairman: G.T. Toussaint, McGill University

* "Minimum Cross-Entropy Pattern Classification and Cluster Analysis," J.E. Shore and R.M. Gray (USA) 66

* "Graph Theoretic Methods for Edited Nearest Neighbor Decision Rules," G.T. Toussaint, B.K. Bhattacharya and R.S. Poulsen (Canada) 66

"A Test of the Gaussian-ness of a Data Set Using Clustering," K. Fukunaga and T.E. Flick (USA) 67

"Sequential Procedures in Identification," J. Ghosh and N. Mukhopadhyay (USA) 68

"Nearest Neighbor Rule Classification of Non Stationary Time Series: Preliminary Observations on the Information for Discrimination in Human Evoked Potentials," W. Gersch and T. Brotherton (USA) 68

"Nonlinear Classifier Designed with a Feature Space Sampling Technique," S. Tatsumi, S. Kimura and T. Kitahashi (Japan) 70

"An Algorithm for Optimal Linear Distance-Preserving Mappings," S.A. Starks and M.D. Vanstrum (USA) 70

* Denotes Long Paper

SESSION C4
SHANNON THEORY II

Chairman: L.D. Davisson, University of Maryland

* "The Error Exponent for the Noiseless Encoding of Finite Ergodic Markov Sources," L.D. Davisson (USA), G. Longo and A. Sgarro (Italy). 71

"Universal Noiseless Source Coding Techniques for Markov Sources," A.C. Blumer, R.J. McEliece, M.B. Pursley and M.S. Wallace (USA) 71

"Universal Noiseless Coding of Sources with Memory," H. Tanaka (Japan) and A. Leon-Garcia (Canada). 72

"On Total Boundedness for the Existence of Weakly Minimax Universal Codes," R.J. Fontana and W. C. Chen (USA). 72

"An Approach to Source Coding," T. Hashimoto (Japan) 73

"Sufficient Condition of Universality for Variable-to-Variable-Length Methods of Coding and Some Properties of Methods of Coding Satisfying this Condition," B. Fitingof (Germany). 73

SESSION C5
CODING III

Chairman: S.W. Golomb, University of Southern California

"A Selective Update on Shift Register Sequences," S.W. Golomb (USA). 74

"Spread Spectrum Applications Using de Bruijn Sequences," H. Fredricksen (USA) 74

"Sequences for Spread Spectrum Multiple Access Systems Generated from Cyclic Error-Correcting Codes," C.E. Sundberg (Sweden). 75

"Further Results on Maximum-Length Decimal Sequences," S.C. Kak (USA) 75

"New Results Concerning the Greismer Bound," H.C.A. van Tilborg (The Netherlands) 75

"A Linear Programming Minimum Distance Bound for Linear Codes," M.R. Tanner (USA). 76

"Generalization of the Minimum Distance Bound on Goppa Codes," G.L. Feng (USA). 76

* * * * * *

TUESDAY AFTERNOON, FEBRUARY 10, 1:30

PLENARY SESSION II

Invited Lecture: "Distributed Sensor Networks", Dr. R.E. Kahn, Advanced Research Projects Agency Department of Defense (USA). . . .

* * * * * *

TUESDAY AFTERNOON, FEBRUARY 10, 2:30

SESSION D1
STOCHASTIC PROCESSES II

Chairman: T.T. Kadota, Bell Telephone Laboratories

"Bias and Variance of DTOA Estimates Based on Noisy,Sampled, Clipped Data," T. Berger (USA) 77

"The Reconstruction of Analog Signals from the Sign of Their Noisy Samples," E. Masry (USA) 77

"Min-Max Linear Extrapolation of Bandlimited Sequences," T. Gaarder, K. Rege and D. Slepian (USA) 78

"Delta Modulation of Time-Discrete Processes with I.I.D. Increments Having a Rational Characteristic Function," A. Hayashi (Japan) . . . 79

"Third-Order Intermodulation due to Quantization," N.M. Blachman (USA). 79

"Stochastic Quantization for Performance Stability," P. Papantoni-Kazakos (USA) 79

"Observations on F.M. in a Rayleigh Channel," D.J. Thomson (USA) 80

"Simulations of Two-Stage Adaptive Signal Extractors," J. Kazakoff and W.A. Gardner (USA) 81

SESSION D2
IMAGE PROCESSING I

Chairman: W. Pratt, Compression Laboratories

* "Tree Encoding of Images in the Presence of Channel Errors," J.W. Modestino, B. Vasudev (USA) and J.B. Anderson (Canada). 82

"Hybrid Coding of NTSC Signals - Channel Error Studies," K.R. Rao and F.A. Kamangar (USA) 82

"Adaptive Image Transform Coding: A Theoretic Approach and Approximations for Simplifying the Digital Implementation," W. Mauersberger (Germany). 83

* Denotes Long Paper

"Predictive Data Compression of Color Picture Signals Using a Component Coding Method," V.E. Neagoe (Romania). 83

"A Hybrid Coding Method of Video Signals," O. Telese and G. Zarone (Italy). 84

"Encoding Moving Pictures by Using Adaptive Straight-Line Approximation," Y.T. Wang (China) and J.P.M. Schalkwijk (The Netherlands). 84

"Performance of Image Transmission Systems on Fading Channels," D.G. Daut and J.W. Modestino (USA) 84

SESSION D3
COMMUNICATION NETWORKS II

Chairman: L.M. Nirenberg, TYMNET

* "A Class of Optimal Routing Algorithms for Communication Networks," D.P. Bertsekas (USA). 86

"Routing in Computer Communication Networks: An Approach Based on Sequential Procedures," R. Singh, S. Subba Rao and S.C. Gupta (USA) 86

"Bandwidth Control in Computer Networks," M. Gerla (USA) 86

"Flow Control Power is Non-Decentralizable," J.M. Jaffe. 87

"Coding Gains from ARQ Error Control Systems," J.A. Heller and J.K. Wolf (USA). 87

* "The Analysis of Some Selective Repeat ARQ Schemes with Finite Receiver Buffer," M.J. Miller and S. Lin (USA). 88

"An Analysis of an ARQ Error Control Scheme Using Sequential Decoding," A. Drukarev and D.J. Costello (USA) 88

SESSION D4
SHANNON THEORY III

Chairman: A. Leon-Garcia, University of Toronto

"Robust Coding of Indecomposable Finite State Channels," B. Pátek (Czechoslovakia). 90

"Finite State Indecomposable Channels Are Almost Finite," D.L. Newhoff and P.C. Shields (USA). 90

"Block Coding for a Stationary Channel Satisfying a Local Stability Condition," J.C. Kieffer (USA) 90

"On Choquet Capacities and Their Derivatives with Respect to σ- Finite Measures," K.S. Vastola and V.H. Poor (USA). 91

"On the Capacity of Arbitrarily Varying Channels for Maximum Probability of Error," I. Csiszár and J. Körner (Hungary). 91

* Denotes Long Paper

"A Binary Noise Primitive Channel," Y. Matsuyama (Japan). 92

"On the Capacity of the Gaussian Channel with Feedback," C.R. Baker (USA). 92

"Nonlinear Feedback in Sequential Digital Communication Systems," A.F. Hassan (Egypt) 93

SESSION D5
CODING IV

Chairman: C.R.P. Hartmann, Syracuse University

"Bit-Serial Reed-Solomon Encoders," E.R. Berlekamp (USA). 94

"Bounds and Constructions for Error Correcting/Detecting Codes on the Z Channel," M.J. Borden (USA) 94

"On the Construction of Systematic Single Error Correcting and Multiple Unidirectional Error Detecting (SEC-MUED) Codes," B. Bose (USA) 95

"Non-Redundant Codes for Transmitting Quantized Signals under Channel Error Conditions," M. Copperi (Italy) 95

"Coset Coding," J.M. Goethals and L. Huguet-Rotger (Belgium). 96

"Improved Decoding Scheme for Frequency Hopped Multilevel FSK Systems," U. Timor (USA). 96

"Synchronization of Reed-Solomon Codes," R.L. Miller (USA) and B.B. Newman (Brazil). 97

"On the Design of Mean-Square Error Channel Coding Systems Using Cyclic Codes," G.R. Redinbo (USA) 97

* * * * * *

WEDNESDAY MORNING, FEBRUARY 11, 9:00

SESSION E1
COMPLEXITY

Chairman: K. Yao, University of California, Los Angeles

"On the Power of Straight-Line Computations in Finite Fields," A. Lempel, G. Seroussi and J. Ziv (Israel). 99

* "The Complexity of Information Structures," M.L. Fredman (USA). . . 99

* "Digital Signal Processing Applications of Polynomial Transforms," H.J. Nussbaumer (France). 100

* "The Complexity of Searching Games," J. Pearl (USA) 100

* Denotes Long Paper

* "Khachiyan's Algorithm and the Complexity of the Linear Programming Problem," R.E. Stone (USA). 101

SESSION E2
STOCHASTIC PROCESSES III

Chairman: W. Gersh, University of Hawaii

"Spectrum Estimation via Orthogonal Windows," D.J. Thomson (USA). . .102

"On the Method of Maximum Entropy Spectrum Estimation with Application to Seismology," A. Arcese (USA) 102

"Tone Estimation Using an Autoregressive-Moving Average Model," C.R. Guarino (USA). . . . . .

"Autoregressive Models for Nonstationary Discrete-Time Processes," H. Lev-Ari and T. Kailath (USA) 103

"New Methods for Probability Density Estimation," R.B. Holmes and L.K. Jones (USA). 103

"Computing the Distribution of a Random Variable via Gaussian Quadrature Rules," M. Meyers (USA). 104

SESSION E3
MULTI-USER INFORMATION THEORY II

Chairman: J. Wolf, University of Massachusetts

* "To Get a Bit of Information May Be as Hard as to Get Full Information," R. Ahlswede (Germany) and I. Csiszár (Hungary). 105

"The Problem of Isomorphism for General Discrete Memoryless Stationary Correlated Sources," K. Marton (Hungary) 105

"An Iteration Lemma and Its Application to Successive Coding of Multiple Sources," T. Ericson (Hungary). 105

"Some New Results of Shannon Theory," G.D. Hu and S.Y. Shen (China) 106

"Information of Partitions with Applications to Random Access Communications," B. Hajek (USA) 106

"The Capacity of Computer Memory with Defects and Noise," A.A. El Gamal and C. Heegard (USA). 107

"The Capacity and Computation Cut-Off Rate of a Multiple-User Random-Access Communication System," V.W.S. Chan (USA). 107

* Denotes Long Paper

SESSION E4
SPEECH COMPRESSION I

Chairman: J.B. Anderson, McMaster University

* "Tree Coding versus Differential Encoding of Speech: A Perspective," J.D. Gibson(USA). 108

* "Adaptive Methods for Tree Encoding with Speech Applications," S.G. Wilson and S. Pizzi (USA). 108

"Speech Compression Systems Using a Set of Inverse Filters," Y. Matsuyama (Japan). 110

"Tree and Trellis Speech Compression," L.C. Stewart (USA) 110

* "On the Information Rate of Quantized Speech," D.L. Cohen and J.L. Melsa (USA). 111

SESSION E5
CODING V

Chairman: F.J. MacWilliams, Bell Telephone Laboratories

"On APP Decoding," C.R.P. Hartmann, L.D. Rudolph and K.G. Mehrotra (USA). 112

"On the Majority Logic Decoding of a Class of Composite Codes," S.G.S. Shiva and V. Mimis (Canada). 112

"Efficient Decoder Algorithms Based on Spectral Techniques," R.E. Blahut (USA) 113

"A Type I Erasures-and-Errors Decoder for Majority-Logic-Decodable Codes," Y. Sugiyama, M. Kasahara, T. Inoue, S. Hirasawa and T. Namekawa (Japan) 113

"A Modified Omura Algorithm for Decoding Binary Group Codes," G.C. Clark, J.B. Cain and G.H. Thaker (USA) 113

"Syndrome Decoding - Re-Examined from a Combinational View Point," M. Rahman (Saudi Arabia). 114

"Design and Hardware Implementation of a Versatile Transform Decoder for Reed-Solomon Codes," D.O. Carhoun, B.L. Johnson and S.J. Meehan (USA) 114

* * * * * *

WEDNESDAY AFTERNOON, FEBRUARY 11, 1:30

PLENARY SESSION III

Invited Lecture: "The Evolution to Integrated Voice/Data Networks"
Dr. L.G. Roberts, GTE-TELENET (USA) . . . . . .

* Denotes Long Paper

WEDNESDAY AFTERNOON, FEBRUARY 11, 2:30

SESSION F1
ESTIMATION I

Chairman: J. Hibey, University of Notre Dame

* "On Adjoint Models and Fixed-Interval Smoothing," H.L. Weinert and U.B. Desai (USA) 116

"Optimal Bayes Smoothing with Uncertain Observations," M. Askar and H. Derin (Turkey) 116

"Nonlinear Smoothing Using Finite State Models and the Viterbi Algorithm," J.K. Omura (USA) and K. Kozlowski (Poland) 117

"A Two-Dimensional Recursive Smoothing Algorithm Using Polynomial Splines," C.S. Kim and C.N. Shen (USA) 117

"A Robustized Vector Recursive Algorithm in Estimation and Image Processing," I. Kadar and L. Kurz (USA) 117

"An Estimation of a Gaussian Message from Non-Gaussian Observation Using Linear Time-Varying Filter," R. Doraiswami (Brazil) 118

"A Nonparametric Method on Receiver Timing Acquisition and Tracking," S.Y. Mui (USA) 118

SESSION F2
COMMUNICATION NETWORKS III

Chairman: R. Gallager, Massachusetts Inst. of Technology

* "Poisson Flows on Markov Step Processes," F.J. Beutler and B. Melamed (USA) 119

"Delay Analysis of a Two-Queue, Non-Uniform Message Channel," S.B. Calo (USA) 119

"On Genie-Aided Upper Bounds to Multiple Access Contention Resolution Efficiency," T. Berger, N. Mehravari and G. Munson (USA) 120

"Bounds on the Capacity of Infinite Population Multiple Access Protocols," M.L. Molle (USA) 120

"Topology Design for Time Slotted Packet Radio Networks," D. Towsley and C.G. Prohazka (USA) 121

"A Distributed Shortest Path Protocol,"F.B.M. Zerbib and A. Segall (Israel) 121

"Finite State Description of Communication Devices in Computer Networks," A. Faro (Italy) 122

* Denotes Long Paper

"Explicit Concentrators from Generalized N-gons," M.R. Tanner (USA). 122

SESSION F3
DETECTION THEORY

Chairman: I.S. Reed, University of Southern California

"Performance of a Robust Detector for the Rayleigh Fading Channel," S.A. Kassam and J.G. Shin (USA) 123

"Detection of Weak Secondary Signals with the Aid of Already Detected Strong Primary Signals," H.M. Hall, T.T. Kadota, J.B. Seery and M.H. Silverberg (USA). 123

"Convexity Properties of Measures of Class Separation in Statistical Decision Theory," P. Fishman and L.K. Jones (USA) 123

"Self-Adaptive Tuning Detection of Aperiodic Signals from Aperiodic Noise," G. Colonnese and B. Castagnolo (Italy). 124

"Generalized Detection Procedure Based on the Weighting of Partial Decisions," V. Milutinović (Yugoslavia) 124

"A Geometric Approach to the Detection of Signals of Unknown Energy in Gaussian Noise of Unknown Mean and Power," M.A. Blanco (USA) 125

"An Innovative Approach to Signal Detection for Unknown Signals," G. Sogliero (USA) 126

"Optimal M-ary System with Polynomial Form Pulse Code Modulation," V.E. Neagoe (Yugoslavia). 126

SESSION F4
SHANNON THEORY IV

Chairman: R. McEliece, University of Illinois

"Competitive Optimality of Kelly-Breiman Gambling," R.M. Bell and T. Cover. 127

"Shannon's Entropy and Some Distributions of Binomial Coefficients Defined on Pascal's Triangle," N. Cot (France). 127

"On the Selection of Measures of Distance Between Probability Distributions," J. Abrahams (USA) 128

"Schurconvexity and Measures of Certainty and Information," J.C.A. van der Lubbe and Y. Boxma (The Netherlands) 128

"Minimization of Discrimination Measures," N.L. Aggarwal and B. Bouchon, (France). 128

"On the Hierarchy of Codes for DMC", T. Hashimoto and S. Arimoto (Japan). 129

"The Best Known Codes Are Highly Probable and Can Be Produced by a Few Permutations," R. Ahlswede and G. Dueck (Germany) 129

SESSION F5
IMAGE PROCESSING II

Chairman: A. Sawchuk, University of Southern California

* "The Effect of Median Filter on Edge Location Estimation," G.J. Yang and T.S. Huang (USA) 130

"Subpixel Measurement of Edge Location," R.O. Mitchell, A.J. Tabatabai and E.J. Delp (USA) 130

"On Improving the Efficiency of Chain Encoded Line Drawings," J. Koplowitz (USA) 131

"Sequential Estimation in Two-Dimensional Discrete Random Fields," J.A. Ponnusamy and M.D. Srinath (USA) . . . . . .

"Advanced MAP Restoration - Filtering Techniques with Application to Image Processing," V. Cappellini, E. Del Re, G. Francolini and S. Taiuti (Italy). 131

"Speckle Analysis and Smoothing of Synthetic Aperature Radar Images," J.S. Lee (USA) . . . . . .

"Image Enhancement and Recognition of Moving Objects in a Cluttered Background," N.C. Mohanty, J. Pasek and K. Taylor (USA). 132

"Digital Halftones and Image Coding," E. Angel (USA) 132

* * * * * *

WEDNESDAY EVENING, FEBRUARY 11,

COCKTAIL PARTY, BANQUET

Invited Speaker: Robert Blalack, Composite Optical Photography 1978 Academy Award Winner for Special Effects Lucas Films, Ltd.. . . .

Audiovisual presentation on: "Movie Magic: The Special Effects of Star Wars and Beyond". . . . . .

* * * * * *

THURSDAY MORNING, FEBRUARY 12, 9:00

SESSION G1
COMMUNICATION SYSTEMS IV

Chairman: M. Simon, Jet Propulsion Laboratory

"Error Bounds for Multi-h Phase Codes," S.G. Wilson, J.H. Highfill and C.D. Hsu (USA) 134

* Denotes Long Paper

"Error Probability Bounds for Viterbi Detected Continuous Phase Modulated Signals," T. Aulin (Sweden) 135

"On a Tight Error Probability Bound for a Quantized Detector," S. Reisenfeld and K. Yao (USA) 135

"The Use of Moment Space Bounds for Evaluating the Performance of Nonlinear Digital Communication Systems," K. Yao and L.B. Milstein (USA) 136

"Optimization and Comparative Performance of Selection Diversity Receivers for the Rician and Lognormal Channels," M.A. Blanco (USA) 136

"Least Square Approximation to Error Probabilities using Generalized Gram-Charlier Expansions," R.S. Freedman (USA) 137

"A Fast Evaluation of the Error Rate of CPSK System with Intersymbol and Multiple Co-Channel Interferences by Means of Local Approximations of the Error Function," P. Amadesi (Italy) 137

SESSION G2
ESTIMATION II

Chairman: D. Snyder, Washington University

"Optimal Filter Based on Mutual Information," S. Omatu and T. Soeda (Japan) 139

"Maximum Likelihood Estimates of the Mean and Covariance Based on a Set of Nonlinear Observations," F.K. Sun (USA) 139

"On Optimal Reduction of Observations for Estimation," B. Picinbono and M. Benidir (France) 139

"Invariant Imbedding Approach to the Solution of Linear Least-Squares Estimation Problem with Degenerate Covariance," S. Ueno (USA) 140

"Linear Prediction in Case of Non Positive Definite Covariance Matrices," C. Gueguen (France) 140

"Analysis of Performance of the LMS Algorithm for Adaptive Estimation in a Nonstationary Environment," W.A. Gardner and M. Hajivandi (USA) 141

"Improvements of Adaptive Linear Prediction by Non-Linear Methods," T. Denker and D. Wolf (Germany) 142

"Maximum Variance Stochastic Realizations," F. Perez, T. Kailath and A.A. El Gamal (USA) 143

SESSION G3
SHANNON THEORY V

Chairman: J.K. Omura, University of California, Los Angeles

* "About Lattices and the Random Coding Theorem,"
R.G. de Buda and W. Kassam (Canada). 145

"A New Look at the Viterbi Algorithm and Trellises,"
F.E. Othmer (Germany). 145

"Optimal Metric-First Code Tree Search Algorithms,"
S. Mohan (USA) and J.B. Anderson (Canada). 145

"An Information Theoretic Approach to the Construction of
Efficient Decision Trees," J.M. De Faria, Jr. (Brazil),
C.R.P. Hartmann, C.L. Gerberich and P.K. Varshney (USA). 146

"Algorithm of Storage Reduction for Codings with the Use of
Code Trees," B. Fitingof (Germany) 146

SESSION G4
SPEECH COMPRESSION II

Chairman: N. Gallagher, Purdue Univeristy

* "An 800 bps Speech Compression System Based on Vector
Quantization," D.Y. Wong, F.B. Juang and A.H. Gray, Jr. (USA). 147

* "Vector Coding: A New Approach to Medium-Band Speech Coding,"
J.P. Adoul and P. Mabilleau (Canada) 147

"Vector Quantization Applied to Speech Coding," G. Rebolledo
and R.M. Gray (USA). 148

"Vector Quantization of Speech and Speech-Like Waveforms,"
H. Abut, R.M. Gray and G. Robelledo (USA). 149

"A Fast Method for Optimal Adaptive Data Compression,"
J. Karhunen and E. Oja (Finland) 149

SESSION G5
CODING VI

Chairman: E. Posner, Jet Propulsion Laboratory

"On Finding the Roots of Polynomials over Finite Fields,"
C.L. Chen (USA). 150

"Voronoi Regions of Sphere Packings," N.J.A. Sloane (USA). 150

"On the Covering Radius of Binary Linear Codes,"
M. Karpovsky (USA) 150

* Denotes Long Paper

"Some Generalizations of Perfect Codes," G. Cohen, M. Deza and P. Frankl (France). 150

"(n,k,t) - Covering Systems and Error-Trapping Decoding," A.H. Chan and R.A. Games (USA). 151

"On Determining the Independent Point Set for Doubly Periodic Arrays and Encoding Two-Dimensional Cyclic Codes and Their Duals," S. Sakata (Japan) 151

"Goppa Codes Related Quasiperfect Double Error Correcting Codes," O. Moreno (Puerto Rico) 152

"A Berlekamp-Massey Type Procedure for the Solution of the Pade Approximation Problem for Scalar Rational Sequences," J. Conan (Canada). 152

* * * * * *

THURSDAY AFTERNOON, FEBRUARY 12, 1:30

PLENARY SESSION IV

Invited Lecture: "Overview of the Technology of Error-Correcting Codes", Professor E.R. Berlekamp, University of California, Berkeley. . . . . .

SHANNON LECTURE: "The Computer as a Theoretician's Tool", Professor W.W. Peterson, University of Hawaii . . . . . .

* * * * * *

SESSION A1

Stochastic Processes I

PARTIAL BALANCE, INNOVATIONS GAINS, AND THE INTENSITY FILTERING METHOD OF FLOW ANALYSIS IN MARKOVIAN SYSTEMS, P. Bremaud (France). We will give a brief account of a general method for determining the law of a point process representing a subflow in a Markovian system (for instance, an output of a queueing network, or a feedback flow in a queue) and we will give illustrations of the method including Burke-Kelly output theorems, the general independence result of Melamed. We will also review results of Varaiya, Walrand, and Sismail. The method is based on the Martingale approach to the notion of stochastic intensity of a point process and the innovations theory of filtering. It is a by-product of the general Martingale approach to point process systems considered in the author's other works.

A FOURTH-ORDER HOMOGENEOUS RANDOM FIELD IN OCEANOGRAPHY, T.T. Kadota and F.M. Labianca (USA). We establish some mathematical properties of a certain random field which is used as a phenomenological model for wind pressure exciting the ocean surface. Specifically, we prove that the random field, consisting of ordinary processes and point processes and given in terms of an infinite series, is well defined, namely, it converges with probability 1, and is a wide-sense homogeneous field having an explicit form of spectral representation, and has a finite fourth moment everywhere.

SOME COMMENTS ON CONDITIONALLY MARKOV AND RECIPROCAL GAUSSIAN PROCESSES, J. Abrahams and J.B. Thomas (USA). Mehr and McFadden's conditionally Markov processes and Jamison's reciprocal processes are two independent extensions of Slepian's work on a particular stationary Gaussian process. This paper shows that reciprocal processes which are conditionally Markov and that Gaussian processes which are conditionally Markov over all subintervals of some interval are reciprocal on that interval. Stationary processes are included in, but do not exhaust, the latter class of processes. Furthermore, conditionally Markov and reciprocal

Gaussian processes can be represented as the sum of two independent processes, one a Gauss-Markov process and the other, the product of a Gaussian random variable with a deterministic function. Conversely, processes given by sums of the appropriate forms are conditionally Markov or reciprocal. (This research was supported by the National Science Foundation under grant ENG-76-19808, by the U.S. Army research Office under grant DAHC04-75-G-0192, and by the American Association of University Women Educational Foundation Dissertation Research Fellowship Program.)

PSEUDO INNOVATIONS REPRESENTATIONS FOR ALPHA-STATIONARY PROCESSES, M. Morf and J.M. Delosme (USA). We have recently introduced an index of stationarity (alpha), the significance of this index is that the larger the value of alpha the more nonstationary a process is. In addition, the complexity of models and calculations increases only proportional to this index. In the discrete case, alpha can be used to measure the distance of a matrix, e.g., a covariance matrix, from being Toeplitz. Solutions of linear equations involving such matrices can be obtained efficiently via the use of existing methods, such as the Krein-Levinson type algorithms, and more recently our doubling type algorithms. Several different notions related to alpha, such as the displacement rank, will be discussed, they lead to a classification on one hand and the question of minimality of the various associated representations. In the discrete case, a new Toeplitz block matrix embedding principle provides us with an elegant framework for relating various algorithms for solving Toeplitz systems, and an interpretation of the embedding matrix as a joint covariance matrix. Because of the larger size of the matrix, the associated number of random variables is alpha times the original number of variables, hence alpha is a multiplicity or rank of the process. Alternatively, a process can be modeled as the prediction error of one process given alpha other processes. The Alpha underlying (white) innovations can now be viewed as "pseudo" innovations. However, unlike the true innovations they can in general not be obtained in a casual way, i.e., they are smoothing residuals, and they have in general an unobservable component. This component can be viewed as an additive "ditter" whitening noise or "enciphering key" that allows the alpha pseudo innovations to be white. In particular the last reference points out some potential applications of this representation. In general a mixed representation can be used, some fraction of the alpha pseudo innovations is actually passed through anti-casual or adjoint filters instead of casual ones. This mixed representation avoids a particular signature problem. Physical interpretations of these results will be given, as

well as an outline of the continuous equivalents and so called ladder realizations.

EXPECTATION OF A MULTIPLICATIVE FUNCTIONAL OF A LINEAR ITO PROCESS, J.L. Hibey (USA). The expectation of the multiplicative functional $\exp[-\int_0^t x(\sigma)Q(\sigma)x(\sigma)d\sigma]$, where x is a vector Brownian motion process and Q is a deterministic nonnegative definite matrix, can be evaluated using the well-known Cameron-Martin. The result is characterized in terms of a Riccati equation associated with some auxiliary linear quadratic control problem. In this work, we extend these results to Ito processes x that satisfy linear stochastic differential equations. The technique involves a measure transformation similar to the type used to derive the above result. In addition, by allowing for nonzero initial time and initial state, we are able to show that the solution satisfies a partial differential equation of the backward Kolmogorov type. An example of a scalar, time-invariant process is given to illustrate the procedure.

ALPHA-STATIONARY DISTORTION MEASURES VIA LADDER FORMS, D.T.L. LEE AND M. Morf (USA). Measures such as the Bhattachrya, the Kullback-Leibler, and the related Itakura-Saito for second order processes involve determinants, traces and ratios of covariance matrices. In many applications, it is of interest to compute these measures efficiently, e.g., in speech processing, pattern recognition, and digital communication. In many applications, one may be interested in efficient parametrizations of such measures, either to simplify the calculations and design, or in the hardware implementation (e.g., VLSI). Distortion measure calculations of second order processes often involve Toeplitz operators, they can be handled efficiently via the use of existing methods, such as the Krein-Levinson type algorithms, or our new doubling type algorithms. They both have the advantage that they can handle a class of non-stationary processes, referred to as alpha-stationary. Alpha was defined as an index of stationarity, with the significance that the larger the value of alpha the more non-stationary a process is. In addition, the complexity of process models and calculations involving such processes increases only proportional to this index. In the paper we show that recently popular ladder canonical forms, which are based on partial-correlation coefficients, have many advantages in computing distortion measures. These ladder forms in fact represent in some sense

a "natural" canonical parametrization of many of the measures. Several examples involving distortion measures will be given, and their physical significance and applications to communication and estimation, e.g., speech processing and digital communication shall be discussed.

SESSION A2

Multi-User Information Theory I

*ON SOURCE CODING WITH SIDE INFORMATI*ON VIA A MULTIPLE-ACCESS CHANNEL AND RELATED PROBLEMS, T.S. Han (Japan) and R. Ahlswede (Germany). We give first a simple proof of the coding theorem for the multiple-access channel (MAC) with arbitrarily correlated sources (DMCS) of Cover-El Gamal-Salehi, which includes the results of Ahlswede for the MAC and of Slepian-Wolf for the DMCS and the MAC as special cases. Then we introduce and establish a coding theorem for another type of source-channel matching problem, i.e., a system of source coding with side information via MAC, which can be regarded as an extension of the Ahlswede-Korner-Wyner type noiseless coding system. Then we extend this result to a more general system with several principal sources and several side information sources subject to cross observation at the encoders in the sense of Han. The regions are shown to be optimal in special situations. Dueck's example shows that this is in general not the case for the result of Cover, El Gamal, and Salehi and also here. In another direction we improve the achievable rate region for the modulo-two sum source network found by Korner-Marton. Finally, we present some ideas about a new approach to the source-channel matching problem in multi-user communication theory. The basic concept is that of a correlated channel code. The approach leads to several new coding problems.

INFORMATION THEORY OF MULTIPLE DESCRIPTIONS, A. El Gamal and T.M. Cover (USA). Consider a sequence of i.i.d. random variables $X_1, X_2, \ldots, X_n$ and a distortion measure $d_m(X_1, \hat{X}_i)$ on the estimates $\hat{X}_i$ of X_i. Two descriptions $i(\underline{X}) \in \{1, 2, \ldots, 2^{nR_1}\}$ and $j(\underline{X}) \in \{1, 2, \ldots, 2^{nR_2}\}$ are given of the sequence $\underline{X} = (X_1, X_2, \ldots, X_n)$. From these two descriptions, three estimates $\hat{\underline{X}}_1(i(\underline{X}))$, $\hat{\underline{X}}_2(j(\underline{X}))$, and $\hat{X}_0(i(\underline{X}), j(\underline{X}))$ are formed, with resulting expected distortions

$$E\{\frac{1}{n}d_m(X_k, X_{mk})\} = D_m, \qquad m=0,1,2 .$$

This problem was posed by Wyner, Ziv, Wolf, Ozarow, and Witsenhausen. We find that the distortion constraints D_0, D_1, D_2 are achievable if there exists a probability mass distribution $p(x)p(\hat{x}_1, \hat{x}_2, \hat{x}_0|x)$ with $Ed_m(X, \hat{X}_m) \leq D_m$ such that

$$R_1 > I(X;\hat{X}_1)$$

$$R_2 > I(X;\hat{X}_2)$$

$$R_1 + R_2 > I(X;\hat{X}_1, \hat{X}_2, \hat{X}_0) + I(\hat{X}_1;\hat{X}_2) ,$$

where I denotes Shannon mutual information. These rates are shown to be optimal for deterministic and degraded distortion measures.

A NEW ACHIEVABLE RATE REGION FOR THE INTERFERENCE CHANNEL, T.S. Han and K. Kobayashi (Japan). A new achievable rate region R* for the general interference channel is presented and evaluated which extends the previous results. The technique used should be regarded as a natural generalization of the Cover's superposition coding (and also of Ahlswede's random coding) to many variables case, where superiority of simultaneous superposition to sequential superposition is pointed out. The constituent subregion R(Z) of the region R* can be expressed simply and explicitly by making full use of a polymatroidal property which holds relying heavily on the assumed independence of auxiliary random variables. The interesting idea consists in intersecting two polymatroids of three dimensions. For the Gaussian interference channel case, comparison of our numerically computed results with those of Carleial and Sato reveals that our region considerably improves the previous ones. Finally, the capacity region of a class of Gaussian interference channel with less strong interference is established, which extends the theorem of Carleial for the strong interference case.

THE WIRETAP CHANNEL WITH FEEDBACK, R.M. Kahn (USA). The issue of privacy was introduced into multi-user information theory by Wyner, whose paper on "The Wiretap Channel" examined the trade-off between the rate at which information can be conveyed across a channel to a legitimate receiver and the fraction of that information which can be held

secret from a wiretapper who receives a degraded version of the legitimate output. Cziszar and Korner extended this result to a general two-output broadcast channel with confidential messages. When feedback is allowed from the legitimate receiver, higher levels of secrecy can be obtained, even when the feedback is fully observed by the eavesdropper (public feedback). The essential concept lies in the generation of common information between the legitimate users which is secret from the eavesdropper and hence may be used as a one-time pad to protect the message. This key generation is an information theory analog of the public key distribution systems of Diffie, Hellman, and Merkle in the field of computational cryptography. This paper discusses these ideas via a simple channel model and then describes an achievable rate region for the general wiretap channel with feedback. (This work was sponsored in part by the U.S. Air Force Office of Scientific Research under Contract F49620-73-0065 and by the Joint Services Electronics Program under Contract N00014-75-C-0601.)

FEEDBACK AND SEMI-FEEDBACK INVESTIGATIONS FOR MULTI-USER CHANNELS, F.M.J. Willems, E.C. Van der Meulen (Belgium) and J.P.M. Schalkwijk (The Netherlands). Feedback and semi-feedback strategies are investigated for the additive white Gaussian noise multiple access channel, the discrete memoryless multiple access channel, the additive white Gaussian noise broadcast channel, and the additive white Gaussian noise interference channel.

Motivated by Ozarow's doctoral dissertation (1979), a semi-feedback scheme is presented for the additive white Gaussian noise multiple-access channel which yields rate pairs outside the non-feedback capacity region. For the additive white Gaussian noise broadcast channel a feedback scheme is developed which uses a common message and appears more general than the scheme presented by Ozarow (1979), also in his dissertation. For the discrete memoryless multiple access channel it is shown that with semi-feedback one can reach the same achievability region as Cover and Leung-Yan-Cheong (1976) found with complete feedback. This result extends a result by Dueck (1979). For the additive white Gaussian noise interference channel an example is given which shows that for this channel feedback may increase the capacity region, as we already know it does for the multiple-access channel and broadcast channel. The example uses a constructive feedback scheme.

ON THE CAPACITY OF AN n-RECEIVER BROADCAST CHANNEL WITH PARTIAL FEEDBACK, C. Leung (Canada). It has recently been shown by Dueck that partial feedback can increase the capacity region of a memoryless broadcast channel. This was done by demonstrating that for a certain two-receiver memoryless broadcast channel, the region achievable with partial feedback is larger than no-feedback capacity region. In this paper, this two-receiver example is generalized, and the capacity regions of the resulting n-receiver channel with no feedback C_{NFB}, partial feedback C_{PFB} and complete feedback C_{CFB} is a proper subset of C_{PFB} which is in turn a proper subset of C_{CFB}.

SESSION A3

Communication Systems I

ADAPTIVE EQUALIZER FOR CARRIER MODULATED DATA TRANSMISSION, N.C. Mohanty (USA). An adaptive equalizer, based on a minimum mean square error criterion, has been derived for the purpose of extracting carrier modulated data transmitted through an unknown and asymmetric channel. The weights of the equalizer are obtained by using a simple formula containing the transform of the parallel channels. The performance of the equalizer is expressed in terms of the variance of the estimation error and the error is much less than that of direct demodulated data.

EMBEDDED PILOT SIGNALS FOR ADAPTIVE SIGNAL EXTRACTION IN MULTI-CHANNEL ENVIRONMENTS, B.G. Agee and W.A. Gardner (USA). The concept of using a broadband source-embedded pilot signal for receiver-site adaption, used in the telephone industry as an early technique for channel equalization, is applied here to signal extraction in multichannel environments. Multiple-stage adaptive receiver structures are described for two methods of embedment, and system performance is analyzed for several two-input mixtures of signal and noises. Results are then generalized to several inputs and interpreted for a number of applications in telecommunications and array processing. Additionally, several known results in these fields are reinterpreted in terms of the embedment concept to clarify the potential of this technique in these applications.

ADAPTIVE CHANNEL ENCODING FOR MULTIPLEX TRANSMISSION OVER DISCRETE CHANNELS HAVING VERY VARIABLE ERROR RATE, A. Bernardini and G.M. Poscetti (Italy). A method for improving the performance of multiplex transmission over discrete channels affected by very variable error rate is described. Adaptive channel encoding, that takes into account both the error statistics on the binary multiplex message and the statistics of the user access to the system, is employed. Comparisons of practical results in a digital radio relay system with the theoretical upper bounds of the overall capacity of the system are made. The obtained improvements

are significant and have practical applications in the case of newly designed digital networks.

DIFFUSION APPROXIMATIONS FOR THE ANALYSIS OF DIGITAL PHASE LOCKED LOOPS, H.J. Kushner and H. Huang (USA). Recent results for getting diffusion limits of a sequence of suitably scaled stochastic processes are applied to the synchronization problem for a digital phase locked loop (DPLL). The discrete time parameter error processes is suitably amplitude scaled and interpolated into a continuous time parameter process. For small filter gains and symbol intervals, a diffusion process approximation is rigorously obtained. This approximation is a Gauss-Markov process and it yields approximate error variances, passage time distributions, correlation properties, (among other properties) for the DPLL. The tracking problem when the clock drifts is also treated. The technique is applicable to a wide variety of related problems, to get continuous time Markov systems which are easier to analyze the original (continuous or discrete time) systems which they approximate. In fact, a currently common method attempts to handle the same problem by getting an 'equivalent' PLL and then using a linearization to get the error variances. Close examinations of this latter formal technique shows that its implicit assumptions are similar to our assumptions. The method of the paper is versatile and it has been used on many problems; e.g., adaptive quantizer, adaptive antenna array and various types of phase locked loops with wide band signal and noise inputs.

PHASE SEQUENCE ESTIMATION IN THE PRESENCE OF RAYLEIGH FADING, S.R. Robinson and D.E. Meer (USA). Maximum A Posteriori (MAP) sequence estimation is used to estimate (modulo-2) the phase of a signal with rapid amplitude (Rayleigh) fluctuations. The sequence estimation is made tractable by quantizing the estimates to a finite number of levels in $(-\pi,\pi)$ so that a recursive (Viterbi) algorithm can be used. Expressions for predicted mean-square-error are presented and verified by computer simulation. The phase estimation algorithm is implemented assuming that a perfect measurement of the amplitude of the signal realization is available; however, simulation results indicate that the estimator's performance is relatively insensitive to the accuracy of the amplitude measurements. The estimator is shown to outperform a phase-locked loop (PLL) by roughly 2-6dB for constant signal amplitude. For a signal with

rapidly fading (Rayleigh) amplitude, the improvement in performance is convervatively predicted to be 10dB. (This research was supported in part by the Air Force Office of Scientific Research under AFOSR 76-3063C, in part by the National Science Foundation under NSF-Eng. 7712946 and in part by the Office of Naval Research under N0014-76-C-0279-P0004.)

ENTROPY AND ABSOLUTE PHASE DEMODULATION, R.S Bucy (USA), J.M.F. Moura (Portugal), and A.J. Malinckrodt (USA). The problem of absolute demodulation has been studied by many authors in the context of the suboptimal demodulator phase locked loop. In this paper we study the performance improvement obtainable by implementation of the optimal by implementation of the optimal nonlinear filter. Further, the phenomenon of cyclic slips is shown to be connected to the entropy of the conditional distribution of the phase given the observations. The statistical properties of the slip distribution of an optimal phase estimator based on the optimal non-linear filter are studied via Monte Carlo simulation. (This work was partially supported by NATO Scientific Affairs Division under grant 157/79/80, by the Air Force Office of Scientific Research under AFOSR-3100, by JNICT under 118.79.80, and by Instituto Nacional de Investigacao Cientifica.)

SESSION A4

Radar

MAXIMUM LIKELIHOOD ESTIMATION IN DETECTION OF RADAR SIGNALS, R.N Madan and J.M. Guild (USA). For noncoherent detection of signals in a radar receiver, a linear detector is employed. The detection threshold is set by the Neyman-Pearson criterion, which requires the detection probability to be maximized for a given probability of false alarm. For a linear detector the detection threshold T is parameterized in terms of a multiplier K applied to an estimation of the mean x of the probability density of noise. In this paper we study the effects of estimation of x on the threshold multiplier K in order to maintain a predetermined probability of false alarm. Depending upon the variance of the estimate of the mean, the threshold multiplier is elevated to maintain a fixed probability of false alarm. The elevation of the threshold results in a loss of detection sensitivity. Following the maximum likelihood estimation (MLE) scheme to estimate the mean of the noise process, we show that the MLE approach leads to a reduction in detection desensitization as compared to the loss in the mean squared error (MSE) scheme. Qualitative and quantitative results are reported in the form of a plot and two tables with values for comparing the two schemes, MLE and MSE.

THE APPARENT DISPARITY BETWEEN THE RESPONSES OF A MONOPULSE RECEIVER TO JAMMERS AND TO PASSIVE TARGETS, I. Kanter (USA). A monopulse receiver exhibits three apparently distinct types of average response when the radar sees two jammers, two passive targets, or one of each. This variety of responses are shown to be special cases of a general formula which applied to two independent targets with uniformly distributed phase difference.

A DOPPLER ESTIMATION CIRCUIT FOR AN ADAPTIVE MTI IN THE PRESENCE OF A CHIRP WAVEFORM IN A TRACKING RADAR, T. Bucciarelli and D. Ricardi (Italy). A problem of interest in mobile radar systems is the extraction of useful information (range, speed) in presence of undesired echoes (sea clutter, weather clutter, ground clutter, angels). A

conventional moving target indicator (MTI) cannot be used for the presence of a disturb carrier (due to the platform motion and/or to the wind) which shifts the power spectrum. Different approaches have been used to avoid (or to reduce) the influence of this carrier: the well known MTD (moving target detector) or AMTI (adaptive MTI). In the latter solution the major problem is the estimation of the doppler carrier which can be compensated by a proper mixing circuit. It is obvious that this estimation doesn't optimize the performances of the canceller as the influence of the magnitude correlation between following echoes is negelected. A closed loop estimation circuit is proposed which is able in a few sweeps to measure the input carrier avoiding the influence of the stagger and the frequency agility, nearly always present in modern radars for ECM reasons. The input signal is one sweep delayed and the phase is measured between the delayed and undelayed signals; so an error is obtained due to the difference between the input carrier (with its doppler spectrum) and the feedback carrier. This error is clearly influenced by the transmission carrier and pulse repetition frequency changes. The physical source of error is the radial relative speed of target and platform and this is not affected by the radar features; so from the knowledge of the frequency parameters of the system (prf and transmission carrier) this error can be compensated.

THE EFFECT OF THRESHOLDING IN REDUCING GLINT FROM EXTENDED TARGETS, I. Kanter (USA). By thresholding either the sum channel amplitude or magnitude of the imaginary part of the output of a monopulse receiver, or both, one can reduce the angular errors associated with the tracking of an extended target. Formulas are derived which give the achievable glint reduction and the fraction of data rejected as a function of the two thresholds. The analysis is valid for arbitrary location of the target in an arbitrary antenna pattern.

LINEAR VS LOGARITHMIC FRAME-INTEGRATION FOR COHERENT LASER RADAR, J.H. Shapiro (USA). We have recently developed a system model for a compact heterodyne-reception infrared imaging-radar. From this model it follows that, under high carrier-to-noise ratio (CNR) conditions, single-pixel image signal-to-noise ratio (SNR) is severely limited by turbulence-induced scintillation and target speckle. Multiframe averaging must be used to combat these fluctuations. In this paper we present results comparing

linear and logarithmic frame-averaging systems. For glint targets viewed through strong atmospheric turbulence, logarithmic averaging is found to be far superior to linear averaging. For speckle targets in the absence of turbulence, linear averaging is at most 3dB better than logarithmic averaging; the logarithmic processor is clearly superior for speckle targets viewed through strong turbulence. The preceding results apply to single-pixel targets. The subjective difference between linear and logarithmic frame-averagers operating on multi-pixel targets has been probed by use of computer simulation. The results obtained for strong turbulence indicate the superiority of the logarithmic processor.

IMPLEMENTATION AND PERFORMANCES OF NAR-AGC ADAPTIVE DETECTION SYSTEMS, B. Picinbono and A. Ouamri (France). In the last symposium on Information Theory was presented the principle of a Noise Alone Reference Automatic Control (NAR-AGC) system in order to achieve adaptive detection in presence of non-stationary noise. We remind that the NAR property means that it is possible to extract a functional of the observation which has the same value in the presence or absence of a known signal. Then this functional is only depending of the noise. In the case of an AGC system, this functional is a power estimator which allows us to estimate the noise power even in the presence of a strong signal. Nevertheless, the effective implementation of the system presented was difficult because of the necessary calculation at every time instant of a quadratic form of the observation on a large matrix. In this paper we present some new possible versions of NAR-AGC systems and we discuss their performances. In particular we compare the complexity of the calculations in order to realize a practical implementation. The performances of various possible solutions are compared and discussed.

SESSION A5

Coding I

GRAPH THEORETIC APPROACHES TO THE CODE CONSTRUCTION FOR THE TWO-USER MULTIPLE-ACCESS BINARY ADDER CHANNEL, T. Kasami (Japan), S. Lin, V.K.W. Wei (USA), and S. Yamamura (Japan). In this paper, we relate coding for the two-user multiple-access binary adder channel to a problem in graph theory, known as independent set problem. Graph-theoretic approaches to coding for both synchronized and nonsynchronized two-user adder channels are presented. Using Turan theorem on the independence number of a simple graph, we are able to improve the lower bounds on the achievable rates of uniquely decodable codes for the nonsynchronized adder channel. We show that the rates of Deaett-Wolf codes for the synchronized adder channel fall below the bounds. Finally, synchronizing sequences for the nonsynchronized adder channel are constructed. (This research is supported in part by the National Science Foundation under ENG 75-05151.)

CODING FOR T-USER BINARY SYMMETRIC BROADCAST CHANNELS, S.C. Chang (USA). Coding for T-user binary symmetric broadcast channels are studied. T independent information sources send messages from a common transmitter to T separate receivers via a T-user broadcast channel. The T-user broadcast channel consists of T components which are binary symmetric channels with crossover possibilities $P_1<P_2<\ldots<t_T$.

Basic properties of T-user broadcast codes are derived, such that the constructive broadcast codes can correct $t_1<t_2<\ldots<t_m$ component-channel errors. Bounds on the achievable rates are found. Some coding schemes are proposed which are close to the theoretical bounds. The schemes indeed improve the common engineering solution of time-sharing a transmitter among T separate receivers.

GROUP CODES FOR THE M-RECEIVER GAUSSIAN BROADCAST CHANNEL, C. Downey and J. Karlof (USA). The M-RECEIVER GAUSSIAN BROADCAST CHANNEL is a model of a communication system in which a single codeword is transmitted over M distinct

Gaussian channels and is received by M receivers. The receivers have no contact with each other and the channels have different signal to noise ratios. According to the signal to noise ratio of its channel, each receiver decodes a different amount of information from the received word. The purpose of this paper is to define the concept of group code for the M-Receiver Gaussian Broadcast Channel and study permutation codes as a special case. Such a code is generated by an initial vector x, a group G of orthogonal n by n matrices, and a sequence of subgroups of G. The subgroups are used to partition the codewords into subsets, called clouds. For each channel we form a different set of clouds. The codewords in the same cloud represent the same message to that channel's receiver. We state conditions on the subgroups and the initial vector that are needed to generate good codes (in terms of minimum distances). We use variant II permutation group codes as examples.

ON THE COMBINATIONAL AND DELAY COMPLEXITY OF ASYMPTOTICALLY GOOD CODES, Y. Imber and J.E. Savage (USA). In this paper the complexity of decoders for the asymptot cally good Justesen codes and the iterated Justesen codes intr duced by Sugiama, Kasahara, Hirasawa, and Namekawa [SKHN] are investigated and new bounds are derived. We present a decoding scheme for Justesen codes and derive an upper bound on its combinational complexity that improves on the best known upper bound. Furthermore, we derive bounds on the delay complexity of the Justesen codes as well as for the SKHN codes. Finally, we present and analyze a new class of asymptotically good codes generated by using the Justesen codes as inner codes and an RS code as an outer code. (This work was supported in part by the National Science Foundation under grant ENG 75-17614.)

BILINEAR CYCLIC CONVOLUTION ALGORITHMS OVER FINITE FIELDS, S.D. Morgera and M.D. Wagh (Canada). This paper explores the structure of bilinear cyclic convolutional algorithms over finite fields. The algorithms derived here are valid for any length not devisible by the field characteristic and are based upon the small length polynomial multiplication algorithms. The multiplicative complexity of these algorithms is small and can be decreased by enlarging the field of constants. The linear transformation matrices A,B (premultiplication) and C (postmultiplication), defining the algorithm, have block structures which are related to one another. The rows of A and B and the columns of C are

maximal length recurrent sequences. Because of this highly regular structure of A,B, and C, these algorithms can be very easily designed even for large lengths. The applications of these algorithms to compute linear convolutions and for R-S decoding are also examined. (This work was supported by NSERC grant A0912.)

SESSION B1

Quantum Channels

NONCOMMUTATIVE PROBABILITY MODELS IN QUANTUM COMMUNICATION AND MULTI-AGENT STOCHASTIC CONTROL, J.S. Baras (USA). In this paper we present a survey of basic results in quantum communication theory that utilize so called noncommutative probability models. We indicate by means of examples how these mathematical methods can lead to actual computations in specific examples. We offer a careful review of these noncommutative models and we observe the similarities with desired features in the representation of the statistics in multi-agent stochastic control problems. We then give suggestions for interpreting some of the basic constructs of quantum models in the language of multi-agent stochastic control systems. (This research was partially supported by the National Science Foundation under grant ENG 75-20900, and by the Army Research Office contract ARO DAAG 29-77-C-0042.)

OPTIMAL POINT PROCESS ESTIMATORS FOR GAUSSIAN OPTICAL FIELD INTENSITIES, F. Davidson and Y.C. Park (USA). The real and imaginary parts of the analytic signal description of a Gaussian optical field with exponential covariance function evolve as a pair of coupled Gauss-Markov diffusion processes. Application of the Ito differential rule to the sum of the squares of these two components yields a stochastic equation of evolution that can be used to obtain a stochastic equation of evolution for the Gaussian optical field intensity itself. This last one dimensional equation is of the form of a Markov (but not Gauss-Markov) diffusion. It was used to obtain a one dimensional equation of evolution for the posterior conditional probability density for the optical field intensity given observations of photoelectron emission times. Numerical solutions to this equation using actual data were used to obtain minimum mean square error (MMSE) estimates of the field intensity as a function of time. In addition, a pair of coupled stochastic equations of evolution for approximately MMSE estimates of the field of intensity and its variance were obtained. Numerical solution to these equations using the same data sets as before produced intensity estimates that agreed to within a few percent of the exact MMSE intensity estimates. The approximate equations have the advantage that they require only a small fraction of the computational time for solution as the exact equations.

VARIABLE STRUCTURE NONLINEAR QUANTUM MECHANICAL FILTER FOR A VECTOR-VALUED SYSTEM PROCESS WITH THE SEMI-MARTINGALE DECOMPOSITION, D.D. Ilic (USA). When the quantum mechanical stochastic process to be estimated is vector-valued, the essentially quantum mechanical problem of simultaneous observations arises, and two independent, inherently non-classical, problems must be solved: (1) optimal simultaneous quantum observation and (2) optimal postprocessing of observations. Spectral calculus for normal operators in Hilbert spaces is used for design of optimal (in the minimum error variance sense) simultaneous quantum observation, while the optimal postprocessing is based on optimization over σ-algebras method. Both methods have been developed by the author elsewhere.

The new Fundamental Lemma for simultaneous observations in quantum mechanics is stated and applied.

The only assumption imposed on the stochastic process to be filtered is that it possesses a semi-martingale decomposition with respect to the global past history of the dynamic system and involved probability measures. It is demonstrated that the observed eigenvalue stochastic process has a semi-martingale decomposition and the recursive filter representation is obtained by the innovations method. The resulting filter is the most general existing discrete-time stochastic filter.

OPTIMAL CODING AND DECODING OF A RANDOM TELEGRAPH WAVE FOR TRANSMISSION THROUGH A POISSON TYPE CHANNEL, A.A. Lazar and S.C. Schwartz (USA). The optimal coding and decoding of a random telegraph wave for transmission through a Poisson type channel is considered. The observation process is a counting point process described by a stochastic differential equation of the type:

$$dN_t = \lambda_t dt + dM_t, \qquad 0 \leq t \leq T,$$

where $\lambda_t, 0 \leq t \leq T$, represents the random intensity rate (RIR)

and $M_t, 0 \leq t \leq T$, is a martingale.

The aim of our investigation is to represent the RIR as a function of the "information bearing process" X and the observations N, i.e., $\lambda_t(X,N), 0 \leq t \leq T$, such that we attain or come close to some optimal properties.

λ is determined from among the class of codes satisfying a peak and average power constraint. Three optimality measures are considered: the estimation (m.m.s.e.), detection

(maximum power) and information theoretical (maximal mutual information) criterion. Letting X be a random telegraph wave, it is shown that the optimal coding is linear and does not require feedback. An analogy to the optimal transmission of a Gaussian random process through the white Gaussian channel is also presented.

PERFORMANCE OF QUANTUM SIGNALS IN UNIMODAL AND BIMODAL OPTICAL COMMUNICATIONS, C.W. Helstrom (USA). The performance of two-photon coherent-state and integral-quantum signals in binary optical communications will be compared, under the constraint of fixed average probability of error, with that of ordinary coherent signals for noisy unimodal and bimodal channels of known and random phase. The manner in which the advantage of these quantum signals over ordinary coherent signals vanishes as the channel transmittance goes to zero will be illustrated. (This material is based upon research supported by the National Science Foundation under grant ENG77-04500.)

DIRECT AND INDIRECT QUANTUM MEASUREMENTS YIELD EQUAL MAXIMUM INFORMATION, L.B. Levitin (Germany). A quantum system is considered, which states are random, occurring with probabilities $p_i (i=1,2,\ldots)$ and described by density operators $\hat{\rho}^{(i)}$ in a separable Hilbert space H_1. Quantum information obtainable by direct (respectively, indirect) measurements is defined as the least upper bound $I\{\hat{\rho}^{(i)};p_i\}$ (respectively, $J\{\hat{\rho}^{(i)};p_i\}$) of Shannon's information about the state of the system in the outcome of a quantum-mechanical measurement, associated with an orthogonal resolution of the identity in the space H_1 (respectively, in the tensor product space $H_1 \otimes H_2$, where H_2 is a separable Hilbert space corresponding to an auxiliary quantum system). The least upper bound is taken over all possible direct (respectively, indirect) measurements.

The following theorem solves a controversial problem of optimality of indirect vs direct quantum measurements.

Theorem: For any set of density operators $\hat{\rho}^{(i)}$ in a separable (infinite-dimensional) Hilbert space, which occur with probabilities p_i such that $H=-\sum p_i \ln p_i < \infty$,

$$J\{\hat{\rho}^{(i)};p_i\}=I\{\hat{\rho}^{(i)};p_i\}$$

THE CUTOFF RATE REGION FOR MULTIPLE ACCESS OPTICAL COMMUNICATION SYSTEMS, P. Narayan and D.L. Snyder (USA). The "cutoff rate region" for a multiple access channel is a natural generalization of the cutoff rate parameter for a single user channel. In this paper, we define the cutoff rate region and explore some of its properties and implications for the coordinated design of the encoders and modulators of the multiple users. We find for block encoding that the cutoff rate is the same with and without frame synchronization between the multiple users. Choices of modulation are identified that maximize the cutoff rate region for an additive thermal-noise limited channel subject to average energy and bandwidth constraints and for an additive shot-noise limited channel subject to average energy and peak amplitude constraints. (This work was supported by the National Science Foundation under grant ENG76-11565 and by the National Institutes of Health under grant RR00396 from the Division of Research Resources.)

ON THE CAPACITIES AND ERROR PERFORMANCE OF THE FREE-SPACE OPTICAL CHANNEL, H.P. Yuen (USA). For coherent state and two-photon state transmitters, the error behavior of direct detection, homodyne, and heterodyne receivers are analyzed and compared for the free-space channel as a function of bandwidth, signal level, and data rate with special emphasis on PPM signaling. A bound on the highest achievable quantum capacity is used as a benchmark.

For bandlimited systems with high signal level, it is concluded that homodyne and heterodyne systems can greatly outperform a direct-detection system.

SESSION B2

Communication Systems II

*TIME SLOT ASSIGNMENTS IN AN SS/TDMA SYSTEM WITH MINIMUM SWITCHINGS, K.S. Natarajan and S.B. Calo (USA). The problem of optimal time slot assignment in a satellite-switched time division multiple access system with a minimum number of switching modes is considered. Lower bounds on the optimal transmission time required are derived. Three heuristic algorithms are proposed and studied for the assignment problem; and lower bounds on the performance of the approximation algorithms are derived. Experimental results showing the effectiveness of two of the algorithms in producing near-optimal solutions have also been obtained.

NARROWBAND INTERFERENCE SUPPRESSIONS IN PSEUDO-NOISE SPREAD SPECTRUM SYSTEMS, J.G. Proakis and J.W. Ketchum (USA). This paper addresses the problem of demodulating a binary-modulated pseudo-noise (PN) spread spectrum signal that is corrupted by narrowband interference, white Gaussian noise, and with/without channel multipath. The emphasis of the paper is on the performance of adaptive filtering techniques for suppressing the narrowband interference and on the performance of equalization techniques for reducing inter-chip interference in the PN signal. Results will be presented that illustrate the advantages of interference suppression and equalization.

HARD-DECISION VERSUS SOFT-DECISION DECODING FOR FREQUENCY-HOPPING MULTIPLE-ACCESS SYSTEMS IN A RAYLEIGH FADING ENVIRONMENT, O. Yue (USA). In comparing two proposed frequency-hopping mobile radio systems for digitized speech, Goodman et al (1980) have observed that the system employing multiple-frequency-shift-keying (MFSK) can accommodate many more users than the one with differential-phase-shift-keying (DPSK). Besides the differences in coding and modulation methods, the MFSK system uses hard-decision decoding while the DPSK one uses soft decisions. In this paper, we show that using soft decisions in the MFSK system causes the performance to degrade considerably, and that the DPSK system with hard decisions

can support about twice as many users as the original one. These results are not surprising because, while soft-decision decoding is optimum for Gaussian noise, the multiuser interference is non-Gaussian.

A METHOD OF SIGNAL DESIGN FOR SPREAD SPECTRUM SYSTEMS, K.V. Cai and G.R. Cooper (USA).A modified procedure for designing large sets of frequency hopped signals for spread spectrum multiple access systems is presented. This procedure yields signals for which all out-of-phase autocorrelation functions and crosscorrelation functions are small for all relative time shifts.

It is well known that non-repeating integer sequences of length p-1, p prime, exhibit a "one-coincidence" aperiodic crosscorrelation property when the power residue sequence of any primitive root of p is used as a permutation operator. In this paper it is shown that if the index sequence of the prime number is used as the initial sequence, the set of difference values between any pair of sequences has non-repeating elements for any relative shift greater than zero.

The above result is proven and its implication with respect to the design of signal sets with good correlation properties is discussed. The characteristics of the resulting signal sets are described and several computed results are prcvided to illustrate the effectiveness of the method. These computed results are for signals having a time-bandwidth product on the order of 5000 and indicate that the maximum crosscorrelation peaks do not exceed the rms crosscorrelation envelope by factors larger than about three.

SPECTRA OF LINEARLY CODED DIGITAL SIGNALS, J.B. Bezerra and D.S. Arantes (Brazil). The automata theory is used to find the spectral properties of digital signals coded by convolutional codes. The transfer matrix of the encoder is obtained in a straightforward way from the generator matrix of the code. This result as well as the fact that a linear block code is a particular kind of convolutional code are used to determine the equivalent parallel encoder of linear block codes and thus to find their spectral properties.

SPECTRAL ANALYSIS OF THE POWERS OF A PAM DIGITAL SIGNAL, S. Pupolin (Italy) and G. Bilardi (USA). The computation of the spectral density of the powers of a PAM digital signal $x(t)=y^n(t)$ has been performed. The formula, which gives the continuous as well as the discrete component of the spectrum, is obtained by an extension of the spectral analysis at the output of a discrete-time Volterra system. The result is general, since the only assumptions made are: mutually independent symbols, and square summable impulse response of the digital modulator. Also, it has been proved that under the above assumptions the discrete part of the spectrum is given by the deterministic spectrum of the mean value of the cyclostationary version of $x(t)$.

SESSION B3

Cryptography

A CRYPTOSYSTEM MAKING USE OF THE CORRELATION BETWEEN MESSAGE AND KEY, S.C. Lu (China). A cryptosystem making use of the correlation between the message and the key is proposed. The cryptosystem is based on variable length source coding for correlated information sources. It is shown that the channel capacity required to transmit cryptogram is less than the entropy rate of the message and that the system is secure against ciphertext only attack.

MAXIMUM LIKELIHOOD ESTIMATION APPLIED TO CRYPTANALYSIS, D. Andelman (USA). A general cryptanalysis method is presented based on statistical estimation theory. It is applied to two systems of practical interest: Rotor Machines and Substitution- Permutation Networks. To cryptanalyze these systems the finite keyspace is imbedded in a continuous set and the key estimate is a proper quantization of the continuous Maximum Likelihood Estimate.

In our study of rotor machines, the key specifies a set of alphabet permutations, implemented by the rotors. Cryptanalysis of this model is based on maximizing the likelihood function when the rotors are considered as (possibly) noisy communication channels. The correct rotors (permutations) are noiseless channels and therefore extreme points of the parameter set. Using English in a ciphertext only attack, a two-rotor machine is successfully cryptanalyzed. The ciphertext length is only 3 to 5 times the unicity distance.

In the analyzed substitution permutation network the key bits are used to select between pairs of known invertible substitutions (S-boxes). Allowing the key bits to range continuously between 0 and 1, the maximum likelihood estimate of the continuous key is evaluated and quantized. Using a known plaintext attack, a 27 bits key size system is easily and very competitively cryptanalyzed. (This work was supported by the National Science Foundation under grant ENG10173.)

KNAPSACKS WHICH ARE NOT PARTLY SOLVABLE AFTER MULTIPLICATION MODULO q, I. Ingemarsson, Sweden. An ordered knapsack is a set of K positive integers. X is an array of K bits and ones of the same length as K. S is the scalar product of K and X.

Given S and K, it is usually a very difficult problem to find X. In a special case, where each entry is larger than the sum of all the previous ones, it is easy to find X. Such knapsacks are used by Merkle and Hellman in a public key cryptosystem.

We are interested in a larger class of knapsacks with the following definition.

Definition: An entry in a partly solvable knapsack is larger than the sum of the rest of the entries in the knapsack.

If K is partly solvable, we can obviously find some of the components in X from S and K.

Tore Herlestam (1978) has proposed an iterative method to possibly derive X from S and K. Even if K is not partly solvable, we might obtain a partly solvable knapsack by multiplication of K with a suitable integer modulo q. The knapsack is reduced by removing the derived components and the procedure is repeated.

Not all knapsacks, however, are transformed into partly solvable knapsacks by multiplication mod q. We have derived classes of knapsacks which are not partly solvable after multiplication mod q.

CRYPTANALYSIS OF THE DATA ENCRYPTION STANDARD BY METHOD OF FORMAL CODING, I. Richl, J. Biermeier, D. Gollmann, and F. Winkler (Austria). The Method of Formal Coding (MFC) is a "known-plaintext-attack" against which the DES is not conditionally secure. The main idea of the MFC is to represent every bit of cipher-text as a function in XOR-sum-of-product-form of the 56 key-bits and the 64 plain-text bits in an efficient way. The MFC-complexity measure is introduced as the overall sum of the numbers of products necessary to represent the cipher-text bits. It can be shown that this measure is quite adequate to meet the needs of cryptocomplexity. It can be shown that the MFC-complexity of a version of the DES in which all S-boxes are affin, is very small compared with the estimated MFC-complexity of the original DES. At this time of our investigations of the DES by the MFC, the limits are given by the enormous amount of the computer-memory which is needed.

The investigation of the S-boxes using the MFS and their realization by coordinate descriptions of finite automata in the sense of Rainbridge brought us the following results:

[illegible] approval of the conjectures by Professor Hellmann concerning S-box 4.

If the S-boxes are linear or affin, the MFS-attack is successful.

[illegible] computation of S-boxes which are MFS-optimal.

[illegible] computation of nonlinear and nonaffine S-boxes with small [illegible] complexity.

[illegible] showing how well such "trap-door S-boxes" can be hidden.

We [illegible] FORTRAN dialog-implementation of the DES with graphic support.

[illegible] PUBLIC-KEY SYSTEMS, D. Dolev and A. Yao [illegible]. We are concerned with the security of public-key [illegible] traitors and intruders). The current ways of analyzing protocols are ad hoc, and do not [illegible] why some schemes are bad, while others seem secure. In this paper, we develop ways to [illegible] and analyze the security of protocols against a [illegible]. We will prove that some general classes of [illegible] traitor-insecure while slightly different [illegible] traitor-secure.

[illegible] MESSAGE EQUIVOCATION FOR SIMPLE SUBSTITUTION CIPHERS, [illegible]. For simple substitution ciphers an exact expression and bounds are derived for the message equivocation in terms of the key equivocation. It is established that the message equivocation approaches the key equivocation exponentially fast for discrete memoryless sources. It is observed that the exponential behavior of the message equivocation is not determined by redundancy in the message source, but by either the symbol probabilities which are [illegible] or the sum of the two [illegible] probabilities. This work was supported in part by [illegible] grant [illegible].

ON COMPUTING LOGARITHMS OVER $GF(2^p)$ OR AN ATTEMPT TO SWINDLE MITRE CORPORATION, T. Herlestam and R. Johannesson (Sweden). Some public key distribution systems are based on the difficulty of computing logarithms over $GF(2^p)$, among them one used by MITRE Corporation.

In this paper, a new heuristic algorithm for computing logarithms over $GF(2^p)$ is presented, based on the interdependent relations

$$f_{rs}(t)=t^{-2} f(t)^2$$

and

$$\log f_{rs}=-2^r + 2^s \log f,$$

$GF(2^p)$ being implemented as the ring of residues modulo prime polynomial of degree p over GF(2).

Numerical tests have been carried out when p=13,17,19, and 31. As a result, the logarithms of hundreds of randomly chosen elements of $GF(2^p)$ have been computed in very short running times and without a single failure.

Thus it is concluded that the logarithm problem for $GF(2^p)$ may not be as difficult as previously thought.

ON SECRET SHARING SYSTEMS, E. Krasniansky, J.W. Greene, M.E. Hellman (USA). Methods have been suggested by Shamir and Blakely for dividing a secret S into n pieces such that S is recoverable from any k of them, while knowledge of k-1 pieces leaves S completely undetermined. In this paper we present a more general approach to sharing the secret. The pieces which are the same size as S, are obtained by applying a public linear transformation to the secret data.

Our method is closely related to Blakely's, but is deterministic and has guaranteed performance. Shamir's polynomial interpolation scheme is shown to be a special case of our method, anf for some values of k and n we can design more efficient systems.

Our method can be generalized to protect more than one secret without increasing the information content of each of the n pieces. Or equivalently, we can protect a large secret with each piece being of smaller size than the secret. While the secret is then not completely protected, we show that it is adequately protected for most purposes.

We discuss possible generalizations and derive general upper bounds (which apply to any secret sharing scheme) on the number of pieces as a function of k and the secret size. We also discuss the problem of detecting deliberate tampering by one of the trustees holding the n pieces of information and suggest a method based on one-way functions to detect such tampering.

ON FACTORING AND RANDOM GRAPHS, J.M. Reyneri and M.E. Hellman (USA). The RSA public-key cryptosystem relies for its security on the difficulty of finding proper factors of large composite integers. Richard Schroeppel has developed a rapid algorithm, for factoring an integer N, which appears to run in time $O(\exp\sqrt{\ln N \ln\ln N})$. This is not fast enough to threaten the RSA system. Schroeppel has suggested an additional modification to the algorithm, which was motivated by the fact that only $O(\sqrt{m})$ random binary m-vectors with a single 1 are needed before a dependent subset is expected. The modification leads to improved performance under the assumption that sets of random binary m-vectors with two 1's behave similarly.

In this note, we show that a set of binary m-vectors with two 1's can be identified with an m-vertex graph. A result from graph theory is then applied to show that $O(m)$ random binary m-vectors with two 1's are needed before a dependent subset is expected, and that therefore the addition does not significantly improve the running time of the basic algorithm.

SESSION B4

Shannon Theory I

*THE ERGODIC AND ENTROPY *THEOREMS REVISITED, P.C. Shields (USA). The usual proofs of the individual ergodic theorem of Birkhoff and the entropy theorem of Shannon, McMillan, and Breiman use tricky combinatorial or analytic arguments which are unrelated to the way information theorists use these theorems. We present proofs of these theorems which are parallel in structure and close in spirit to the usual sample path and counting concepts used elsewhere in information theory. Our basic tool is a lemma about properties of measure preserving transformations T which goes as follows. Let $P_n(x)$ be a measurable property of the sequence $Tx, T^2x, \ldots, T^nx$ such that for almost all x there is an n such that $P_n(x)$ is true. We prove that if N is sufficiently large than for most x, most of the sequence $Tx, T^2x, \ldots, T^Nx$ is contained in disjoint blocks $T^{m+1}x, T^{m+2}x, \ldots, T^{m+n}x$ for which $P_n(T^mx)$ is true. This result enables us to estimate measures of sets and count sample paths which lead to proofs of the ergodic theorems. (This work was supported in part by NSF grant MCS7807739-A02.)

THE ASYMPTOTIC REDUNDANCY OF HUFFMAN CODING, R.J. McEliece (USA). By the redundancy $r(X)$ of a discrete random variable X we mean the difference $r(X)=L(X)-H(X)$, where $H(X)$ is the binary entropy of X and $L(X)$ is the minimum possible average length for a uniquely decodable binary code for X. Shannon showed in 1948 that $0 \le r(X) < 1$ for any X. Here we get more detailed bounds on $r(X)$, using the basic idea, not entirely new, that $r(X)$ "almost" depends only on the distribution of the fractional parts of the numbers $-\log_2 P\{X=x\}$. We obtain a lower bound $r(X) \ge \rho(X)$, where $\rho(X)$ is the best possible lower bound that depends only on these fractional parts. We show that $r(X) \le \rho(X) + \sup\{P\{X=x\}\}$. Thus in the absence of large probabilities $\rho(X)$ is a very good estimate of $r(X)$. We show that $0 \le \rho(X) \le G$=Gallager's constant=.086071332, for all X. If X is a uniform random variable on (0,1), $r(X)$=Krichevskii's constant=K=.028766373. In a certain sense a random variable chosen at random will have redundancy K. We remark finally that our methods easily allow us to reproduce Krichevskii's remarkable but relatively unknown result that the normalized redundancy of the n-th extension of a discrete memoryless source approaches K as $n \to \infty$, for almost all such sources. (This research was supported by the Joint Services Electronics Program under contract N00014-79-C-0424.)

ALGORITHMS FOR SLIDING BLOCK CODES (AN APPLICATION OF SYMBOLIC DYNAMICS TO INFORMATION THEORY), R.L. Adler and M. Hassner (USA). The algorithms described are an application and a generalization of coding methods developed in conjunction with an isomorphism theorem for a special class of symbolic models that arise in the qualitative study of general dynamical systems. This class of symbolic models consists of topological Markov chains, which are infinite sequence spaces defined over a finite alphabet and specified by finite lists of excluded blocks, and their homomorphic images. In information theory the very same models are known as finite state channels or, in a source coding context, as nonprobabilistic sources. The observation of this identity provides the link between the two fields and the basis for this paper.

The isomorphism theorem for this class of symbolic models and the coding methods described may be viewed as the nonprobabilistic analogs of Ornstein's isomorphism theorem for B-processes whose operational interpretation is given in terms of noiseless (shift commuting) sliding block maps. However, in contrast to the latter, the shift commuting maps between topological Markov chains (or between their homomorphic images) are constructive in a practical sense and hence result in engineering applications. We present specific applications for both noiseless channel and source coding.

A SLIDING-BLOCK CODE FOR SMALL USER ALPHABETS WITH PERFORMANCE NEAR THE RATE-DISTORTION LIMIT, W.A. Pearlman (USA). We investigate a new sliding-block code for generator/decoder for an i.i.d., unit variance, Gaussian source and squared-error distortion for a size constrained user alphabet. For trellis encodings at 1 bit/source symbol and only four user values, we obtain average distortions of .303 and .301 with decoder lengths of 9 and 10, respectively. These distortions are lower than any yet obtained for a comparable time invariant source coding. They are within 0.8 dB of the rate-distortion bound and surpass the optimal entropy-coded quantizer by 0.7 dB. Moreover, the trellis search effort is much smaller than any previous efforts that use an approximately continuous user alphabet.

SOURCE CODING WITH RESPECT TO A MULTIDIMENSIONAL FIDELITY CRITERION, J.-E. Stjernvall (Sweden). In source coding the discrepancy between the source and the reproduction is given

by a distortion measure as one real number. In this paper we consider multidimensional distortion measures, i.e., measures which give the distortion as set of real numbers. We give the straightforward extensions of the rate-distortion function (RDF) and achievable rate in order to include such distortion measures. The rate-distortion theorem is easily shown to hold also in this case. The main result is a connection between the RDF for the multidimensional distortion measure and a RDF for a onedimensional distortion. This is used to derive the RDF for a stationary discrete time Gaussian source with respect to a multidimensional distortion measure. This measure consists of different frequency weighted mean square error measures.

INFORMATION RATES OF TIME-DISCRETE STATIONARY GAUSSIAN SOURCES, D. Wolf, H.P. Weber, and T. Denker (Germany). The rate distortion functions for time-discrete stationary Gaussian random processes were studied using the mean squared-error fidelity criterion. Three types of sources have been investigated with (a) linearly, (b) non-linearly monotonously, and (c) oscillatorily decaying memory. The influence of the memory type on the information rate is discussed.

THE RATE-DISTORTION FUNCTION ON CLASSES OF SOURCES DETERMINED BY SPECTRAL CAPACITIES, V.H. Poor (USA). The quantity $\sup_{a \in A} R_a(D)$ is considered, where A is a class of homogeneous n-parameter sources and $R_a(D)$ denotes single-letter MSE rate-distortion function for the individual source a. In particular, the case in which the class is specified in terms of spectral information is treated for general classes of spectral measures whose upper measures are capacities (in the sense of Choquet) alternating of order two. This type of class includes many common models, and neighborhoods generated by Kolmogorov (total-variation) and Prohorov metrics. It is shown that each class contains a worst-case source whose rate-distortion function achieves the supremum over the class for each value of distortion. This source is characterized as having a spectral density that is a derivative (in the sense of Huber and Strassen, Ann.Stat., vol. 1, pp. 251-263) of the upper spectral measure with respect to Lebesgue measure on $[-\pi,\pi]^n$. Moreover, it is shown that the spectral measure of the worst-case source is closest, in a sense defined by J-divergence, to Lebesgue

measure (which corresponds to a memoryless source). Numerical results are presented for the particular case in which the source spectral measure is a mixture of a Gauss-Markov spectrum and an unknown contaminating component. (This research was supported by the Joint Services Electronics Program under contract N00014-79-C-0424 and by the National Science Foundation under grant ECS79-16453.)

SESSION B5

Coding II

A QUICK-LOOK DECODER WITH ISOLATED ERROR CORRECTION AND NODE SYNCHRONIZATION, C.A. Greenhall, R.L. Miller, and S.A. Butman, (USA). Quick-look inversion by a linear sequential circuit can be used for decoding a clean, hard-quantized, convolutional code stream. For the (7,1/2) code with connection vectors 1011011, 1111001, the raw inversion circuit has an asymptotic bit error rate of 7p, where p is the channel error rate. The problem addressed here is: How can one easily do better? Although syndrome decoding does as well as Viterbi decoding, a much simpler pattern-recognition scheme, operating on the syndrome stream, improves the bit error rate to $133p^2$. The scheme works by recognizing isolated symbol errors.

We also give a node sync algorithm that drives an up-down counter from the syndrome stream. Expected times to resync and to false alarm are estimated as functions of counter design parameters, channel error rate, and bit transition density. (This paper presents the results of one phase of research carried out at the Jet Propulsion Laboratory, California Institute of Technology, under contract NAS 7-100, sponsored by the National Aeronautics Administration.)

SEQUENTIAL DECODING FOR BURST ERROR CHANNELS, L.R. Bahl, J. Cocke, C.D. Cullum (USA) and J. Hagenauer (Germany). Sequential decoding cannot be used directly on burst noise channels, because clusters of errors cause sequential decoders to do an enormous amount of searching, which generally results in storage to time overflow problems. One common method of transforming bursty channels into non-bursty channels is to use interleaving before transmission over the noisy channel, and deinterleaving before decoding. The usual approach is to consider the interleaved channel as a memoryless random noise channel and treat errors as being uncorrelated. Each received bit is considered to have a probability of error equal to the average error probability of the channel. A disadvantage of treating the interleaved channel as a memoryless channel is that the capacity of the channel is lowered, as has been shown by Gilbert.

In this paper, we describe a scheme which uses interleaving/deinterleaving to break up bursts, but does not ignore the correlation between errors. A Gilbert-type Markov model is used to model channels which produce both random and burst errors. During decoding, the probability of error for each bit is estimated from previously decoded data and from the channel model. These estimates are used by the sequential decoder in computing likelihood values. This scheme has two advantages. First, one can transmit at rates higher than those possible if error correlations are ignored. Second, decoding time is reduced since the sequential decoder can adjust its search to take into account the reliability of each bit. This paper describes the basic concepts of the method, some details of implementation with the Stack and Fano sequential decoding algorithms, and the results of computer simulations.

STACK AND INPUT BUFFERS OVERFLOW OF STACK DECODING ALGORITHMS, D. Haccoun and M. Dufour (Canada). Multiple-path variants of the stack algorithm which reduce the computational variability of sequential decoding are presented together with their impact on the behavior of the waiting line in the input buffer. Buffer sizes required for a given overflow probability, as determined by computer simulation, will be given in terms of both channel and decoder parameters. Comparing the variants of the stack algorithm it is observed that an overflow may occur in either the input buffer or the stack. When the stack size is small, it is shown that the average number of computations is the dominant factor for the overflow event rather than the Pareto exponent of the cumulative distribution. On the other hand, for large stack sizes the overflow event is dominated by the tail of the distribution of the computational effort. Trade-offs between these two effects are presented.

Finally, it appears that containing the overflows in the stack rather than in the input buffer is more attractive from a performance and hardware implementation points of view. Exploiting this observation, a technique using a short stack decoder with a retransmission procedure is presented, and computer simulation results about effective rate, error probability, buffer size, etc. are compared to those of the usual sequential decoder. (This research was supported in part by a National Sciences and Engineering Research Council of Canada grant A-9336 and an FCAC-Quebec group EQ-210.)

ON THE CLASS $L_{2,v,1}$ OF CONVOLUTIONAL CODES, A.J. Vinck (The Netherlands). This paper concerns the application of the class $L_{2,v,1}$ of convolutional codes introduced by Vinck, de Paepe, and Schalkwijk (1980). We investigated how the tree structure, connected with the class $L_{2,v,1}$, can be used in the Fano decoding algorithm for convolutional codes. Then, from simulation results it followed that a significant improvement in the distribution of the number of computations (forward and backward moves) per decoded information digit can be realized. Also the average number of computations is reduced considerably. From the class $L_{2,v,1}$, we took the subclass $L_{2,v,v-1}$ of codes with encoder connection polynomials $g_1(D)^{2,v,v-1}$ and $g_2(D)$ such that $g_1(D)$ $Og_2(D)=D^{v-1}$, and optimized the column distance function. These codes can be seen as reserved QLI codes and hence, also reasonable free distance can be obtained. Simulations were carried out for several Binary Symmetric Channel transition probabilities.

BINARY CONVOLUTIONAL CODES DERIVED FROM CYCLIC CODES OVER $GF(2^n)$, G. Sequin (Canada). By considering the input sequence to an $(n,k)_k$ convolutional encoder as a sequence of elements from $GF(2^k)$ and the output as a sequence over $GF(2^n)$, it is possible, in the case when k divides n, to consider encoders which correspond to multiplication by a polynomial $g(D)$ over $GF(2^n)$. It is shown that in this case the polynomial of least degree in the code leads to a minimal polynomial encoder with a polynomial inverse. The class of codes so obtained is shown to form an infinite group under multiplication. When the rate is 1/2, it is shown that a code from the above class and its inverse have the same constraint length and in the case $k=1,n=2$, have the same weight spectrum. The divisors of $D^{15}+1$ afford 80 non-catastrophic encoders and the d_{free} of each corresponding convolutional code is computed. Most of these have a d_{free} close to the optimum and optimum codes of constraint lengths 3,6, and 8 are obtained.

NON-SYNCHRONIZING SEQUENCES IN CONVOLUTIONAL CODES, P. Godlewski (France). This paper is concerned with the problem of symbol synchronization in decoding convolutional codes. The notion of non-synchronizing sequence (NSS) is presented. Such sequences do not exist for all (n,k) convolutional codes. For binary (2,1) codes with constraint length v we show that there always exists a NSS of period less than 2^{2v-1}. Good convolutional codes of rate 1/2 seem to have NSS

with long period. We also study the case of (n,1) codes and consider some acquisition procedures.

ON THE COMPLEXITY OF SEQUENTIAL DECODERS, J.P.M. Schalkwijk and J.A.M. de Brouwer, (The Netherlands). This paper concerns ways of reducing the complexity, the number of computations and the storage requirement, of sequential decoders. Encouraged by earlier results for maximum likelihood (ML) decoders of convolutional codes we were let to an investigation regarding the complexity of the stack decoder and the Fano decoder. In the decoding of block codes syndrome decoding results in a smaller [2] decoding table. To obtain a similar advantage in sequential decoding one has to search a tree of reduced (compressed) noise sequences, i.e., a binary tree with a variable number of noise digits along the branches. We present simulation results comparing the distribution of the number of computations per frame decoded of the reduced tree stack decoder, and of the classical stack decoder.

NEW BOUNDS ON THE PERFORMANCE OF BINARY CONVOLUTIONAL CODES USING VITERBI DECODING ON A BINARY SYMMETRIC CHANNEL, K.A. Post (The Netherlands). For a non-catastrophic binary convolutional code the error events of length k have a minimal weight that can be bounded from below by increasing linear function of k. This implies that with Viterbi decoding on a BSC those noise sequences $\{x_i\}$ for which the (real) sum $x_1+\ldots x_k$ is below an appropriate linear function of k (k=1,2,3,...) can never cause decoding errors. The remaining noise sequences (that may, but need not cause decoding errors) are defined to be "error-suspicious". The probability of error-suspiciousness for a random sequence can be calculated exactly in terms of p, the probability of ones, by random walk techniques. The resulting upper bounds on the decoding error probabilities turn out to have in general a wider domain than Viterbi's union bounds and improve these union bounds considerably for moderate values of the crossover-probability.

SESSION C1

Communication Systems III

THE COMPUTATION CUT-OFF RATE R_{comp} FOR AN OPTICAL CHANNEL WITH MULTILEVEL AM SIGNALING AND DIRECT DETECTION RECEIVERS, V.W.S. Chan (USA). The computation cut-off rate R_{comp} for a free-space optical channel is obtained for multilevel AM signaling and multimode photon-counting direct detection receivers. Maximization of R_{comp} over the signaling levels and signal symbol size is considered. (This work was sponsored by the Department of the Air Force.)

CAPACITY, CUT-OFF RATE, AND CODING FOR A DIRECT-DETECTION OPTICAL CHANNEL, J.L. Massey (Switzerland). It is shown that Pierce's pulse-position modulation scheme with 2^L pulse positions used on a self-noise-limited direct-detection optical communication channel results in a 2^L-ary erasure channel that is equivalent to the parallel combination of L completely-correlated binary erasure channels. The capacity of the full channel is the sum of the capacities of the component channels, but the cut-off rate of the full channel is shown to be much smaller than the sum of the cut-off rates. An interpretation of the cut-off rate is given that suggests a complexity advantage in coding separately on the component channels. It is shown that if short-constraint-length convolutional codes with Viterbi decoders are used on the component channels, then the performance and complexity compare favorably with the Reed-Solomon coding system proposed by McEliece for the full channel. The reasons for this unexpectedly fine performance by the convolutional code system are explored in detail, as are various facets of the channel structure. (This research was performed while the author was a consultant to the Communication Theory Group, Section 331, Jet Propulsion Laboratory, Pasadena, CA, and was supported by NASA contract NAS7-100.)

EFFECTS OF ISI ON VITERBI DECODING, D. Divsalar and J.K. Omura (USA). We examine the performance of convolutional codes with Viterbi decoders that are designed for an AWGN channel with no ISI when in fact there is ISI. In this case,

the Viterbi decoder will be "Mismatched" to the channel. Our approach is based on a generalization of transfer function bounds using pair state diagrams where the bit error probability bound can be computed by an iterative algorithm. We find that the performance of such mismatched coding and decoding over ISI channels can depend on the order of the switching of the output symbols of the convolutional codes. Finally, we extend our results to include the effects of nonlinear channels with memory on such Viterbi decoders.

CUT-OFF RATE EVALUATION FOR DIVERSITY TRANSMISSION WITH RAYLEIGH FADING, J.J. Komo and A. Aridgides (USA). This paper presents cut-off rate, R_o, expressions for equal-strength FSK diversity transmission over the Rayleigh fading channel. The closed form expression for the unquantized R_o for D diversity, which upper bounds the channel performance, is given. R_o expressions are then developed for various quantization levels which show that 8 level quantization yields performance within a few tenths of a dB of the optimum. Tradeoffs between D and the number of quantization levels for equivalent performance are presented as a function of signal-to-noise ratio using the R_o expressions for the unquantized and quantized channels. These tradeoffs illustrate the reduction in signal energy, system bandwidth, and system complexity by increasing the quantization levels which decreases D.

THE COMPUTATIONAL CUTOFF RATE OF CHANNELS HAVING MEMORY, E. Biglieri (Italy). A random coding bound is derived for block coded transmission over channels characterized by a deterministic, finite-memory part followed by the addition of white Gaussian noise (intersymbol interference channels are a special case of these). According to this bound, a "product-measure cutoff rate" can be defined quite naturally for such a class of channels.

POWER-BANDWIDTH PERFORMANCE OF SMOOTHED PHASE MODULATION CODES, J.B. Anderson (Canada), C.-E.W. Sundberg, T. Aulin, and N. Rydbeck (Sweden). Constant envelope phase varying sinusoids of the form $\sqrt{2E/T}\cos(w_c t + \phi(t))$ are studied, in which the phase function $\phi(t)$ follows some coded pattern in

response to data. Power and bandwidth performance are studied for such patterns. The patterns depend on a phase shaping function, a modulation index, h, and a sequence of M-ary underlying changes in phase which are chosen at random. A cut-off rate-like parameter R_o is computed, which guarantees existence of codes at all rates $R<R_o$ bits/T-interval whose error performance varies as $\exp[-N(R_o-R)]$, where N is the code word length in T-intervals. Plots of R_o are given as a function of interval energy E, the shaping function, h, and M. Extensive spectral calculations give the spectra of these phased sinusoids, and their performance is plotted in the power-bandwidth plane. The results give strong evidence that phase codes can approximate any power-bandwidth combination consistent with Shannon's Gaussian channel capacity, and that linear channels are not required for narrowband transmission.

MINIMUM DISTANCE AND BANDWIDTH OF M-ary MULTI-h CONTINUOUS PHASE MODULATED SIGNALS, T. Aulin and C.-E. Sundberg (Sweden). A class of power and bandwidth efficient constant envelope digital modulation schemes is analyzed in terms of the tradeoff between bandwidth and error probability. The class considered is continuous phase, multi-level (M-ary), multi-h (i.e., time-varying modulation indices) signals of both full response and partial response type. New upper bounds on the minimum Euclidean distance are given for full response binary, quaternary, and octal multi-h schemes with 2,3, and 4 different h-values which are varied in a cyclic manner. It is shown that using more than 2 h-values gives little extra gain in E_b/N_o. When the gain in E_b/N_o is considered in a power-bandwidth tradeoff, it is concluded that 2-h schemes with 4 levels are preferable. Considerable gains can be made over the binary multi-h schemes by using 4 levels both for full response and partial response schemes. Examples of such schemes are given in the paper. (This research was supported by the Swedish Board of Technical Development under grant 79-3594.)

PACKET WAITING TIME FOR MULTIPLE ACCESS CHANNELS, A. Ephremides and T. Saadawi (U.A.). We develop an approach for calculating the queueing waiting time at terminals with unlimited buffer space for storing arriving packets that must be transmitted over a multiple access channel. The approach is suitable for a variety of accessing schemes including random access Aloha as well as variants of conflict resolution tree algorithms and reservation based demand access.

The approach is based on modeling the interaction between the competing terminals by a combination of two Markov chains. The central feature behind the interaction is the fact that successful transmission of a packet by a user depends, for a variety of accessing rules and regimes, on the "status" of the other users. Thus it is possible to consider the "state" of a user (represented by the size of his queue) modeled by an imbedded Markov chain whose parameters (transition probabilities) depend on the "state" of the system (basically, the number of users who need service opposed to those who do not). The latter state can also be represented by an imbedded Markov chain whose parameters are in turn functions of the state of the users. Thus it is possible to obtain sets of coupled equations for the steady-state equilibrium distributions of these states. They can readily be solved numerically and the performance of different schemes that can be subjected to this modeling can be calculated.

The approach is utilized in a) the classical slotted Aloha scheme, b) a reservation scheme where reservation packets are broadcast in TDMA fashion over a fraction of the main channel, and c) the classical conflict resolution scheme developed by Capetanakis.

We consider that it is important to take into account the buffering delay, since 1) it is realistic to assume non-rejection of packets in a number of applications including Satellite access networks and 2) packet rejection is costly and drastic means of flow control that produces misleading high performance results for a number of accessing schemes.

CHANNEL SHARING AMONG MANY BURSTY SOURCES, J.F. Hayes (Canada). Techniques for providing transmission facilities to a number of bursty sources are studied. Due to the burstiness of the sources, dedication of resources is not efficient and sharing is indicated. Several techniques for effecting this sharing are compared on the basis of message delay.

A CLASS OF HYBRID TDMA/TREE-RANDOM-ACCESS SCHEMES FOR MULTI-ACCESS COMMUNICATION CHANNELS, I. Rubin and M. Louie (USA). A slotted multi-access broadcast communication channel is considered. The traffic accommodated by the channel is composed of single-packet messages arriving at geographically distributed stations. A hybrid multiple-access scheme, which uses a combination of TDMA and tree-random-access components, is introduced and studied. Under this scheme, the network stations are divided into groups, each of which is assigned a dedicated time period within the TDMA time frame. The stations belonging to the same group employ a random-access strategy which uses a tree decision structure to resolve collisions. Delay-throughput performance functions are derived to demonstrate how the scheme performs and adapts to the underlying traffic statistics, as the structure varies from a pure TDMA format to a pure random-access protocol.

A TELETRAFFIC PERFORMANCE ANALYSIS OF A DIGITAL COMMUNICATIONS LINK, B.W. Stuck (USA). The teletraffic handling characteristics are investigated of a general class of models with different policies for integrating synchronous and asynchronous streams from multiple sources into a common or shared facility using time division multiplexing. The common facility or link transmits information in repetitive time intervals called frames. Each frame consists of one or more time intervals called slots or envelopes. For synchronous traffic, when an arrival occurs, a set of time slots is required in each frame for the duration of the call or session; if all available time slots are occupied, the new arrival is rejected, and presumably will retry later. For asynchronous traffic, when the arrival occurs, a set of time slots is required, and if all available time slots are filled, the arrival is buffered until time slots become available (in order of arrival). The synchronous traffic streams are handled via a generalization of conventional line or circuit multiplexing. Traffic performance as a function of offered load is

specified for synchronous traffic by blocking characteristics, and for asynchronous traffic by delay characteristics and buffering requirements.

Three examples are discussed in detail:

(1) V synchronous competing for a total of S time slots per frame with D asynchronous sources

(2) N asynchronous sources competing for S time slots per frame

(3) a special packetizing algorithm for a data communications network interface that waits until at least L chunks of data are buffered before sending a packet, and sends a maximum size packet of H>L chunks.

MODELING AND ANALYSIS OF AN INTEGRATED VOICE-DATA MULTIPLEXER, K. Sriram, P.K. Varshney, and J.G. Shanthikumar (USA). Integrate transmission of voice and data on a common communication facility results in a more effective system utilization. In this paper, we study a moveable boundary frame allocation scheme for multiplexing voice and data. A discrete-time model, which represents the actual system closely, is analyzed. It is shown that the behavior of the voice traffic can be modeled by a Markov chain. This model is used to derive an expression for the loss probability for the voice traffic. The data traffic is assumed to follow a Poisson arrival pattern and its message length, in terms of the number of packets, is assumed to have a general distribution. The moment generating function approach is followed to find the expected waiting time for the data traffic. Obtaining exact values of the expected waiting time in realistic situations involves considerable computational effort. Therefore, approximations which provide much simpler analytical expressions for the expected waiting time are considered. (This work was supported in part by AFOSR grant AFOSR-80-0074, RADC contract F30602-78-C-0083, and Syracuse University Research and Equipment Fund.)

PERFORMANCE ANALYSIS OF A HYBRID-SWITCHED LINK, A. Leon-Garcia (Canada). In this paper, we investigate the interaction between the voice and data traffic in a hybrid-switched link. We develop a fluid approximation approach for estimating the average data buffer contents, and we verify the accuracy of the results by comparison to

simulation results. We find that the moveable boundary approach is not effective in increasing the utilization of bandwidth. We then propose a flow control procedure in which the input data flow is regulated according to the voice random process and show that the approach is very effective in increasing the bandwidth utilization. Finally we discuss the network flow control and routing implications of our results.

APPLICATIONS, OF COMBINATORIAL SETS IN SATELLITE COMMUNICATIONS, W.W. Wu (USA). Not too long ago, satellite communication system design implied only link budget calculations. System implementations were extension of familiar R.F. technologies and digital satellite transmission referred only to PCM. As the device and sub-system technologies have matured some of the theories and principles of how to design a better system remain lack or behind. The purpose of this paper is to demonstrate how a class of simple combinatory set theory has not only touched upon a diversified satellite communication system disciplines, but also very often provided the optimum solution.

The paper addresses the following specific applications:

The elimination of intermodulation product in FDMA through frequency selection

The generation of synchronizable sequence with prescribed correlation properties in TDMA

The minimization of message collision in superpacket satellite data transmission

The optimal arrangement in pairwise network connection for on-board switching

Sub-Nyquist temporal sampling for whitening the aliasing effects for high speed signal processing

Sidelobe control in multi-beam antenna arrays

The generation of distinct signatures for interference identifications and random multiple access transmission.

Each application will be demonstrated by a simple example.

EFFECT OF CHANNEL ERRORS ON CERTAIN RANDOM-ACCESS ALGORITHMS, J.L. Massey (Switzerland). The earlier recursive analysis of the Capetanakis-Tsybakov-Mikhailov serial tree algorithm (CSTA) for the random-accessing of a common receiver by many transmitters is extended to include the effect of errors in the forward channel and/or in the feedback channel. It is shown that no combination of errors can result in deadlock and, moreover, that the error rates must be abnormally high to cause a significant reduction in the maximum stable throughput of the CSTA. However, it is shown that the Capetanakis-Massey-Tsybakov-Mikhailov algorithm, which differs from the CSTA only by the deletion of transmissions that in the error-free case are certain to yield collisions, suffers from deadlock that can be induced by a single channel error. Some "fixes" to eliminate this deadlock are proposed, and the relative merits of the various random-access algorithms considered are discussed.

TIME AND FREQUENCY TRANSFER IN DATA COMMUNICATION NETWORKS, W.C. Lindsey, F. Ghazvinian, and W. Hagmann (USA). One of the major problems in developing an efficient digital communication network is associated with the task of synchronization of the frequency and phase of all clocks in the network. Different methods of distributing time and frequency are discussed and a general mathematical model describing all these techniques is developed. Special attention is given to mutual synchronization and functional models are introduced for this method.

Performance measures for time and frequency distribution networks are discussed. The influences of frequency drift and phase noise process of the clocks on the time error processes are investigated. A comparison is made between mutually synchronized and plesiochronous networks. Finally, a special network growth algorithm is presented which minimized network disturbances due to topological changes in the network structure. (This work was supported under the following contracts: NSF-ENG-782219 and ARO-DAAG29-79-C-0054.)

SESSION C3

Pattern Recognition

*MINIMUM CROSS-ENTROPY PATTERN CLASSIFICATION AND CLUSTER ANALYSIS, J.E. Shore and R.M. Gray (USA). This paper considers the problem of classifying an input vector of measurements by a nearest-neighbor rule applied to a fixed set of vectors. The fixed vectors are sometimes called characteristic feature vectors, codewords, cluster centers, models, reproductions, etc. The nearest-neighbor rule considered uses a non-Euclidean, information-theoretic distortion measure that is not a metric, but that nevertheless leads to a classification method that is optimal in a well-defined sense and is also computationally attractive. Furthermore, the distortion measure results in a simple method of computing cluster centroids. Our approach is based on cross-entropy minimization (also called minimum discrimination information or minimum directed divergence), and can be viewed as a refinement of a general classification method due to Kullback. The refinement exploits special properties of cross-entropy that hold when the probability densities involved happen to be minimum cross-entropy densities. The approach is a generalization of a recently-developed speech coding technique. (This research was partially supported by the Office of Naval Research and by the National Science Foundation.)

*GRAPH THEORETIC METHODS FOR EDITED NEAREST NEIGHBOR DECISION RULES, G.T. Toussaint, B.K. Bhattacharya, and R.S. Poulsen (Canada). In order to combat the storage problem, and resulting computation, of the nearest neighbor decision rule (NN-rule), many researchers have in the past proposed schemes for "editing" (reducing, condensing, thinning) the original set of training vectors $\{X,\theta\}$. All these techniques suffer from several disadvantages. They are sequential, resulting in a non-unique edited set $\{X,\theta\}_E$ that depends on the order in which $\{X,\theta\}$ is processed, they are not guaranteed to yield an edited set that is decision-boundary consistent (implements the same decision boundary as $\{X,\theta\}$), and they use heuristics which render the procedures involved and clumsy.

In this paper two exact methods for editing the data in the NN-rule are proposed and compared experimentally, with respect to storage requirements and resulting error rate,

with the exhaustive (full training set) rule. The methods are based on first computing two well known graph structures on $\{X, \theta\}$, the Delaunay (Voronoi) triangulation and the Gabriel graph. The first method does not suffer from any of the above mentioned disadvantages. While the second method fails to yield a decision-boundary consistent subset, the resulting subset is much smaller and yields the same error rates. Finally, algorithms are given for obtaining the edited sets efficiently.

A TEST OF THE GAUSSIAN-NESS OF A DATA SET USING CLUSTERING, K. Fukunaga and T.E. Flick (USA). The "magnifying glass" method of clustering was proposed by Patrick (1972). The method consists of estimating the expected vector of a distribution from a weighted sum of data points. The weighting function is a Gaussian typr curve achieving its maximum value at a point X_s. Samples close to X_s are weighted more heavily. Thus, we can interpret the "magnifying glass" method as estimating the expected vector by local properties about X_s.

This method was developed specifically for clustering Gaussian distributions. Given an n-dimensional Gaussian data set, the method is capable of generating an unbiased and consistent estimate of the expected vector from any point X_s. On the other hand, if the data set is distributed according to a non-Gaussian density, a biased and inconsistent estimate of the expected vector results. These properties of the clustering technique allow us to develop a method for testing a set of points to determine whether or not they are Gaussian.

The proposed Gaussian test is as follows. We generate a set of points X_s. At each of these points an unexpected vector estimate, M, is generated. Then, the variation of these estimates about the theoretical expected vector, M, is measured. The decision to accept or reject a data set as Gaussian depends upon the size of this scalar quantity. The points X_s could be chosen as part of the data or they could be generated independently. In this paper, the latter approach is chosen to allow theoretical simplifications.

The variation of M was found to be composed of two parts, a consistent part and an inconsistent part. Whereas the consistent part becomes negligible for large numbers of data points, the inconsistent part is not dependent on sample size. In fact, this part disappears only for Gaussian data and is positive otherwise. Furthermore, we show that the inconsistent part can be estimated from a finite number of data points. We use this estimate as a more sensitive test

of a distribution. Once the estimate is taken, it is compared in a simple threshold test. Values for the threshold are suggested. If the estimate is above the threshold, the data can be assumed to be nonGaussian.

An example of a bimodal Gaussian distribution is considered. The theoretical sensitivity of the Gaussian test against this distribution is clearly shown for various dimensionalities and sample sizes of data. The test is able to reject the distribution as Gaussian when the modes are too far apart.

SOME RESULTS IN SEQUENTIAL PATTERN RECOGNITION, N. Mukhopadhyay (USA). We begin by considering the problem of identifying a population P_0 with one of the other two populations P_1 and P_2. We wish to control the probabilities of two types of errors at levels a and b, $0<a, b<1$. Towards this end, we discuss the following situations:

(a) When the P_i's are all Gaussian with unknown means, but the common variance is known, we propose a sequential probability ratio test based on the maximal location invariants. We consider a design where we can have only a fixed number of samples from P_0, whereas from P_1, P_2 we can have unlimited number of samples. One is referred to Ghosh and Mukhopadhyay (1980).

(b) Here we do not assume Gaussian distributions, and the common variances are assumed to be unknown. Using the design that we can have unlimited samples from all the three populations, we propose a sequential procedure along the lines of Robbins and Starr (1965). We show that, in the limit, the probabilities of errors tend to a and b. Also, we study the rate convergence of these probabilities utilizing the recent results of Landers and Rogge (1976) and Ghosh (1980).

Next, we consider the possibility of utilizing the ideas of distinguishability as introduced in Robbins (1970) in the case when P_0 is identified with only one $P_1, \ldots, P_k$ for $k>3$ having a small uniform bound on all the probabilities of errors.

NEAREST NEIGHBOR RULE CLASSIFICATION OF NONSTATIONARY TIME SERIES: PRELIMINARY OBSERVATIONS ON THE INFORMATION FOR DISCRIMINATION IN HUMAN EVOKED POTENTIALS, W. Gersch and T.

Brotherton (USA). A nearest neighbor rule approach to the classification of ensembles of nonstationary time series is introduced here for the solution of an exploratory population screening-time series-classification problem. Ensembles of time series occur in the analysis of human evoked potential electroencephalogram (EEG) time series. This approach was applied to evoked potential data in a preliminary exploration of a scientific question of interest; Where in the human evoked potential is the information for discrimination?

In the nearest neighbor approach, a measure of dissimilarity between a new to-be-classified time series ensemble and each of a set of labeled sample time series ensembles is computed. The new time series is classified with the label of the labeled sample time series which is least dissimilar. The measure of dissimilarity is computed as an estimate of the Kullback Liebler number between the time series ensembles, as if the time series were Gaussian distributed.

That dissimilarity measure can be seen to have sufficient metric properties, i.e., (1) $d(x^{(o)},x^{(o)})=0$, (2) $d(x^{(o)},x^{(m)})>0$ for any $x^{(m)}=0$ and iii) $d(x^{(o)},x^{(m)})$ approaches zero as the number of labeled samples, approaches infinity. In that case, a statistically reliable estimate of the best possible probability of misclassification is achieved by the nearest neighbor rule applied to classify the labeled sample time series in a leave-one-out cross validation estimate, Cover (1969), Rogers (1977).

In conventional discriminant analysis of human evoked potential data only the mean value function of the time series ensemble or average evoked potential is utilized. Implicit in that analysis are the assumptions that EEG covariance structure is uniform over subjects and had relatively little information for discrimination between ensembles of evoked potentials. Evidence obtained in a preliminary visual evoked potential experiment suggests that the background EEG is neither stationary nor uniform over subjects, that the average evoked potential is relatively unimportant and that the covariance structure of the EEGs is dominant in distinguishing between human evoked potential EEGs.

Our observations are potentially relevant to neurological data-population screening problems that are based upon the analysis of ensembles of evoked potential time series. Our results suggest that in those analyses, the nearest neighbor-Kullback Leibler type dissimilarity rule can be statistically more efficient for discrimination than average evoked potentials.

NONLINEAR CLASSIFIER DESIGNED WITH A FEATURE SPACE SAMPLING TECHNIQUES, S. Tatsumi, S. Kimura, and T. Kitahashi (Japan). This paper presents a new method of organizing a nonparametric and nonlinear classifier for multicategory without supervisors. At first, partitioning the feature space into mutually disjoint cells whose volumes are equal, we obtain many lattice points. Among all lattice points we select the lattice points which represent the configuration of the sample set. We name the selected point the representative lattice point. For the set of many representative lattice points the graphical clustering procedure is executed and with using gradient information at each lattice point all lattice points are classified based on the representative lattice points classified in the clustering procedure. As a result, the configuration of classified lattice points distributed in the feature space organizes the nonlinear classifier. It is shown that this method is effective with applying to a few artificial nonlinear data sets.

AN ALGORITHM FOR OPTIMAL LINEAR DISTANCE-PRESERVING MAPPINGS, S.A. Starks and M.D. Vanstrum (USA). This paper presents an algorithm which generates an optimal linear mapping for data structure analysis. The optimality criterion for the mapping is based upon an interpoint distance criterion first presented by Sammon. The algorithm is iterative in nature and is implemented using a steepest descent method. Preliminary numerical results have been obtained which indicate that the quality of distance preservation for this algorithm exceeds that obtained using the standard principal components expansion. This algorithm is very suitable for interactive Pattern Recognition applications due to the distance-preserving nature of optimality criterion.

SESSION C4

Shannon Theory II

*THE ERROR EXPONENT FOR THE NOISELESS ENCODING OF FINITE ERGODIC MARKOV SOURCES, L.D. Davisson (USA), G. Longo, and A. Sgarro (Italy). A new approach to the classical fixed-length noiseless source coding problem is proposed for the case of finite ergodic Markov sources. This approach is based on simple counting arguments. The central notion of "Markov type" (a set containing all the source sequences having the same transition counts from letter to letter) is introduced and the cardinality of such a set is evaluated via graph-theoretical tools. The error exponent is shown to be a weighted average of informational divergences, and the universal character of the result is stressed. As a corollary, the classical source coding theorem (determining the achievable rates) is rederived.

UNIVERSAL NOISELESS SOURCE CODING TECHNIQUES FOR MARKOV SOURCES, A.C. Blumer, R.J. McEliece, M.B. Pursley, and M.S. Wallace (USA). Although the theory of universal variable-rate source coding is fairly complete much work remains on the actual construction of universal source codes for sources with memory. Several construction techniques for the class of all binary memoryless sources, and a general method of universal code construction for discrete stationary sources have been developed. This general method can be applied to Markov sources and is developed further in the present paper.

The redundancy of a given code applied to a Markov source may depend on the initial state distribution for the Markov chain that characterizes the source. For asymptotic results, an ergodic chain can be assumed to be in steady state and the initial state distribution can be taken to be the limiting state distribution for the chain. This is the standard assumption for which it can be shown that the minimax redundancy is asymptotically $R_n^* \sim s \log n/2n$ for the class of all binary, unifilar, s-state, ergodic Markov sources.

In the present paper, a stronger form of universal coding for unifilar Markov sources is presented. We consider the situation in which the encoder knows the structure of the source but does not know the transition probabilities. The

code is to be strongly universal with respect to both the initial state and the transition probabilities. In contrast, the codes in in some prior work are more accurately described as weighted universal with respect to the limiting state distribution, although they are strongly universal with respect to the transition probabilities. One reason for interest in our stronger form of universal coding for Markov sources is that in practice the transition probabilities may be changing slowly, and hence the source may not be accurately characterized by a steady state or limiting distribution. (This research is supported by the Joint Services Electronics Program under contract N00014-79-C-0424 and the National Science Foundation under grant ENG75-20864.)

UNIVERSAL NOISELESS CODING OF SOURCES WITH MEMORY, H. Tanaka (Japan) and A. Leon-Garcia (Canada). In this paper we investigate the performance of a new coding scheme for sources which are known to be Markov but for which the specific statistics are unknown. The fundamental idea of this coding scheme is in a reversible transformation that maps the output sequence of the original source into a sequence of lower first order entropy. The transformed sequence is then coded as if it were the output of a memoryless source. The difference between the average codeword length and the entropy of the Markov source is bounded and the bounds are evaluated for Markov source up to order 4. The universal bound is also given.

ON TOTAL BOUNDEDNESS FOR THE EXISTENCE OF WEAKLY-MINIMAX UNIVERSAL CODES, R.J. Fontana and W.-C. Chen (USA). Stationary processes whose restrictions are totally bounded in variation distance are shown to be equivalent to the class of tight measures when the alphabet is countable. For uncountable alphabets, total boundedness implies tightness but the reverse implication need not hold as shown by example. Necessary and sufficient conditions for the class of Gaussian processes to be totally bounded are presented. An application of these results to universal coding for composite sources is considered. (This work was supported by NSF grant ENG79-08132.)

AN APPROACH TO SOURCE CODING, T. Hashimoto (Japan). In this paper an elementary proof is given for the process definition of the distortion-rate function of stationary ergodic sources $\underline{X}$ with finite alphabets and a single letter distortion measure d, where the infimum is over all stationary ergodic $(\underline{X},\underline{W})$. In view of this definition, a direct proof of the source coding theorem for stationary ergodic sources is deviced, and the argument in the proof is used to show directly that source codes can possess a kind of universality, called the quasi-universal property therein. Finally this property is shown to give another direct proof of the coding theorem for stationary nonergodic sources.

SUFFICIENT CONDITION OF UNIVERSALITY FOR VARIABLE-TO-VARIABLE-LENGTH METHODS OF CODING AND SOME PROPERTIES OF METHODS OF CODING SATISFYING THIS CONDITION, B. Fitingof (Germany). A sufficient condition of universality of variable-to-variable-length methods of coding is proved in terms of quasi-entropy of input words. Concepts of average probability of a letter and entropy-on-average per letter of a set of input words are introduced for any source (not necessarily a stationary one). Those quantities for a stationary source of independent letters coincide with probability of a letter and entropy per letter.

A concept of optimality of coding methods in case of unknown input message statistics (universality-on-average for the class of all sources) is introduced. Universal optimality for the class of all Bernoullian sources results immediately from its universality-on-average for the class of all sources.

The sufficient condition of universality for the class of all stationary sources of independent letters is proved to be a sufficient condition of universality-on-average of coding methods for the class of all sources. This condition is shown to keep the same meaning for concatenations of input words.

SESSION C5

Coding III

A SELECTIVE UPDATE ON SHIFT REGISTER SEQUENCES, S.W. GOLOMB (USA). During the fifteen years since the original edition of Shift Register Sequences went to press, there has been substantial progress in many areas treated in that book. Several conjectures have been proved, including the "Z(n) conjecture" on the maximum number of cycles in the de Bruijn graph (by J. Mykkeltveit), and a conjecture on trinomial factorization (by Mills and Zierler). The table of irreducible trinomials over GF(2) has been extended to degree 1000 (by Zierler and Brillhart). The constant λ, representing the relative expected length of the longest cycle of a random permutation, has been observed (notably by D. Knuth) to arise in other statistical contexts as well. Efficient methods of generating the members of large subsets of the set of all de Bruijn cycles have been published (mostly by H.M. Fredricksen); and priority for the investigation of the de Bruijn graph, including the theorem that there are $2^{2^{n-1}-n}$ de Bruijn cycles of span n, has been pushed back to a nineteenth century publication by C. Flye Sainte-Marie (an historical discovery made by N.G. de Bruijn himself). The theory of the cross-correlation of linear PN sequences with the same period has expanded greatly, and the instances of three-valued cross-correlation have been identified and explained (in papers by Kasami, Gold, Welch, Niho, Helleseth, and others). Many new applications of shift register sequences have also been found, but that exceeds the scope of this selective update.

USING FULL SEQUENCES FOR SPREAD SPECTRUM APPLICATIONS, H.M. Fredricksen (USA). A full sequence is a binary sequence of length 2^n+n-1 where every binary n-tuple appears exactly once. Such sequences can be generated by an n-stage nonlinear feedback shift register for any length n. These sequences share many properties with the n-stage maximum length linear sequences but have linear span approximately equal to their length and are a class of exponentially greater size. Subclasses of full sequences can be generated efficiently for use in certain spread spectrum applications. (This work was supported by the Naval Postgraduate School Foundation Research Program.)

SEQUENCES FOR SPREAD SPECTRUM MULTIPLE ACCESS SYSTEMS GENERATED FROM CYCLIC ERROR-CORRECTING CODES, C.-E. Sundberg (Sweden). Binary sequences with good even periodic autocorrelation and cross-correlation properties are constructed from cyclic error-correcting codes (BCH codes). Comparisons are made with Welch lower bound and Gold codes. It is concluded that codes better than Gold codes are found for certain lengths. It is also concluded that sequences which are near Welch lower bound can be constructed. Numerical data are presented for codes of length 63 and 255. The construction principle only assures good even periodic autocorrelation and cross-correlation properties. Aperiodic and odd periodic autocorrelation data is presented and discussed. It is concluded that search by means of computer among the sequences with good even periodic correlation properties yield sequences with good aperiodic and odd periodic correlation properties. Such properties are important for synchronization, multipath and multiple access properties of the sequences.

FURTHER RESULTS ON MAXIMUM-LENGTH DECIMAL SEQUENCES, S.C. Kak (USA). The paper presents new results on binary maximum-length decimal sequences. It shows that the lower bound on the hamming distance between a binary maximum-length sequence and its cyclic shifts is the integer closest to $q/3$, where $(q-1)$ is the sequence period. It is also established that the Hamming distances for shifts half the period apart add up to $(q-1)$. Furthermore, since the autocorrelation function $C(j), j \neq 0, (q-1)/2$ is generally close to zero as the sequence length increases these sequences appear promising for use in error-correction coding, simulation, signal design and cryptology. It has also been shown that the frequency of any subsequence of length j tends to $1/2^j$ as the sequence length becomes large, which shows that in the limit the statistical characteristics of a maximum-length sequence approach that of a random sequence. Sequences obtained by expanding $1/f(D)$, where $f(D)$ is a polynomial over GF(q) have also been discussed.

NEW RESULTS CONCERNING THE GRIESMER BOUND, H.C.A. van Tilborg (The Netherlands). The Griesmer bound gives a lower bound on the length of binary linear block codes. A review will be given of all the results concerning this bound. A new construction will be presented of codes meeting the Griesmer bound.

A LINEAR PROGRAMMING MINIMUM DISTANCE BOUND FOR LINEAR CODES, R.M. Tanner (USA). In this paper we give a lower bound on the minimum distance of a linear error-correcting code derived by analyzing a bipartite graph associated with the code. The graph contains nodes for digits and nodes for representing each linear equation (parity check for binary codes) defining the code, and an edge for every non-zero entry in the null matrix. A set of relations on pairs of edges is developed on the basis of the number of walks of each length connecting the two edges. The minimum distance of the code is established indirectly via a linear programming problem for a normalized vector representing the distribution of relations between pairs of edges incident on non-zero digit nodes in a codeword. There are three sets of constraints: the first is a positivity constraint derived by transforming the relation distribution into a vector of squared magnitudes of the eigenspace components of the corresponding codeword; the second is a set of inequalities implied by the linear equations; the third is a set of equalities that must be satisfied for the digits to have unique values. The bounding technique is applied to several block and convolutional codes.

GENERALIZATION OF THE MINIMUM DISTANCE BOUND ON GOPPA CODES, F. Gui-Liang (China). A new lower bound on the minimum distance of Goppa codes is presented. For a Goppa code defined by the Goppa polynomial $G(Z)$, its minimum distance d is known to be lower bounded by deg $G(Z)+1$. In this derived. paper, a new lower bound on d is derived. The new lower bound improves over the existing bound considerably in many cases. Furthermore, as the BCH codes are a special class of Goppa codes, it has also been shown that, when applied to BCH codes, the new lower bound also reduces to the generalized BCH bound obtained by Hartmann and Tzeng.

SESSION D1

Stochastic Processes II

BIAS AND VARIANCE OF DTOA ESTIMATES BASED ON NOISY, SAMPLED, CLIPPED DATA, T. Berger (USA). At site i (i=1,2) we observe hard-limited, uniformly spaced samples of

$$V_i(t)=A_iS(t-d_i)+N_i(t)$$

where $\{S(t)\}$,$\{N_1(t)\}$ and $\{N_2(t)\}$ are zero mean, mutually independent, stationary Gaussian random processes bandlimited to $|f|\leq B/2$. We wish to estimate d_2-d_1, the differential time of arrival (DTOA) of $S(t)$ at the two sites. We assume that the time T between successive samples is much less than B^{-1}, i.e., we assume a highly oversampled situation which is typical for systems that employ one-bit clipping.

Expressions are derived for the bias and the variance of a DTOA estimate based on quadratic interpolation of the crosscorrelation sequence of two bit streams. By specializing to the noisefree case, we obtain explicit results which quantify the fundamental limitations imposed on DTOA estimation by the combination of sampling and clipping.

The analysis is based on a random walk model for the difference between successive lags of the sample crosscorrelation sequence. The number of steps in the walk is the random number of zero crossings of $S(t)$ during the observation interval, and the bias of walk depends on the value of the DTOA modulo T. Some worthwhile by-products are a formula for the variance of the quotient of two correlated random variables and expressions for the probabilities of certain inequalities involving triples of independent Gaussian random variables.

THE RECONSTRUCTION OF ANALOG SIGNALS FROM THE SIGN OF THEIR NOISY SAMPLES, E. Masry (USA). A continuous-time signal $s(t)$ cannot, in general, be reconstructed from its sign, $\operatorname{sgn}[s(t)]$. It is shown that the deliberate addition of noise $\{X_k\}$ to periodic samples $\{s(k/W)\}$ of the signal prior to its one-bit quantization, allows for the reconstruction of $s(t)$ from the ± 1sequence $\{\operatorname{sgn}[s(k/W)+X_k]\}$ as the sampling rate W goes to infinity. Specifically, sequential, generally

nonlinear, estimates $s_W(t)$ of $s(t)$ are established and their convergence to $s(t)$ in the mean as well with probability one is obtained. The signal $s(t)$ need not be bandlimited. The degradation in the reconstruction of the signal, due to transmission of the binary data over a noisy channel, is also discussed. (This work was supported by the Office of Naval Research under contract N00014-75-C-0652.)

MIN-MAX EXTRAPOLATION OF BANDLIMITED SEQUENCES, N.T. Gaarder, H.J. Landau, K. Rege, and D. Slepian (USA). A sequence of complex numbers $\{x_n\}$ is said to be bandlimited to W if its amplitude spectrum $X(f)=\sum x_n \exp(-2\pi inf)$ vanishes for $W<|f|\leq 1/2$. Here W is a real positive number less than 1/2. Unlike a bandlimited function which is determined everywhere by its values on any finite interval, a bandlimited sequence is not determined uniquely by specifying its values on some finite index set. This fact permits us to construct a nonstochastic theory of extrapolation for such sequences.

Let the numbers $\underline{x}=(x_1,x_2,\ldots,x_K)$ be given. There are infinitely many ways to extend $\underline{x}$ to an infinite sequence $\{x_n\}$ that has bandwidth W. Let $S(\underline{x},W,E)$ denote the set of all such extensions that have energy not greater than E. We are interested in extrapolating $\underline{x}$ for L more terms so use

$$d(\{x'_n\},\{x''_n\})=L^{-1}\sum_{K+1}^{K+L}|x'_n-x''_n|^2$$

as a measure of the difference between two such extrapolations. We determine the unique extension $\{y_n(\underline{x})\}\in S(\underline{x},W,E)$ that minimizes $\mu(\{y_n\})=\max d(\{y_n\},\{x'_n\})$, where the maximization is over all extensions $\{x'_n\}\in S(\underline{x},W,E)$. That is, we find the bandlimited extension of given energy for which the worst possible average squared error in the L predicted places is as small as possible. This min-max extrapolator depends linearly on $\underline{x}$ and we give explicit formulas for it and the min-max error obtained. Generalizations, asymptotic results and some numerical examples are given. (This work was supported in part by the National Science Foundation under grant ENG74-19788 and in part by General Telephone/Hawaiian Telephone fellowship.)

DELTA MODULATION OF TIME-DISCRETE PROCESSES WITH I.I.D. INCREMENTS HAVING A RATIONAL CHARACTERISTIC FUNCTION, A. Hayashi (Japan). We investigate the mean-squared error (MSE) performance of a perfect integrating delta modulator driven by an input sequence of i.i.d. increments having a rational characteristic function $\phi_Y(u)$. Although the input process is non-stationary, the MSE can be finite under some conditions. The limiting characteristic function of the error sequence is found by the method of Wiener-Hopf, and tnen a formula for the MSE is given in terms of the coefficients of the defining polynomials for $\phi_Y(u)$, roots of transcendental equations involving $\phi_Y(u)$ and certain quantization parameters. Curves are presented of normalized MSE versus the distribution parameter or quantization parameter, where the increments are one- or two-sided gamma distributed. The results obtained here give some insight to asymptotic performance of delta modulation of stationary Markov processes having an amplitude distribution belonging to a wide class. (This work was supported in part by the National Science Foundation under grant ENG-19788.)

THIRD-ORDER INTERMODULATION DUE TO QUANTIZATION, N.M. Blachman (USA). When an input consisting of a strong signal and a weak signal is handled digitally, the resulting quantization introduces not only noise and distortion of the stronger signal (which have been thoroughly studied elsewhere) but also intermodulation between the two. Third-order intermodulation is the principal source of spurious in-band signals, and it is important therefore to determine its strength in comparison with that of the true weak-signal output.

The assumption that the weaker signal's amplitude a is very much smaller than the quantization step size permits a relatively simple analysis by an unorthodox application of Taylor's series that leads to a finite series for the amplitude c_2a of the intermodulation. This series is easily evaluated numerically, but simple approximations obtained by truncation of Euler's summation formula show the behavior of c_2 more clearly as a function of the amplitude of the stronger input and will be found adequate for most applications.

STOCHASTIC QUANTIZATION FOR PERFORMANCE STABILITY, P. Papantoni-Kazakos (USA). We consider stochastic stationary analog signals. For such signals, we consider quantizers

hose performance remains stable under perturbations in the statistical description of the signals. Our definition of performance is demanding, but realistic. We require that the output rate and the signal distortion do not fluctuate much within a family of stochastic signals, even for low output rates (not asymptotically large number of quantization levels). We also require that at least asymptotically the quantizer maintains certain important signal characteristics (such as some mean values, or some important spectral frequencies) within the family of stochastic signals. The stability (low fluctuations) in output rate guarantees the existence of a unique compressor for close to optimal compression within the family of stochastic signals.

We found that stochastic quantization satisfies stable output rate as well as stable asymptotic consistency even for low output rates (not asymptotically large number of quantization levels). This result is significant, since asymptotically high output rates defeat the very purpose of quantization (the purpose being reduction of the output rate below limits dictated by the transmission channel).

Specific efficient, and implementable stochastic quantization schemes are proposed for highly correlated as well as weakly correlated and uncorrelated stationary signal families. In addition, a noiseless compressor is described.

The fact that stochastic quantizers induce stable output rate should not be surprising to information theorists. The concept is a special case of random source encoding whose stability properties are well-established. (This research was supported by the Air Force Office of Scientific Research under grant AFOSR-78-3695A.)

OBSERVATIONS ON F.M. IN A RAYLEIGH CHANNEL, D.J. Thomson (USA). This paper explores various aspects of discriminator detection of F.M. in a Rayleigh channel with Gaussian Noise. It is shown that Rice's [1948] distribution for the instantaneous frequency of a sinusoid plus noise can be used to give an excellent approximation to the observed characteristics of F.M. From this distribution it can be shown that the distribution of a discriminator output in the Gauss-Rayleigh channel is t_2, a Student's distribution with two degrees of freedom. Since the effective distribution of coherent P.S.K. in a Gauss-Rayleigh channel is also t_2 equivalent F.M. characteristics near threshold as well as more accurate formulae for bit error rates in binary F.M. in Rayleigh fading channels may be obtained.

SIMULATIONS OF TWO-STAGE ADAPTIVE SIGNAL EXTRACTORS, J. Kazakoff and W.A. Gardner (USA). Computer simulations of two-stage adaptive signal extractors are described. In these two-stage configurations, the first stage reduces additive noise and the second stage reduces a signal distortion introduced by the first stage. Two configurations are presented, one useful for intermittent signal applications, the other useful for slow time-varying signals. In addition, an evaluation by computer simulation of a general mathematical model of the misadjustment and rate of convergence of estimated-gradient descent adaptive adjustment algorithms is also presented.

SESSION D2

Image Processing II

*TREE ENCODING OF IMAGES IN THE PRESENCE OF CHANNEL ERRORS, J.W. Modestino, B. Vasudev (USA) and J.B. Anderson (Canada). The performance and complexity of tree encoding of images in the presence of channel errors is considered. We demonstrate that performance close to the rate-distortion bound is achievable in the absence of channel errors for synthetic images modeled as 2-D autoregressive random fields and employing a variation of the (M,L) algorithm. Tradeoffs in optimizing the choice of tree search parameters are described and experimental results on real-world images are presented. Simple tree search procedures are shown to provide signal-to-noise improvements in excess of 5dB at the important rate of 1 bit/pixel; the effect is clear and striking to the eye. Channel error effects are treated by computer simulation and demonstrate signal-to-noise ratio improvement as high as 8dB using tree encoding. Finally, a combined source-channel coding approach is described which exploits the significant tradeoffs between source quantization accuracy and vulnerability to channel errors. (This work was supported in part by ONR under contract N00014-75-C-0281.)

HYBRID CODING OF NTSC SIGNALS - CHANNEL ERROR STUDIES, K.R. Rao AND F.A. Kamangar (USA). Interfield hybrid coding of NTSC component video signals is investigated. This coding involves two-dimensional discrete cosine transform (2d-DCT) of each field followed by differential pulse code modulation (DPCM) between fields. An efficient algorithm for fast implementation of 2d-DCT is developed. Three different algorithms for 2d-DCT/DPCM system are simulated and analyzed. In the first algorithm optimum quantizers are used in DPCM loops followed by fixed word length coders. Uniform quantizers along with variable-word-length coders were implemented in the second system. The performance of different deterministic coders are investigated and compared with Huffman coders. The third scheme is an adaptive system. In this system each block is divided into 4 subblocks. The activity of each subblock is monitored and when it exceeds some threshold, the subblock is considered to be spatially active. More bits are assigned to active subblocks and the range of corresponding quantizers are expanded. The error signal of the dc coefficient is is monitored to determine

the temporal activity of a block. For a temporal active block the number of bits assigned to the two lower frequency subblocks are increased. Performance of these three systems for unmatched statistics and in the case of a scene change are studied. The propagation and effect of the channel noise on the system with variable-word-length coders and also on the adaptive system are investigated.

ADAPTIVE IMAGE TRANSFORM CODING: A THEORETIC APPROACH AND APPROXIMATIONS FOR SIMPLIFYING THE DIGITAL IMPLEMENTATION, W. Mauersberger (Germany). An intraframe image transform coding system can be significantly improved by an adaptive control especially if a high compression should be achieved. This paper presents an approach based on a two-dimensional classification variable making possible not only the distinction of more or less detail in a transform block, but also the consideration of the prevailing direction of the structure. Based on several statistical models the system is optimized with respect to an information theoretic criterion. An important part of the investigations concerns approximations for the simplification of a digital implementation. The performance of the coder is discussed with respect to the signal noise ratio and the subjective quality of the reconstructed pictures.

PREDICTIVE DATA COMPRESSION OF COLOR PICTURE SIGNALS USING A COMPONENT CODING METHOD, V.-E. Neagoe (Romania). A predictive encoding system for color television signals is presented, using a component coding method, characterized by the fact that for the color difference signals (E_R-E_Y) and (E_B-E_Y) an adaptive delta modulation with delayed decision and overshoot suppression is used, and respectively, for the luminance signal E_Y, a differential pulse code modulation is used. A simplified encoding algorithm with delayed decision for the chrominance signals is proposed, which minimizes the slope overload noise and eliminates the overshoots. The corresponding step size adaptation system is based on the extraction and storage of the signal derivative. By considering an exponential probability density function of the luminance signal amplitude gradients, a system of transcedental equations is deduced, that determines an optimal quantizing characteristic. The experimentally achieved system is presented, and its subjective performances are evaluated. For a luminance signal E_Y of 3 MHz bandwidth and chrominance signals (E_R-E_Y) and (E_B-E_Y) having each of them 1 MHz bandwidth, the proposed predictive

enco in system of color images is characterized by a digital flow of 30 Mbits/s, assuring a good quality of reconstructed pictures, with a moderate hardware and a flexible behavior of the coder.

A HYBRID CODING METHOD OF VIDEO SIGNALS, O. Telese and G. Zarone (Italy). The hybrid transform/predictive coding of correlated frames is very efficient because it exploits both the spatial correlation (through the 2-D intraframe transform) and the temporal correlation (through interframe DPCM) without the storage requirement of a 3-D transform. The present investigated adaptive scheme adopts a picture domain segmentation (instead of a transform domain one) and the aggregation of moving pels in rectangles. This allows just the transform of the frame difference signal pertinent to these blocks, rather than the whole images, and reduces the necessary address information. The quality of a videotelephone sequence, processed by this coding and using Fourier, Hadamard and Cosine Transforms, with and without any filtering, was evaluated by objective parameters, by displaying it on a monitor and by a parameter tied to subjective opinions of observers.

ENCODING MOVING PICTURES BY USING ADAPTIVE STRAIGHT LINE APPROXIMATION, Y.-P. Wang (China) and J.P.M. Schalkwijk (The Netherlands). In this presentation we discuss a method of data compression for moving pictures (eg. conference television, picture-phone). The current estimate of the picture consists of a straight line approximation, and a texture component. Our algorithm tries to fit the current straight line approximation to the new picture. In places where this fit is poor, a new straight line approximation is made. As soon as an area of the picture becomes stationary, its straight line approximation is once augmented by a new texure component. The straight line approximation is obtained by means of a Kalman filter. As the human eye is less sensitive to error at higher values of the intensity, the Kalman filter is designed to emphasize errors at low intensity.

PERFORMANCE OF IMAGE TRANSMISSION SYSTEMS ON FADING CHANNELS, D.G. Daut and J.W. Modestino (USA). A combined

source-channel coding approach is described for the encoding, transmission, and remote reconstruction of image data. The transmission medium considered is that of a fading dispersive communications channel. Both the Rician fading and Rayleigh fading channel models are considered. A comparison between two image transmission systems is made. In one system the image source encoder employs two-dimensional (2-D) differential pulse code modulation (DPCM). The other system utilizes a block transform encoder employing the 2-D discrete cosine transform (DCT). Both are relatively efficient encoding schemes in the absence of channel errors. In the presence of fading, however, their performance degrades rapidly. By providing error control protection to those encoded bits which contribute most significantly to image reconstruction, it is possible to minimize this degradation without sacrificing transmission bandwidth. Several modulation techniques are employed in evaluation of system performance including noncoherent multiple frequency shift-keyed (MFSK) modulation. Analytical results are provided for assumed 2-D autoregressive image models while simulation results are described for real-world images. (This work was supported in part by ONR under contract N00014-75-C-0281.)

SESSION D3

Communication Networks II

*A CLASS OF OPTIMAL ROUTING ALGORITHMS FOR COMMUNICATION NETWORKS, D.P. Bertsekas (USA). We describe an algorithm for minimum delay routing in a communication network. During the algorithm each node maintains a list of paths along which it sends traffic to each destination together with a list of the fractions of total traffic that are sent along these paths. At each iteration a minimum marginal delay path to each destination is computed and added to the current list if not already there. Simultaneously the corresponding fractions are updated in a way that reduces average delay per message. The algorithm is capable of employing second derivatives of link delay functions thereby providing automatic scaling with respect to traffic input level. It can be implemented in both a distributed and a centralized manner, and it can be shown to converge to an optimal routing at a linear rate. (This work was supported by grants ONR-N00014-75-C-1183 and NSF ENG-7906332.)

ROUTING IN COMPUTER COMMUNICATION NETWORKS: AN A PROACH BASED ON SEQUENTIAL PROCEDURES, R. Singh, S. Subba Rao, and S.C. Gupta (USA). In this paper routing techniques, for Computer Communication, based on sequential testing procedures are proposed. Routing techniques consist of two steps. First step is to detect undesirable levels of traffic intensities using cumulative sum (Cusum) method and second step is to route packets so that traffic intensities at various nodes are close to optimal levels. Both synchronous and asynchronous updates are considered for implementing routing techniques. (This work was supported by AFOSR grant AFOSR-77-3277.)

BANDWIDTH CONTROL IN COMPUTER NETWORKS, M. Gerla and C. Sheedy (USA). In a circuit switched network when a circuit of given bandwidth must be established, the shortest path with sufficient residual bandwidth is generally searched for. A distributed algorithm, called bandwidth control algorithm was recently developed to solve the above routing problem in circuit switched networks. It appears that the

bandwidth control algorithm can be successfully extended also to packet switched networks, in the case in which a virtual circuit is assigned to each user session, and average data rate on each session is declared in advance or is easily predictable. For packet networks, the notion of residual bandwidth must, of course, be replaced by the notion of average residual bandwidth. One major advantage of the bandwidth control algorithm is to integrate routing functions and flow control functions in the same procedure. This eliminates possible conflicts between routing and flow control actions which often arise when these procedures are separately implemented.

The verbal presentation will briefly describe the bandwidth control algorithm and will discuss the associated line and processor overhead. Performance results based on circuit, packet and integrated networks will be presented and will be compared with the performance of conventional routing and flow control schemes.

FLOW CONTROL POWER IS NON-DECENTRALIZABLE, J.M. Jaffe (USA). Flow control in store-and-forward computer networks is appropriate for decentralized execution. A formal description of a class of "decentralized flow control algorithms" is given. The feasibility of maximizing power with such algorithms is investigated.

On the assumption that communication links behave like M/M/1 serves it is shown that no "decentralized flow control algorithm" can maximize network power. Power has been suggested in the literature as a network performance objective. It is shown that no objective based only on the sums of the users' throughputs and average delay is decentralized. Finally, a restricted class of algorithms cannot even approximate power.

CODING GAINS FROM ARQ ERROR CONTROL SYSTEMS, J.A. Heller and J.K. Wolf (USA). The efficacy of forward error correcting (FEC) coding systems utilized for the transmission of data over an additive white Gaussian noise channel is often expressed in terms of the coding gain -- the reduction in the ratio of the energy per bit to noise power density required to achieve some specified bit error probability. In this paper we calculate the coding gain for ARQ systems, optimized with respect to the choice of block length and channel symbol duration. Coding gains are calculated for four situations:

1) ARQ alone (unlimited number of retransmissions).

2) ARQ alone (limited number of transmissions).

3) ARQ along with FEC (unlimited number of retransmissions).

4) ARQ along with FEC (limited number of transmissions).

Curves are presented displaying the information rate of these systems as a function of the carrier-to-noise ratio when the bandwidth of the transmitted signals is limited.

*THE PERFORMANCE ANALYSIS OF SOME SELECTIVE - REPEAT ARQ SCHEMES WITH FINITE RECEIVER BUFFERS, M.J. Miller (Australia) and S. Lin (USA). In order to maintain high throughput efficiency in high speed data transmission systems, some ARQ error control schemes with mixed modes of retransmission are proposed. ARQ schemes utilizing combinations of selective-repeat, go-back-N and repetitive retransmissions are discussed and methods of throughput analysis are presented. The results provide a basis for comparative evaluation of the tradeoffs of protocol complexity and throughput for particular conditions of round trip delay, bit error rate and packet size. Hybrid ARQ schemes using parity retransmission for error correcting based on half-rate invertible codes are also discussed. Such techniques can be used to maintain significant throughput for higher channel error rates.

AN ANALYSIS FOR AN ARQ ERROR CONTROL SCHEME USING SEQUENTIAL DECODING, A. Drukarev and D.J. Costello (USA). Most of the work in the area of ARQ error control has been done using block codes. However, convolutional codes, especially with sequential decoding, can offer significant advantages over block codes in this area. An ARQ scheme is known that uses sequential decoding with a time-out condition. A new algorithm is proposed that allows one to achieve a higher throughput. The algorithm represents a modification of the stack sequential decoding algorithm. The decoder monitors the slope of the metric of every path in the stack, and when the slope of the path at the top of the stack falls below a predetermined threshold, a retransmission request is generated. Theoretical analysis of both algorithms is presented in order to find optimal parameters. Experimental

results verifying the theoretical conclusions are given.
(This work was supported by the National Science Foundation under grant ENG-78-05665.)

SESSION D4

Shannon Theory III

ROBUST CODING OF INDECOMPOSABLE FINITE STATE CHANNELS, B. Patek (Czechoslovakia). Robust coding of binary indecomposable finite state channels with state sequence independent from input and output is investigated. Each channel k is characterized by a parameter $\varepsilon(k)$ which has the sense of an asymptotic error frequency. Let $C(\varepsilon)$ denote the capacity of the binary symmetric memoryless channel with transition probability ε. It is proved that for any class K of channels with common state set and with $\varepsilon(k)\leq\varepsilon$, for any rate below $C(\varepsilon)$ and any $\delta>0$ there exists such a common code for all channels $k\in K$ that the probability of /minimum distance/decoding error is less than δ. Moreover, for rates above $C(\varepsilon)$ transmission with arbitrarily small error probability is not possible with minimum distance decoding through any channel for which $\varepsilon(k)\geq\varepsilon$.

FINITE STATE INDECOMPOSABLE CHANNELS ARE ALMOST FINITE, D.L. Newhoff and P.C. Shields (USA). We show that a finite state indecomposable channel is $\bar{d}$-continuous (a condition on decay of input memory) and almost block independent (a condition on decay of output memory) hence can be approximated arbitrarily well in the $\bar{d}$-metric by a primitive channel (i.e., the cascade of white noise and a sliding block encoder). We also prove the converse for those finite state channels for which the output is the state of the channel. (This research was supported by AFOSR under grant AFOSR-80-0054.)

BLOCK AND SLIDING-BLOCK CODING THEOREMS FOR A STATIONARY CHANNEL, J.C. Kieffer (USA). Let v be a discrete stationary finite-alphabet channel. If u is an ergodic input to the channel, let uv denote the joint distribution of input and output, and let I(uv) denote the information rate for uv. The channel is said to be weakly continuous at u if the mapping $\lambda\to\lambda v$ (with domain the set of all ergodic inputs) is continuous at $\lambda=u$ with respect to weak convergence; it is ergodic at u if uv is ergodic. If the channel is weakly continuous and ergodic at u, then every ergodic source with entropy less than I(uv) is block transmissible over the chan-

nel. If the channel is weakly continuous and ergodic in some weak neighborhood of u, then every ergodic, aperiodic source of entropy less than I(uv) is zero-error transmissible using infinite sliding-block encoder and decoder. If the channel is weakly continuous at every ergodic input, then the information quantile capacity C* of Gray and Ornstein is the maximum number such that every ergodic source with smaller entropy can be block transmitted. If in addition the channel has positive sliding-block capacity C_s, then an ergodic aperiodic source is sliding-block transmissible if and only if its entropy is less than or equal to C_s.

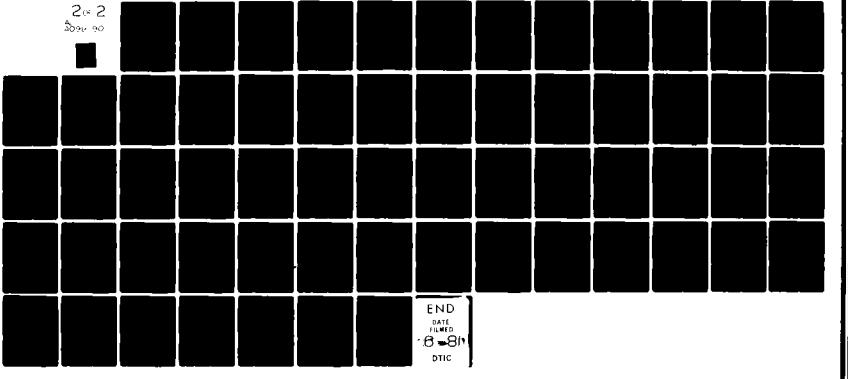
ON CHOQUET CAPACITIES AND THEIR DERIVATIVES WITH RESPECT TO σ-FINITE MEASURES, K S. Vastola and H.V. Poor (USA). Choquet capacities have been shown to be useful in the generalization of the theories of robust hypothesis testing and filtering. To extend the usefulness of this approach, the concept of a capacity on a measurable space is generalized somewhat to that of a semi-capacity, which need not be continuous from above on closed sets when the limit is the empty set. This modification allows various uncertainty models (e.g. ε-mixture models, Kolmogorov neighborhoods, etc.) to be viewed as semi-capacity classes on noncompact spaces. The results of Huber and Strassen for robust hypothesis testing of one capacity class versus another extended (under an easily verifiable condition) to the case of a semi-capacity class versus a σ-finite measure (e.g. Lebesgue measure on R or R^n). This is done by constructing a Radon-Nikodym-type derivative which generalizes that of Huber and Strassen. This result proves useful in filtering and other applications where "white noise" assumptions are desired. Such applications are explored and examples are discussed. Finally, certain technical lemmas used in the above are examined for their ramifications in the various areas of communication theory in which capacities have been found useful. (This research was supported by the National Science Foundation under grant ECS79-16435 and by the Joint Services Electronics Program under contract N00014-79-C-0424.)

ON THE CAPACITY OF ARBITRARILY VARYING CHANNELS FOR MAXIMUM PROBABILITY OF ERROR, I. Csiszar and J. Korner (Hungary). The arbitrarily varying channel (AVC) is a model of communication devices in which the noise may depend on an unknown "state", varying with time in an unpredictable manner. The m-capacity C_m of an AVC is the largest rate of codes which, no matter what the state sequence is, guarantee correct ...

AD-A099 190 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS INC--ETC F/G 9/4
IEEE INTERNATIONAL SYMPOSIUM INFORMATION THEORY, HELD AT SANTA --ETC(U)
1981 I RUBIN, K YAO AFOSR-81-0032

UNCLASSIFIED AFOSR-TR-81-0454 NL

2 of 2
AD A099 190



END
DATE FILMED
8-81
DTIC

coding with small probability of error for each message (rather than on [illegible]essages, as in the definition of a-capacity).

An AVC with input alphabet X, set of states S, and output alphabet Y is given by the transition probabilities $W(y|x,s)$. Denote by W the set of matrices V the rows $V(.|x)$ of which are convex combinations of the distributions $W(.|x,s)$, $s\in S$. For a distribution P on X, denote by C(P) the minimum of the mutual informations $I(P,V)$, $V\in W$, and by D(P) the minimum mutual information of RV's X and X' both having distribution P and such that for each pair (x,x') with $\Pr\{X=x,X'=x'\}>0$ there exists a $V\in W$ with $V(.|x)=V(.|x')$.

Theorem: $C_m \geq \min(C(P),D(P))$ for every P. If there is a P_o maximizing C(P) such that $C(P_o)\leq D(P_o)$ then $C_m=C(P_o)$.

This generalizes a recent result of Ahlswede who determined C_m for the case when no matrix $V\in W$ has two identical rows. The proof of the theorem uses an interesting new decoding rule.

A BINARY NOISE PRIMITIVE CHANNEL, Y. Matsuyama (Japan). A $\bar{d}$-continuous and conditionally almost block independent channel on countable alphabet space can be simulated by a binary noise primitive channel (or a binary noise stochastic sliding block coder) within arbitrary accuracy in the d-sense. Imbedding of a bunch of binary i.i.d. sequences is utilized in the proof besides the techniques developed by Neuhoff and Shields.

It is also shown that the capacities of the true channel and the simulated one remain close, however, the relative entropy introduced by a hypothesis test on two output processes may diverge. Such a case essentially occurs in practical simulations when the countably infinite output alphabet is reduced to finite. (This research was supported in part by the Science Research Fund of the Ministry of Education, Japan.)

ON THE CAPACITIES OF GAUSSIAN CHANNELS, C.R. Baker (USA) and A.F. Gualtierotti (Switzerland). We consider first the additive Gaussian channel without feedback. Let N be the Gaussian noise, m the message process, A(m) the transmitted signal. Let W be a second Gaussian process equivalent (mutually absolutely continuous) to N. $I(m,A(m)+N)$ is the mutual in-

formation between m and A(m)+N. We determine the capacity sup $I(m,A(m)+N)$, where Q is the set of all (A,m) such that $E\|A(m)\|^2 \leq P$, with $\|\cdot\|_W$ the RKHS norm for W. A special case of these results is for W the Wiener process on [0,T], with the constraint $E\int_0^T [A(m)_t]^2 dt \leq P$. Using these results, we give partial results on the capacity of the same channel with casual feedback.

NONLINEAR FEEDBACK IN SEQUENTIAL DIGITAL COMMUNICATION SYSTEMS, A.F. Hassan (Egypt). The paper deals with a sequential digital communication system with nonlinear feedback. The forward channel is distributed by an additive zero mean white Gaussian noise while the feedback link is assumed noiseless. The transmitter uses the output of the feedback link "y(t)" to modify the transmitted signal power so as to hasten the receiver's decision. The transmitted signals under both hypotheses $S_{1,0}=A\,X(t)\exp(FBy)$. The average transmission time is obtained using Fokker-Planck technique. For a given prescribed small error probability and large peak-to-average transmitter power ratio, we design the signal parameters A and B so as to minimize the average transmission time.

Comparison of this system with the system with linear feedback where $S_{1,0}=\pm(1+\alpha y)\cdot x(t)$ shows 3 dbs saving time for a probability of error 10^{-10} and for a peak-to-average transmitter power ratio of 20.

SESSION D5

Coding IV

BIT-SERIAL REED-SOLOMON ENCODERS, E.R. Berlekamp (USA). This paper presents new concepts and techniques for implementing encoders for Reed-Solomon codes, with or without interleaving. Reed-Solomon encoders based on these concepts and techniques often require substantially less hardware than even linear cyclic binary codes of comparable redundancy.

BOUNDS AND CONSTRUCTIONS FOR ERROR CORRECTING/DETECTING CODES ON THE Z CHANNEL, J.M. Borden (USA). We consider the problem of designing binary codes capable of detecting or correcting errors made on the Z channel; here the transition 0 to 1 is impossible. The best (maximal number of codewords) asymmetric error detecting codes are exhibited and bounds are obtained on the size of the best asymmetric error correcting codes, allowing us to compare the performance of these codes with the best symmetric error correcting codes (where both transitions 0 to 1 and 1 to 0 may occur).

Unlike the situation encountered in coding for symmetric errors, on the Z channel, error detecting codes require a different combinatorial structure than error correcting codes. The requirement for error detection is weak enough for Klietman's generalization of Sperner's theorem to be applicable and we find that the maximal length n, e asymmetric error detecting codes have as codewords those vectors whose Hamming weight is congruent to n/2 modulo e+1. (When n is odd, use $(n+1)/2$.) Consequently the best asymmetric error detecting codes have a much higher information rate than the best symmetric error detecting codes.

This situation changes when we consider error correcting codes. Denote by $A(n,e)$ the maximal number of codewords in a length n,e asymmetric error correcting codes; define $S(n,e)$ similarly for symmetric codes. Of course, $S(n,e) \leq A(n,e)$. We give a construction that extends (n,e)-asymmetric codes to $(n+e,e)$-symmetric codes and obtain the bound $A(n,e) \leq S(n+e,e)$, generalizing a result of Stanley and Yoder. Another upper bound, $A(n,e) \leq (e+1)S(n,e)$, is obtained by piecing together constant weight codes. This inequality is quite interesting for, if we set $e=\varepsilon n$ and let $n \to \infty$, there results $\log A(n,\varepsilon n) = \log S(n,\varepsilon n) + o(n)$; that is, maximal

$(n,\varepsilon n)$-asymmetric and symmetric codes have the same rates as $n \to \infty$.

We also give a construction yielding, when n is a prime power, $A(n,e) \geq 2^n/(n^e+n^{e-1}+\ldots+1)$. The codes constructed are a type of group code (as introduced by Varshamov) and the construction is based on a theorem of Bose-Chowla regarding sum-sets in cyclic groups. This appears to be the best construction to date although we feel there is still room for improvement.

Our last result is a low rate bound. Considering all codes containing M codewords, we wish to maximize the ratio e/n. Plotkin's and Levenshtein's theorems show that for symmetric codes $e/n \leq 1/4+O(1/M)$ (for all n and as $M \to \infty$) and this estimate is best possible. We obtain for asymmetric codes the best possible estimate $e/n \leq 1/3+O(1/M)$ by solving a linear program. One interpretation of this result is that on a very noisy binary symmetric channel with transition probability p, $\frac{1}{4} < p < \frac{1}{3}$, the requirement of reliable communication leads to an upper bound on the number of codewords in any code. On the Z channel with the same transition probability we may have as many codewords as desired and still communicate reliably.

ON THE CONSTRUCTION OF SYSTEMATIC SINGLE ERROR CORRECTING AND MULTIPLE UNIDIRECTIONAL ERROR DETECTING (SEC-MUED) CODES, B. Bose (USA). In this paper first we prove that any systematic SEC-MUED code with k bits of information requires at least 2 log k check bits. Then we describe a method of constructing systematic SEC-MUED codes. The proposed method requires approximately 3 log k check bits. The encoding/decoding algorithms for this code are also discussed.

NON-REDUNDANT CODES FOR TRANSMITTING QUANTIZED SIGNALS UNDER CHANNEL ERROR CONDITIONS, M. Copperi (Italy). This paper describes a method for code classification which utilizes a distance criterion depending on both the source symbol probability and the channel error pattern (i.e., single error, double error, etc. for each codeword).

This approach is useful for choosing the most suitable encoding for a given noisy channel, in order to reduce the confusion between transmitted and received messages, when error-correcting codes cannot be used or it is not crucial to keep the exact reproduction of each symbol sent to the

receiving end. Interesting properties of non-redundant codes under different channel error conditions are pointed out by an example, where the source is characterized by an 8-dimensional finite complete scheme and the channel alphabet is binary.

COSET CODING, J.-M. Goethals (Belgium) and L. Huguet-Rotger (Spain). Given the coset decomposition $C/C_0=\{C_0,C_1,\ldots,C_{M-1}\}$ of a binary code C with respect to a proper subcode C_0, we consider the coding scheme, called coset coding, where for $i=0,1,\ldots,M-1$, each word in the coset C_i conveys the same information, say the source symbol i. This scheme which has been proposed by Tsybakov for masking defects and simultaneously correct random errors in computer memories, is considered here for the purpose of confusing a wire-tapper. We propose a method for calculating explicitly the equivocation at the wire-tapper's end as a function of the error probability p on the wire-tap channel, which is assumed to be binary symmetric. The main result is that this equivocation approaches the source entropy when $(1-2p)^d$ approaches zero, where d is the minimum weight of the dual code of C_0.

IMPROVED DECODING SCHEME FOR FREQUENCY HOPPED MULTILEVEL FSK SYSTEM, U. Timor (Israel). A digital spread spectrum technique employing MFSK modulation with code-division-multiple access (CDMA) by frequency hopping over a common bandwidth has been recently examined for possible applications in satellite communication and in digital mobile radiotelephony. Each user is assigned a distinct address, which is a sequence of L tones chosen from an alphabet of 2^K sinewaves of duration t. Every T(=tL) seconds a K-bit message is transmitted by frequency shifting the address. The receiver, knowing the address, can decode the received signal and extract the message. However, transmissions by other users can combine to cause an erroneous message, resulting in an ambiguous reception. Thus even without channel impairments the number of simultaneous users the system can accommodate at a given error probability is interference limited.

This paper describes a new decoding scheme which makes use of the well defined algebraic structure of the address set. The decoder performs matrix operations (row permutations and cycle shifting of columns) on the received frequency/time energy matrix, to identify and eliminate erroneous messages which come from interference from other users. The result is a significant increase in system performance, allowing a 50

to 60 percent increase in the number of users which can simultaneously share the system at a given error rate. A simple implementation of the decoder using shift registers is described. (This work was performed at Bell Labs while the author was on sabbatical from Armament Development Authority/Israel Ministry of Defense.)

SYNCHRONIZATION OF REED-SOLOMON CODES, R.L. Miller (USA) and B.B. Newman (Australia). A concatenated coding scheme, consisting of an inner (7,1/2) convolutional code and an outer J=8,E=16 Reed-Solomon code, will be used for the Galileo mission, the International Solar Polar Mission, and is part of the multimission packet telemetry guidelines currently being proposed [1]. This report examines the synchronization capabilities of Reed-Solomon codes when an appropriate coset of the code is used instead of the code itself. In this case an E-error correcting Reed-Solomon code is transformed into a new code with the property that the decoder is capable of determining that there are m symbols out of sync, if e symbol errors occurred, whenever m+e<E. In the event that m=0, i.e., the word is in sync, then the decoder will correct any pattern of E-1 or fewer symbol errors.

The key idea to achieving synchronization is to use a coset of the code instead of the code itself. (A coset is obtained by adding the same vector to every code word.) From an error-correcting point of view, the coset is equivalent to the code itself. In addition, useful synchronization characteristics of the coset code can sometimes be achieved which are not present in the original code. The algorithm to be presented differs from usual coding algorithms in that the information is encoded into one code, but decoded in a larger (different) code. The larger code contains the coset of the smaller code.

ON THE DESIGN OF MEAN-SQUARE ERROR CHANNEL CODING SYSTEMS USING CYCLIC CODES, G.R. Redinbo (USA). Channel coding systems that employ linear block codes can be designed according to a mean-square error criterion by assigning integer values to the respective input and output blocks of symbols. The optimum encoder and decoder pair is determined by selecting special elements in a generalized frequency domain based upon the values of the key parameters called ratio weights. This is true for systems that employ either hard or soft decision variables in the decoder. When cyclic codes are used, a minimal ideal decomposition of the code space

may be reflected into the frequency domain. It is shown that the finite field properties of each minimal ideal forces the ratio weights to assume constant values on certain subsets in the frequency domain. This permits a drastic reduction in the number of ratio weights that need to be computed for the design of a minimum mean-square error coding system. For a cyclic code possessing t minimal ideals, it is necessary to compute at most (2^t-1) distinct values for the ratio weights. The subsets on which the values are constant are completely specified by the structure of the minimal ideals.

SESSION E1

Complexity

ON THE POWER OF STRAIGHT-LINE COMPUTATIONS IN FINITE FIELDS, A. Lempel, G. Seroussi, and J. Ziv (Israel). It is shown that a lower bound of n^2 or more on the straight-line complexity of a function f over GF(2^n) is also a lower bound on the network complexity of f and, hence, on the product of run time and program size of Turing machines. It is further shown that most functions over a finite field are hard to compute and that for most hard functions there exists no approximation via an easy algorithm.

*THE COMPLEXITY OF INFORMATION STRUCTURES, M.L. Fredman (USA). This paper concerns the complexity of storing information in a manner which permits both subsequent modification as well as retrieval. We develop a framework in which basic entity of information consists of a record, which has an associated key and an associated value. The key associated with a record uniquely identifies that record and belongs to a set referred to as the key space. The values associated with records may be summed by means of an associative and commutative addition operation. Given a set of records, we assume that information about the set can be retrieved by evaluating queries. Queries are associated with subsets of the key space called regions. A particular query returns the sum of the values of all records in the set whose keys lie in the region associated with the query.

Given a key space and a repertoire of permissible queries, we consider how information should be organized so as to facilitate both efficient query evaluation and ease of updating. Updating means inserting and deleting records, and/or changing the values associated with records. The time required for query evaluation can be improved by maintaining in memory pre-computed sums of the values of various subsets of records. However, this tends to increase the time required for updating, or equivalently, the extent of information redundancy. We address the problem of determining the optimal trade-off between query time versus redundancy. (This research was supported in part by the National Science Foundation under grant MCS 76-08543.)

*DIGITAL SIGNAL PROCESSING APPLICATIONS OF POLYNOMIAL TRANSFORMS, H.J. Nussbaumer (France). In this paper, we present recent results concerning the use of new transforms called polynomial transforms for the fast computation of convolutions and discrete Fourier transforms. Polynomial transforms are Fourier-like transforms where the scalars are replaced by polynomials, the complex exponentials are replaced by powers of the polynomial variable Z and all operations are performed modulo a polynomial. Polynomial transforms can be computed without multiplications and with a reduced number of additions by the use of a fast Fourier transform (FFT) algorithm.

We first present two complementary techniques which use polynomial transforms to map multidimensional discrete Fourier transforms (DFT) into one-dimensional DFTs. We show that this mapping, which is optimal from the standpoint of the number of multiplications, yields an efficient FFT-type implementation for multidimensional DFTs. We then derive the circular convolution property of polynomial transforms from the polynomial representation of multidimensional DFTs and show that this new formulation points to improved implementations for multidimensional convolutions computed by polynomial transforms.

*THE COMPLEXITY OF SEARCHING GAMES, J. Pearl (USA). We consider a class of two-person perfect-information games in which two players, called MAX and MIN, take alternate turns in selecting one out of d legal moves. We assume that the game is searched to a depth h, at which point the terminal positions are assigned a static evaluation function V_0. The task is to evaluate the minimax value, V_h, of the root node by examining, on the average, the least number of terminal nodes.

The most commonly used procedure for searching games-trees is the α-β pruning algorithm. Yet although the exponential growth of game-tree searching is slowed significantly by that algorithm, quantitative analyses of its effectiveness have been frustrated for over a decade. Of major concern are the problems of determining the optimal expected complexity of game-searching tasks and deciding whether the α-β procedure achieves this optimal performance. The standard model for evaluating the expected search complexity employs uniform game-trees where the terminal positions are assigned random values, independently drawn from a common distribution.

This paper highlights some curious properties of tall game-trees with random terminal values and examines their impli-

cations on the complexity of various game-searching methods. In particular, we show that for continuous-valued games, the quantity $\xi/1-\xi$ lower bounds the branching factor of every directional search algorithm where ξ is the positive root of the equation $x^d+x-1=0$. Moreover, algorithms exist (e.g., SCOUT and $\alpha-\beta$) which actually achieve this bound. Games with discrete terminal values can, in almost all cases, be searched with a branching factor of $(d)^{1/2}$. This performance is globally optimal and is also achieved by the ALPHA-BETA procedure.

KHACIYAN'S ALGORITHM AND THE COMPLEXITY OF THE LINEAR PROGRAMMING PROBLEM, R.E. Stone (USA). In 1979 much attention was drawn by a paper of L.G. Khachiyan which stated a certain algorithm would solve the "Linear Programming Problem" in polynomial time. This talk will describe the central ideas behind the algorithm and the problem it solves. We will be chiefly interested in exactly what problem is being solved, what concepts of complexity theory are involved, what within the algorithm and the problem give the result, and how this relates to linear programming. Other models of linear programming complexity and other work, pre- and post-Khachiyan, concerning the basic algorithm and related results on complexity problems will be mentioned.

SESSION E2

Stochastic Processes III

SPECTRUM ESTIMATION VIA ORTHOGONAL WINDOWS, D.J. Thomson (USA). In estimating the spectrum of a stationary time series from a finite sample of the process two problems dominate: First, what algorithm should be used so that the resulting estimate is not dominated by bias; and second, how should one "smooth" the estimate so that the results are consistent and statistically significant.

In this paper we present a new method based on a "local" principle components expansion to estimate the spectrum in terms of the solution of an integral equation. Computationally this method is equivalent to using the weighted average of a series of direct spectrum estimates based on orthogonal data windows (discrete prolate spheroidal sequences) to treat both problems.

In addition to providing estimates of the spectrum which are based on well-established principles instead of heuristics this methodology also permits a unification of the differences between windowed and unwindowed philosophies.

ON THE METHOD OF MAXIMUM ENTROPY SPECTRUM ESTIMATION, A. Arcese (USA) and A.S. Molina (Colombia). In this paper we derive the recursive solution to the Yule-Walker equations by the bordering technique of linear algebra. This also allows us to obtain the recursive formula for the Toeplitz determinant. In the manner of A.J. Lawrence we then introduce the partial correlation as ordinary correlation between two variables after their linear dependence has been removed. Minimization of the forward and backward errors is then done with respect to the partial correlation coefficients. The minimization is done stage wise, constraining higher partial correlation values to zero. Thus, the minimization is done for a maximum entropy Gaussian process; the Toeplitz determinant is a maximum. Numerical results are presented for the Burg (maximum entropy) and Durbin algorithm for a seismic event measured at the site of the National Museum, Bogota, Colombia.

AUTOREGRESSIVE MODELS FOR NONSTATIONARY DISCRETE-TIME PROCESSES, H.Lev-Ari and T. Kailath (USA). It is a widely used fact, for example, in the linear predictive coding of speech waveforms and in maximum entropy spectral analysis, that an autoregressive (AR) model can be fitted to the first N values (lags) of the autocorrelation function of any discrete-time stationary process. This autoregressive model is usually realized by a tapped-delay-line (or transversal) filter with N taps or by a ladder (or lattice) filter with N sections. If the process actually is autoregressive of order n, then we shall need only n taps, which will become constant (time-invariant) as soon as $N \geq n$. Using a ladder-filter implementation has the advantage that the sections have time-invariant gains, except that we have to add in additional sections until N=n. Finally we mention that such AR models have certain best approximation properties, e.g., that AR models minimize the so-called Itakura-Saito distance.

The purpose of listing these known properties of AR model-fitting of stationary processes is that in this paper we shall show that they can all be extended in a nice way to nonstationary processes.

First we shall show that a growing memory-tapped-delay-line filter with time-invariant gains can be used to match the N^2 coefficients $\{R(i,j), i,j=0,\ldots,N-1\}$ of any, stationary or nonstationary, discrete-time process.

The process generated by this particular model also turns out to have the maximum entropy among all probability distributions with covariances that agree in the band specified above with the given covariance function.

Finally we shall show that if C is some set of n-th order models then the best fit in C to any given nonstationary covariance matrix R is the model that minimizes a directed divergence measure, which turns out to be the appropriate nonstationary version of the Itakura-Saito distortion measure.

NEW METHODS FOR PROBABILITY DENSITY ESTIMATION, R.B. Holmes and L.K. Jones (USA). Several methods for probability density function (pdf) estimation are introduced and studied. These new methods involve (1) a variable knot spline approximation to the empirical distribution function; (2) RKHS concepts to estimate an integral transform of the true pdf; and (3) rational modification of orthogonal expansions, combined with a stopping rule determined by a nearest neighbor statistic (with respect to a reference pdf). The latter two

methods apply (in principle) to density estimation in any number of dimensions.

Representatives of these new methods are contrasted with currently popular existing procedures, such as the cosine series expansion, DMPLE, and a kernel estimator. Samples of size 50, 100, and 200 are generated from a variety of test pdf's, the various estimators are applied to these samples, and several error measures (L^1-distance, L^2-distance, divergence, etc.) are computed. Special attention is paid to the ability of the estimators to resolve closely spaced modes of true pdf's.

Recommendations for practical usage are offered, based upon this testing and upon the underlying convergence theory for the various methods. (This work was sponsored by the Department of the Army. The United States Government assumes no responsibility for the information presented.)

COMPUTING THE DISTRIBUTION OF A RANDOM VARIABLE VIA GAUSSIAN QUADRATURE RULES, M.H. Meyers (USA). Approximating the cumulative distribution function of a random variable is a problem of long standing interest and is often the only viable approach to solving certain intractable problems. Here we are interested in techniques based on the use of a finite number of moments of a random variable. In this paper a new estimator for the CDF of an arbitrary random variable is proposed based on the application of Gaussian Quadrature Rules. A number of examples are given which show the convergence of these estimators for the cases of continuous random variables and discrete random variables. The examples illustrate important considerations such as the effect of symmetries on the algorithm, potential stability problems and a useful implementation strategy.

SESSION E3

Multi-User Information Theory II

*TO GET A BIT OF INFORMATION MAY BE AS HARD AS TO GET FULL INFORMATION, R. Ahlswede (Germany) and I. Csiszar (Hungary). We consider the following coding problem for correlated discrete memoryless sources:

The two sources can be separately block encoded and the values of the encoding functions are available to a decoder, who wants to answer a certain question concerning the source outputs. Typically, this question has only a few possible answers (even as few as two). What are the rates of the encoding functions needed to enable the decoder to answer this question correctly with high probability?

We prove that these rates are often as large as those needed for a full reproduction of the outputs of both sources. Furthermore, if one source is completely known at the decoder, this phenomenon already occurs when one asks the joint type (joint composition) of the two source output blocks, or some function thereof such as the Hamming distance of the two blocks or (for alphabet size at least 3) just the parity of this Hamming distance.

THE PROBLEM OF ISOMORPHISM FOR GENERAL DISCRETE MEMORYLESS STATIONARY CORRELATED SOURCES, K. Marton (Hungary). Necessary and sufficient conditions are given for the isomorphism of discrete memoryless stationary correlated sources with maximal correlation less than 1. (This work was completed while the author was on leave from the Mathematical Institute of Hungarian Academy of Sciences, and visiting the Laboratory for Information and Decision Systems at the Massachusetts Institute of Technology. This work was supported by NSF under grant ENG-77-19971.)

AN ITERATION LEMMA AND ITS APPLICATION TO SUCCESSIVE CODING OF MULTIPLE SOURCES, T. Ericson (Sweden) and J. Korner (Hungary). Coding for networks of sources with respect to an additive distortion measure is considered. The key result is an iteration lemma with the aid of which it is, in

certain cases, possible to extend to a whole network certain coding results holding for a part of the network. The idea is illustrated by an application of the iteration lemma to the problem of successive coding of a multiple source. By this we understand a code for a multiple source $\{(X_i(1),X_i(2),\ldots,X_i(m))\}_{i=1}^{\infty}$ such that the encoder is a set of mappings $f_\nu: X^n(\nu) \times \prod_{\mu<\nu} M_n(\mu); \nu=1,2,\ldots,m$ and the decoder is a mapping $: \prod_{\nu=1}^{m} M_n(\nu) \to Z^n$, where $X(\nu)$ is the alphabet of the ν:th component of the source, Z is the reproduction alphabet and the $M_n(\nu)$:s are arbitrary finite sets. With the aid of the iteration lemma we prove a coding theorem showing that a certain rate region is achievable. We do not believe that the bound is tight in general. However, in a special case involving only two sources a complete solution is presented based on an entirely different argument.

SOME NEW RESULTS OF SHANNON THEORY, H. Guoding and S. Shiyi (China). In this paper, we have summarized the fundamental ideas and the new results of the general multi-user communication theory and the source coding theory. The general multi-user communication network system considered in this paper includes as special cases all the models of multiple-access channels with a general correlated encoder (regular multiple-access channels and multiple-access channels with correlated encoder input and with correlated output) and general broadcast channels (regular broadcast channels, degraded broadcast channels, broadcast channels with correlated output and with decoder output multiple-terminal). For this general network system, we obtain a general fundamental coding theorem of multi-user communication sequences, from which we may immediately derive the coding theorem and its converse for the general network system channel capacity region of discrete memoryless channels. For the source coding problem, we obtain the source coding fundamental theorem of the general source sequence and the general source sequence with side information respectively. From the fundamental theorem, we may immediately derive the source coding theorem and its converse for the stationary ergodic source and the stationary ergodic source with side information. For the nonstationary source with memory, we may also obtain the coding theorem and its converse.

INFORMATION OF PARTITIONS WITH APPLICATIONS TO RANDOM ACCESS COMMUNICATIONS, B. Hajek (USA). The minimum amount of information and the asymptotic minimum amount of entropy of

a random partition which separates the points of a Poisson point process is found. It is shown that more information is needed if the partition sets are required to be intervals. The bounds are applied to yield an upper bound to the throughput of a random access broadcast channel. (This research was supported by JSEP grant N00014-79-C-0424.)

THE CAPACITY OF COMPUTER MEMORY WITH DEFECTS AND NOISE, A. El Gamal and C. Heegard (USA). The problem of reliable communication over noisy channels and the problem of reliable storage in computer memories are in many ways similar. However, any realistic model for the sources of error in memory cells must include permanent (hard) errors as well as the intermittent (soft) errors which are found in the communication problem. The capacity of a computer memory with both soft and hard errors is defined as the largest rate at which messages can be reliably stored. A theorem is stated which expresses an achievable storage rate for a memory when complete or partial knowledge of the location and nature of the defects is available at the encoder and/or decoder. This theorem determines the capacity of the memory when the defect information that is given to the encoder and/or decoder is complete. An example of a binary memory with hard errors and symmetric soft errors is given.

THE CAPACITY AND COMPUTATION CUT-OFF RATE OF A MULTIPLE-USER RANDOM-ACCESS COMMUNICATION SYSTEM, V.W.S. Chan (USA). This paper evaluates the performance of a multiple-user, random-access communication system. Simultaneous communication by a large number of users to a single receiver is achieved by coding user messages so that the receiver can sort out messages from individual users. The specific signaling formats discussed are Pulse Position Modulation and Differential Pulse Position Modulation, though the results can be easily applied to arbitrary orthogonal signals or simplex signals. Since no time synchronization is assumed, each user addresses the receiver in a random-access fashion. Communication performance is evaluated by the maximum allowable number of users at given rates using optimum coding-decoding. Important channel characteristics are summarized by two parameters, the capacity and the exponential parameter of the random coding bound (also known as R_{comp}, the computation cut-off rate of the channel). (This work was supported by the Department of the Air Force.)

SESSION E4

Speech Compression I

*TREE CODING VERSUS DIFFERENTIAL ENCODING OF SPEECH: A PERSPECTIVE, J.D. Gibson (USA). Numerous questions concerning tree coder performance are addressed using existing simulation results, new simulation results, and analytical models of the tree coder operation. Specifically, this paper considers the question, "What can tree coders do that differential encoders cannot?" First, it is argued that adapting the code generator, using frequency weighted error criteria, or smoothing do not provide an advantage over differential encoders since these operations are performed in differential encoders under the names of adaptive prediction, noise spectral shaping, and filtering, respectively. Second, it is shown that virtually all of the perceptual improvement and most of the gain in signal-to-quantization noise ratio generated by tree coding is available with only a very "shallow" search of depth 2, and that equivalent performance can be obtained using differential pulse code modulation and a pitch compensating quantizer. Third, it is demonstrated that not only is the SNR gain provided by deeper searches slight, the deeper search reduces output speech quality. This is because deeper searches tend to whiten the reconstruction error in comparison to DPCM, and this white noise is perceptually less pleasing. In spite of these negative results, it is felt that tree coding is still a promising approach for speech coding at 16kbps and below, but that this promise will not be achieved by simply adding a multipath search to an existing single path coder. A new tree coder structure is proposed that uses a reduced rate code in conjunction with a delayed decoding method based on fixed-lag smoothing. Analytical investigations for speech-like sources indicate that improved performance is available with this delayed decoding algorithm.

*ADAPTIVE METHODS FOR TREE ENCODING WITH SPEECH APPLICATIONS, S.G. Wilson and S. Pizzi (USA). For a variety of sources and distortion measures, tree coding is known to have the potential for performing close to the appropriate rate-distortion bound. Several instrumentable search algorithms have been developed which have given impressive performance gains in such cases as coding the binary memoryless source, Gauss-Markov sources, and speech (Anderson; Gray and Linde; Anderson and Bodie; Wilson and Husain).

The design of the code generator for such tree codes is rather crucial, but in general little analytical optimization can be done. This is particularly true for the practical case of only moderate encoder complexity. Even more relevant is that typical sources, such as speech and images, have time-varying models, for which no single code generator is well-matched.

These issues point to the need for self-optimizing encoder/decoder pairs, which within some structural class, optimize the free parameters for best rate-distortion performance by operating on sample functions of the source. Ideally, this self-tuning would be sensitive to such user inputs as code rate, error criterion, search complexity, etc.

Two important points are the following. The problem is not one of system identification, for even if the source were known exactly, determination of the optimal code generator remains a formidable problem. Second, the adaptation and tree search must possess the proper synergy. Clearly, tree searching will be of little benefit unless the code generator is well-matched to the problem. However, one must not adapt prematurely, as for example in real-time adaptive DPCM, but instead allow the search process to achieve its full power.

We consider two approaches to this problem. The first uses gradient-based ideas on the encoder's released codeword and its corresponding error sequence to drive the encoder to a minimum average distortion setting. Since the decoder is not party to the error sequence, the algorithm uses periodic quantization of the encoded error, which is also sent at small overhead in the transmitted codestream. The second approach uses a partitioned code whose subcodes are generated with parameter sets perturbed slightly from what is thought optimal. The super tree is searched for the lowest distortion codeword, and dependent on which partition is selected, adjustments are made to the nominal encoder design. The procedure stabilizes when the partitions, or subcodes, are selected equiprobably. For complexity reasons this approach appears limited to cases with a few degrees of freedom.

These methods are applied to the encoding of a stationary Gauss-Markov source with respect to squared-error. Convergence results and steady-state distortion performance will be presented. Application is also made to the tree coding of speech at rates near 9600 bps. Performance data on mean-square error will be reported, and it is anticipated that short speech evaluation tapes will be played.

SPEECH COMPRESSION SYSTEMS USING A SET OF INVERSE FILTERS, Y. Matsuyama (Japan). Two types of speech compression systems comprising a carefully pre-calculated inverse filter set are studied. The inverse filter set serves as a linear prediction codebook. This codebook benefits the data rate reduction and/or the complexity reduction of the speech compression systems since on-line LPC estimation can be avoided.

The first system considered is a kind of pitch extraction coder, and is called an inverse filter matching vocoder. The encoder finds an index for the best fitting inverse filter in the codebook and an index for the gain and a pitch interval blockwise by using the inverse filters' output processes. The systems work fairly well at lower data rates than plain LPC speech compressors.

The second system discussed is a waveform encoder which makes use of tree coding. The system consists of an inverse filter codebook using a single tree search rather than a parallel tree search at the cost of a very small data rate increase and a longer, yet allowable, delay.

Various comparisons are given. (This research was supported in part by the Science Research Fund, #555132.)

TREE AND TRELLIS SPEECH COMPRESSION, L.C. Stewart (USA). Tree and trellis speech compression systems have traditionally been designed by using a tree or trellis search algorithm to improve the performance of traditional coding systems such as adaptive delta modulation or predictive quantization. Recent work by Linde and Gray has suggested the possibility of designing new tree and trellis codes which are well matched to particular sources. The design procedure iterates on a long training sequence to improve an initial code. Additional procedures, given a trellis code, can produce a larger code which performs at least as well. Combined, these algorithms provide a complete design procedure for trellis codes. Preliminary results indicate that for random sources, performance close to the rate-distortion bound can be achieved with quite modest code complexity. In the applications area of speech coding, tree and trellis coding permit the construction of low-rate residual excited linear predictive coding (RELP) systems with quality similar to that of systems using down sampling and spectral extension.

*ON THE INFORMATION RATE OF QUANTIZED SPEECH, D.L. Cohn and J.L. Melsa (USA). Waveform encoding speech digitization algorithms use various noisy coding procedures to produce a sequence of symbols representing quantized speech. This sequence is then noiselessly encoded into a binary data stream using some form of variable length source coding. The noisy coding procedures are designed to remove the redundancy in the speech waveform caused both by pitch repetition and by vocal tract filtering. If this were effective, the entropy of the symbol sequence could be taken as the information rate of the original speech subject to some acceptable distortion level. In any case, the entropy is a lower bound to the required bit rate of the noiseless source coder. In practice, the local entropy of the symbol sequence varies widely. Therefore, even adaptive noiseless coding procedures have difficulty achieving the entropy bound even with reasonably long buffers. This paper describes various proposed solutions including intentional degradation of the quantized speech when the buffers fill and an over-full source coding procedure that is matched to the nature of the symbol sequence. Finally, an approach known as Pitched Repetition is described. This procedure deletes blocks of symbols from the symbol sequence when the entropy of that sequence gets too high. Thus, during periods which appear to convey high levels of information, it is possible to send essentially no information without noticeable loss of signal quality.

SESSION E5

Coding V

ON APP DECODING, C.R.P. Hartmann, L.D. Rudolph, K.G. Mehrotra, and G.J. Snedeker (USA). In this paper it is shown that a natural extension to nonorthogonal parity checks of Massey's APP decoding yields an optimal symbol-to-symbol decoding rule for any linear binary block code when the parity checks used completely specify the code. The structure explicated in the proof of the result shows how to choose incomplete sets of checks in such a way that the resulting decoding rule is asymptotically optimum. Performance curves for the (21,11) PG code transmitted over the AWGN channel are presented for APP decoding and maximum-radius decoding, both using five orthogonal checks, their iterative extensions, and optimum symbol-to-symbol decoding. (This work was supported by the National Science Foundation under grant ENG 79-04826.)

ON THE MAJORITY LOGIC DECODING OF A CLASS OF COMPOSITE CODES, S.G.S. Shiva and V. Mimis (Canada). Let V_i be a binary (n_i,k_i) cyclic code, where $i=1,2$ and $(n_1,n_2)=1$, d_i and D_i being respectively the minimum and maximum weights in V_i. Let $V^{(2)}$ be the composite code, of length $n=n_1n_2$, such that

$$V^{(2)}(x)=\sum_{i=1}^{2} V_i(x)\frac{1+X^n}{1+x^{n_i}} \quad ,$$

where $V^{(2)}(x)$ belongs to $V^{(2)}$ and $V_i(x)$ to V_i. In this paper we discuss the following result: If V_1 is L-step majority logic decodable with

$$d_1\leq \text{Min}\left\{\frac{n_1(n_2+1)-2D_1}{2n_2},\frac{n_1(n_2-1)}{2n_2}\right\}$$

and if V_2 is an M-sequence code, then $V^{(2)}$ has minimum distance n_2d_1 and error correction can be accomplished by $(L+1)$-step majority logic. Clearly $D_1=n_1$ for codes V_1 which have words of both odd and even weights. As regards codes V_1 which are even-weighted, let V_1' be the (n_1,k_1+1) cyclic code of which V_1 is the even-weighted subset. If V_1' is narrow-sense with designed distance d_1', then upper bounds on d_1 may be developed using this fact. This point is useful since D_1 is not generally known for even-weighted codes.

EFFICIENT DECODER ALGORITHMS BASED ON SPECTRAL TECHNIQUES, R.E. Blahut (USA). Except for the peculiar arithmetic field, the decoding of Reed-Solomon and BCH codes can be described in a way so that it strongly resembles a problem in digital signal processing. The usual decoder consists of a Fourier transform (syndrome computer) followed by an autoregressive spectral analysis (Berlekamp-Massey algorithm) followed by a Fourier transform (Chien search). The signal-processing mode of description is quite suggestive.

This paper will describe the decoding in a signal processing terminology, and use this as a point of departure to describe several new ways of decoding Reed-Solomon and related codes. In particular, we will give a decoder that works entirely in the time domain, without transforms, mimicking the steps of the Berlekamp-Massey algorithm with an equivalent process on the raw input word, and we will also give several procedures for accelerating the decoder.

A TYPE I ERASURES-AND-ERRORS DECODER FOR MAJORITY-LOGIC-DECODABLE CODES, Y. Sugiyama, M. Kasahara, T. Inoue, S. Hirasawa, and T. Namekawa (Japan). A Type I erasures-and-errors decoder for majority-logic-decodable codes is proposed. The decoder is a slightly modified version of the Type II erasures-and-errors decoder suggested by Shiva and Tavares. A major difference of the former decoder from the latter decoder is that a threshold of a majority gate is reduced by 1 when an error digit being decided is in erasure. The decoder is able to decode a received code digit correctly if N_e errors and N_ε erasures which have occurred in the code length or the constraint length satisfy the relation $2N_e+N_\varepsilon<J$, where J is the number of orthogonal parity-checks sums. The decoder presented here is applicable to decoding not only convolutional codes but also L-step majority-logic-decodable block codes, since a Type I decoder is required for decoding L-step majority-logic-decodable block codes.

A MODIFIED OMURA ALGORITHM FOR DECODING BINARY GROUP CODES, G.C. Clark,Jr., J.B. Cain, and G.H. Thaker (USA). A probabilistic decoding algorithm for decoding binary group codes was proposed by Omura in 1969. Using this technique, one postulates a sequence of solutions to the parity check equations. These solutions are chosen by trial and error such that their weight does not increase. When a solution is located which is within the correction radius of the code,

the search is terminated. Otherwise, it is terminated after a fixed number of iterations and the minimum weight solution is selected. It is shown that the average number of computations can be significantly reduced if at each stage the lowest weight solutions which has been found is used to specify a set of positions which must be error free whenever a solution of weight d-w exists. Here d is the minimum weight of the code and w is the minimum weight solution that has been found up to this point. Simulation results are presented for the (48,24) quadratic residue code. For randomly chosen 5 error patterns, the average number of decoding steps is reduced from approximately 37 to approximately 16.

SYNDROME DECODING -- RE-EXAMINED FROM A COMBINATIONAL VIEWPOINT, M. Rahman (Saudi Arabia). For a linear (n,k) code, the syndrome vector $\underline{s}$ is given by $\underline{s}=\underline{r}H^t$ where $\underline{r}$ is the received vector and H is the parity check matrix. $\underline{s}$ is an (n-k)-dimensional column vector and has therefore 2^{n-k} possible states. Each state can be associated with an error-pattern -- the most likely one. Thus a total of 2^{n-k} distinct error-patterns can be identified and corrected. However, if (n-k) is large, the task of decoding may become too impractical due to (1) large storage requirements and (2) large number of operations (comparisons) required to identify the syndrome vector with a particular error pattern. In this paper, the parity check matrix is chosen to have very well known combinatorial structures. Using the properties of these structures, the syndrome vector can be made to quickly identify all patterns of single errors, most double-error patterns, and at the cost of increased decoder complexity, other multiple error-patterns.

DESIGN AND HARDWARE IMPLEMENTATION OF A VERSATILE TRANSFORM DECODER FOR REED-SOLOMON CODES, D.O. Carhoun, B.L. Johnson, and S.J. Meehan (USA). A new design and hardware implementation of a versatile Reed-Solomon encoder and decoder based on a transform decoding algorithm is presented. The design is electronically reconfigurable to accommodate a large number of different code parameters for both primitive and non-primitive codes designed over $GF(2^m)$, the symbol fields ranging from four to eight bits. The discrete transform used for encoding and syndrome computation, regarded as polynomial evaluation, is implemented with an algorithm that tends to minimize the number of extension-field products. The error locator uses

the Berlekamp-Massey feedback shift register synthesis algorithm, which is initialized with the internally calculated erasure locator polynomial, to correct both errors and erasures up to the limit permitted by minimum distance. In a linear sequential circuit implementation, extension-field operations are separated from the normal binary operations to promote reconfiguration. This paper describes the architecture and measured performance of an operating breadboard constructed with medium-scale logic, its design being aimed at eventual VLSI implementation. (This work was supported by Rome Air Development Center, Electronic Systems Division, AFSC, under contract F19628-80-C-0001.)

SESSION F1

Estimation I

*ON ADJOINT MODELS AND FIXED-INTERVAL SMOOTHING, Howard L. Weinert and Uday B. Desai (USA). A new algorithm is derived for the standard fixed-interval linear smoothing problem in which the signal is generated by a state model. The structure of this new algorithm allows the smoothed estimate to be easily updated in response to a change in the initial state covariance matrix π_0, since, unlike in existing algorithms, the relevant Riccati equation is entirely independent of π_0. The derivation of the algorithm is based on a remarkable property of the adjoint of the model that generates the observations.

OPTIMAL BAYES SMOOTHING WITH UNCERTAIN OBSERVATIONS, M. Askar and H. Derin (Turkey). In this paper, the optimum (fixed interval) smoothing with uncertain observations problem is solved using the Bayes approach and under assumptions which are more general than the usual Gauss-Markov model that is widely used in recursive estimation problems. The observations are assumed to be of the form $y_k=g_k(\gamma_k, x_k, v_k)$, $k=1,2,\ldots,N$, where $\{x_k\}$ is the signal sequence which is Markov (not necessarily Gaussian), $\{\gamma_k\}$ is a Markov 0-1 random sequence (representing the uncertainty in the observations), and $\{v_k\}$ is the independent observation noise sequence. A recursive algorithm for the a posteriori density $f(x_k/Y_N)$, $Y_N=\{y_1,y_2,\ldots,y_N\}$, is determined. Thus, the optimal Bayes smoother $x_k(Y_N)$ that corresponds to the specified cost function, can be obtained recursively. The general formulation is then applied to the special case, where the signal x_k evolves as a Gauss-Markov process and the observation is signal (with uncertainty) plus white Gaussian noise, and recursive relationships for $f(x_k/Y_N)$ and $x_k(Y_N)$ are obtained. Due to the uncertainty, the computation of the a posteriori density $f(x_k/Y_N)$ requires geometrically growing memory. However, a computational algorithm is developed where the memory requirement increases only arithmetically with N, the number of observations.

NONLINEAR SMOOTHING USING FINITE STATE MODELS AND THE VITERBI ALGORITHM, J.K.Omura (USA) and K. Kozlowski (Poland). Using finite state model approximations to dynamical systems, the Viterbi algorithm is examined as a fixed-lag smoothing algorithm to estimate the state variables of dynamical systems in the presence of noise. Both linear and nonlinear dynamical systems are simulated on the IBM 3033 for Gaussian disturbances and the results have been compared assuming the mean square error criterion.

A TWO-DIMENSIONAL RECURSIVE SMOOTHING ALGORITHM USING POLYNOMIAL SPLINES, C.S. Kim and C.N. Shen (USA). The problem dealt with in this paper is that of smoothing a set of 2-Dimensional noise corrupted data. Here, this smoothing problem is formulated as an optimal surface fitting problem arising in approximation theory. Even though the nonrecursive technique of smoothing splines provides an optimal solution, the amount of computation increases rapidly with the size of the 2-D data. To overcome this difficulty, we develop a quarter-plane processor which computes smoothed estimates of function values and their derivatives by fitting 2-D smoothing splines in a recursive manner. The amount of computation for this recursive processor increases only linearly with the size of the 2-D data. However, due to some approximations introduced in its derivation, this recursive processor becomes suboptimal. (Research sponsored by NASA Langley Research Grant No. NAG1-61.)

A ROBUSTIZED VECTOR RECURSIVE ALGORITHM IN ESTIMATION AND IMAGE PROCESSING, I. Kadar and L. Kurtz (USA). A class of robustized vector estimators based on vector extension of the Robbins-Monro Stochastic approximation to minimum variance least squares (SAMVLS), of the Gladyshev's form, are developed. The linear regression function is interpreted as a recursive vector correlator and applied to the important problem of parameter estimation in linear models. The unknown class of measurement noise pdf's are represented by a vector extension of generalized Gaussian noise. Robustness is achieved by: (1) component-wise batch preprocessing of the data using linear rank statistics and (2) by the use of recursive estimators of the diagonal elements of the adaptive gain matrix to guarantee maximum efficiency at each step. Monte Carlo simulation in Gaussian mixture noise of a reparameterized k-observation per cell linear model demonstrate rapid convergence of the robustized SAMVLS to the vector of parameters.

AN ESTIMATION OF A GAUSSIAN MESSAGE FROM NON-GAUSSIAN OBSERVATION USING LINEAR TIME-VARYING FILTER, R. Doraiswami (Brasil). An estimation scheme based on modifying the Kalman-filter algorithm to include a pre-filter so that the probability distribution of the estimation error is asymptotically normal, is proposed. The pre-filter is a linear time varying system with innovation process as input. The pre-filter "Gaussianizes" the observation noise component of the innovation process. The message process is modelled as a linear dynamical system excited by white Gaussian noise input. The observation process is modelled as a linear algebraic equation with white non-Gaussian input. The white noise sequences arte independent and identically distributed and have finite variances. The proposed filter is shown to be stable. In the steady-state, the probability of large estimation error is smaller and for a class of message and observation error is linear optimum as well.

A NONPARAMETRIC METHOD OF RECEIVER TIMING ACQUISITION AND TRACKING, S.Y. Mui (USA). The problem of interest is the resolution of timing uncertainty that a receiver may experience on initial power-up. This time-of-arrival estimation problem, as it is generally called, has been widely studied for channels corrupted by only broadband noise. This paper considers in addition the presence of an interfering signal that could disrupt receiver timing. Our approach to the estimation problem is to employ a two-step process: acquisition and tracking. In acquisition we reduce the time ambiguity to less than the duration of the synchronization pulse. A more accurate estimate is then obtained by means of a tracking loop. The acquisition problem is similar to M-ary hypotheses testing. The decision statistics are obtained from a pair of orthogonal filters: one matched to the sync pulse and the other orthogonal to it. Tracking is achieved with a first-order loop driven by a hard-limited error signal derived from an early-late gate estimator.

This paper presents performance bounds on the acquisition algorithm. We also consider optimization of the early-late gate estimator. Finally, the steady state as well as the transient behavior of the tracking lop are studied by computer simulation and approximate analysis. (This work was sponsored by the Department of the Air Force. The views and conclusions contained in this document are those of the contractor and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the United States Government.)

SESSION F2

Communication Networks III

POISSON FLOWS ON MARKOV STEP PROCESSES, F.J. Beutler and B. Melamed (USA). A Markov step process Z equipped with a possibly non- denumerable state space X can model a variety of queueing, communication and computer networks. The analysis of such networks can be facilitated if certain traffic flows consist of mutually independent Poisson processes. Accordingly, we define the multivariate counting process $N = (N_1, N_2, \ldots N_c)$ induced by Z; a count in N_i occurs whenever Z jumps from $x \in X$ into a (possibly empty) target set $L_x(i)$. We study N through the infinitesimal operator A of the augmented Markov process W=(Z,N), and the integral relation connecting A with the transition operator T_t of W. It is then shown that N_i is expressed in terms of a non-negative valued function r_i defined on X; $r_i(x)$ may be interpreted as the expected rate of increase in N_i, given that Z is in state x. For univariate N (i.e., c=1), we show that N is Poisson iff (a) $E[r(Z(t))]$ is constant and (b) $E[r(Z(t))|N(t)]=E[r(Z(t))]$ for each $t>0$. These "local" conditions are weaker than the usual global sufficiency criteria, which moreover require stationarity (of Z) and independence (of N(t) and Z(t)).

A multivariate N is Poisson (i.e., composed of mutually independent Poisson streams N_i) if each $r_i(Z)$ is stationary, and $r_i(Z(t))$ is independent of N(t) for each i and each $t>0$. The latter is already much less restrictive than the independent of N(t) and Z(t), but we are able to find even weaker hypotheses which are both necessary and sufficient for N to be Poisson.

DELAY ANALYSIS OF A TWO-QUEUE, NON-UNIFORM MESSAGE CHANNEL, S.B. Calo (USA). A Message Channel is defined as a tandem connection of single server queues in which the successive service times experienced by any particular customer are scaled versions of the same random variable, and thus serves as a model for sparsely-connected store-and-forward data communications networks (or network segments) where messages typically preserve their lengths as they traverse the system. A particular instance of such a non-standard queueing model is analyzed in this paper. The system consists of two single server queues in tandem subject to a Poisson arrival

process (at the first queue), and providing service according to scaled versions of a sequence of two level, discrete random variables. A set of recursive equations that can be used to solve the model for any given scaling factor at the second queue (normalized with respect to the first queue service) will be explicitly derived. In addition, complete solutions will be displayed for several cases of interest, and the equilibrium mean cumulative waiting times for these instances will be compared as a method of indicating the impact of the scaling factor on the operation of the system. The extension of several results to systems with more general service time processes will be discussed.

ON GENIE-AIDED UPPER BOUNDS TO MULTIPLE ACCESS CONTENTION RESOLUTION EFFICIENCY, T. Berger, N. Mehravari and G. Munson (USA). Molle has used a "genie" argument to derive an upper bound on the efficiency with which Bernoulli or Poisson messages can be multiplexed onto a multiple access broadcast channel. We introduce a new genie who provides less information when contentions occur than does Molle's genie. We prove that the new genie nonetheless is beneficent in the sense that he, too, reduces the multiplexor's uncertainty as to the detailed nature of the contention. It is usually but not always true that entropy and minimal search effort are monotonically related. If that were to prove to be the case for this problem, then our genie would lower Molle's upper bound for the Poisson case from 67.31% to 52.54%. This is very close to the Gallager-Humblet lower bound of 48.78%.

BOUNDS ON THE CAPACITY OF INFINITE POPULATION MULTIPLE ACCESS PROTOCOLS, M.L. Molle (USA). We present bounds on the maximum channel utilization (with finite average delay) when an infinite population of homogeneous stations uses the best synchronous multiple access communications protocol to exchange messages. Messages arrive to the system as a series of independent Bernoulli trials, with probability p of an arrival at each arrival point (the Poisson limit is explicitly included), and are then randomly distributed among the stations. Pippenger has shown that ρ cannot exceed ζ_p for such a system where $\zeta_1=1$ and $\lim_{p\to 0} \zeta_p \approx .744$. Using a "helpful genie" argument, we show that ρ cannot exceed p if $p \geq 1/\sqrt{2}$. The argument is extended to find the exact capacity for all $p \geq .568$ (where the optimal algorithms are FCFS); for smaller values of p, the bound decreases monotonically to $\approx$ .6731 in the Poisson limit as $p \to 0$. If we restrict our attention only to the case of Poisson arrivals, we may take

advantage of the fact that messages can potentially arrive arbitrarily closely in time to show a stronger upper bound of $\approx .6125$, valid for arbitrary multiple access protocols. A similar "genie" argument is used to give a tighter bound for FCFS protocols, exact for all $p>.41$, which converges to $\approx .508$ in the Poisson limit.

TOPOLOGY DESIGN FOR TIME SLOTTED PACKET RADIO NETWORKS, D. Towsley and C.G. Prohazka (USA). A time slotted packet radio network (TSPRN) is a collection of radio broadcast nodes which schedule packet transmission by way of dividing up time into fixed length slots. Different pairs of nodes are allowed to communicate through a combination of frequency division multiplexing and time division multiplexing. In this paper, the problem of designing a good topology for a TSPRN is considered; a good topology being one which provides good performance (low package delays, high packet thruput). This topology design problem is rephrased into the standard graph theoretic problem of obtaining graphs with diameter k whose nodes have degree d ((d,k) graphs) which contain the maximum number of nodes. Though the maximum size (d,k) graphs are not obtained, the solutions in this paper are generally better than those previously reported. Finally, because of the time scheduling nature of TSPRN's the problem of obtaining the maximum size (d,k) graphs which are also d-colorable is studied.

A DISTRIBUTED SHORTEST PATH PROTOCOL, F.B.M. Zerbib and A. Segall (Israel). We present a distributed protocol for obtaining the shortest path between all pairs of nodes in a network with weighted links. The protocol is based on an extension to the Dijkstra (centralized) shortest path algorithm and uses collaboration between neighboring nodes to provide the information needed to successively obtain the shortest paths. We provide the exact algorithm that each node performs to participate in the protocol and complete validation proofs of its properties. One major contribution of this work is to extract the features of the protocol corresponding to the communication of information, while the remaining part is the transposition of the Dijkstra shortest path algorithm to the decentralized protocol. This separation greatly simplifies the formal validation procedure.

FINITE STATE DESCRIPTION OF COMMUNICATION DEVICES IN COMPUTER NETWORKS, A. Faro (Italy). The study of the interlocutor interconnections is a field of great interest in computer networks. The aim of this paper is to give a formal description of the Communication Devices (CDs) as a single finite state machine which summarizes the synchronization between the commands given to CD at the opposite terminals. In order to determine the state transitions and output functions, suitable algorithms must be used because of the high number of the input and state variables of CD. So a typical algorithm is also proposed to facilitate the solution of this problem.

EXPLICIT CONCENTRATORS FROM GENERALIZED N-GONS, M.R. Tanner (USA). Concentrators are sparse but highly connected graphs useful to a variety of information handling problems. This paper gives a simple technique for establishing the concentration properties of a graph by analysis of the first two eigenvalues of MM^T, where M is the input-output incidence matrix associated with the graph. If the ratio λ_2 / λ_1 is small, the graph is a good concentrator. For a class of graphs derived from finite geometries called generalized N-gons, the eigenvalue ratio can be computed easily and shows them to be excellent concentrators. The constructions can be extended by observing that the tensor product preserves eigenvalues ratios; a graph formed by taking the tensor product of two good concentrators is also a good concentrator.

SESSION F3

Detection Theory

PERFORMANCE OF A ROBUST DETECTOR FOR THE RAYLEIGH FADING CHANNEL, S.A. Kassam and J.G. Shin (USA). A robust structure for signal detection in the Rayleigh fading channel is proposed. For the detection of a bandpass known signal with Rayleigh amplitude and uniform phase we first show the degradation in performance of the square-law detector when the in-phase and quadrature noise components have small degrees of non-Gaussian contamination. The robust detector uses limiter-squarers instead of square-law characteristics to limit the influence of occasional, large observations. Specific numerical results illustrate the considerable advantage of the robust structure when small degrees of deviation occur from the nominal Gaussian assumption. This robust structure can also be applied in the binary signalling case. (This research is supported by the Naval Research Laboratory under contract N00014-78-0798.)

DETECTION OF WEAK SECONDARY SIGNALS WITH THE AID OF ALREADY DETECTED STRONG PRIMARY SIGNALS, H.M. Hall, T.T. Kadota, J.B. Seery and M.H. Silverberg (USA). We consider a problem of detecting a weak secondary signal in noise with the aid of a related strong primary signal which has already been detected. Such a problem arises in classification or verification of signal sources. The two signals are assumed to be narrow-band Gauss-Markov processes whose amplitudes and carrier frequencies respectively are constant multiples of each other but the constants are unknown parameters. The noise is assumed white Gaussian. We develop an iterative scheme of obtaining the maximum likelihood estimates of the unknown parameters and use the estimate of the amplitude parameter as the detection statistic. In the case of high primary signal-to-noise ratio and large data (i.e., long observation), it is shown that this estimate becomes the optimum detection statistic in the Neyman-Pearson sense.

CONVEXITY PROPERTIES OF MEASURES OF CLASS SEPARATION IN STATISTICAL DECISION THEORY, P. Fishman and L.K. Jones (USA). Frequently used measures of separability between two statis-

tical hypotheses are the Bhattacharya distance and divergence. It is shown that both these measures are strictly convex functions of their parameters for two important situations related to observations of Gaussian signals in additive Gaussian noise. This property has practical implications for problems of optimal signal design. An illustrative example is given related to the problem of determining the Gaussian noise process which optimally masks a given Gaussian signal process. Some extensions of the convexity property to the non-Gaussian cases are noted.

SELF-ADAPTIVE TUNING DETECTION OF APERIODIC SIGNALS FROM APERIODIC NOISE, G. Colonnese and B. Castagnolo (Italy). A method for self-adaptive signal-from-noise filtering is introduced, which procedes in the same way of the previous PRESIDENC method. Whereas this latter is restricted to pairs of processes, of which at least one is periodic, the new method is extended to completely aperiodic uncorrelated or weakly correlated pairs. This method is based on what could be called "correlation resonance", i.e., a suitable functional which becomes extreme correspondingly to known curves:

$$J_{\Delta} = \int_{\Delta} z[\, p(t)+q(t), \dot{p}(t)+\dot{q}(t), t]\, dt \quad .$$

In this problem, p+q is known, and corresponds to the sum of the autocorrelation functions of the processes of the above mentioned pairs. The suitable function z is found by the solution of the Euler differential equation. Besides the analytical solution, in the discrete-variable domain, this solution could be found by a suitable algorithm at the computer. A resonance curve can be built which indicates, at its extreme, the unknown autocorrelation function of one of the processes. Once the autocorrelation is known, the signal (or noise) detection can be performed by known methods (Wiener optimum, or Widrow, etc.), but we suggest another procedure based on the known relationships between covariance matrices and signal (or noise) samples and other constraints.

GENERALIZED DETECTION PROCEDURE BASED ON THE WEIGHTING OF PARTIAL DECISIONS, V. Milutinovic (Yugoslavia). The suboptimum detection procedure based on the weighting of partial decisions has been previously introduced and analyzed for binary transmission and an antipodal set of signalling symbols. According to this procedure, the band-limited mixture

of receiving signal and noise, during a single signalling interval, is transformed into a set of statistically independent information units. A partial decision is performed upon each unit and the final detection is done over the weighted sum of all partial decision. The procedure is cost-effective, because A.D. conversion and multiplication are avoided. In this paper, the concept of detection procedure based on the weighting of partial decisions is expanded to M-ary transmission and an arbitrary set of signalling symbols. Two variants of detection algorithm are presented. One is based on "relative", the other on the "absolute" approach. Optimization relations for the basic detection parameters are derived for both variants. The connection between this detection procedure and the other two, which were introduced earlier in the literature, is shown. On the basis of this connection, the proof of convergence in case of M-ary signalling is derived. The exact expression for the probability of error versus SNR is given. By means of this expression, the family of error probability versus SNR curves is calculated for binary antipodal and quaternary biorthogonal set.

A GEOMETRIC APPROACH TO THE DETECTION OF SIGNALS OF UNKNOWN ENERGY IN GAUSSIAN NOISE OF UNKNOWN MEAN AND POWER, M.A. Blanco (Italy). In this paper we consider the problem of the detection of a signal $A \cdot s(t)$ of known shape, but unknown energy ($s(.)$ is known but A is unknown), in the presence of additive Gaussian noise of unknown mean and power (the expected value m and variance σ^2 of the noise are unknown), in which case the idealized likelihood ratio test cannot be used. A discrete time approach is followed and the case in which the noise is stationary Gaussian process is considered first. A test statistic is derived by first obtaining estimates of the parameters A, m and σ which are then used in the generalized likelihood ratio. The estimates are obtained by projecting the observed vector onto a subspace orthogonal to the noise mean vector (for the signal energy estimate), or a space orthogonal to the signal vector (for the noise mean value estimate). For the noise power estimate, the observed vector is projected onto a subspace orthogonal to the signal and noise mean vectors. The parameters A, m, and σ are then estimated directly from these projected vectors. It is shown that this approach yields test statistics which have the F and t distributions, and provide constant false alarm rate tests of hypothesis H_0 (signal absent), versus its alternative H_1 (signal present). The performance of these tests in stationary and nonstationary Gaussian noise is examined, and it is shown that for cases of practical interest the CFAR losses are less than 1 dB (for the stationary case).

AN INNOVATIVE APPROACH TO SIGNAL DETECTION FOR UNKNOWN SIGNALS, G. Sogliero (USA). A two-way analysis-of-variance (ANOVA) with cross-classification, when performed on time versus frequency matrices of spectral response characteristics, can be a viable technique for the detection of signals in noisy data. Each ANOVA tests three hypotheses. These hypotheses can be formulated as the following questions: (1) Are there response differences within time? (2) Are there response differences within frequency? (3) Are there response differences between time and frequency? The response variable is some spectral characteristic, such as power, intensity, phase, or degree of polarization. A negative answer to all three questions would imply the normal situation of background noise only. An affirmative answer to one or more of the questions would indicate the presence of an event that needs to be saved for additional analysis and classification into signal-type groups for pattern recognition procedures. The potential of the analysis-of-variance as a signal detector is partially explored by means of computer simulation and a series of systematic experiments. The computer simulation involves modeling the noise field as a (time versus frequency) matrix of exponentially distributed random variables. Four types of signals - narrow-band, broad-band pulsed, slowly drifting narrow-band, and drifting narrow-band signals - are studied at varying signal-to-noise ratios. The sensitivity of the technique to quantization of the data is also examined.

OPTIMAL M-ARY SYSTEM WITH POLYNOMIAL FORM PULSE CODE MODULATION, V.E. Neagoe (Romania). An original M-ary multiform transmission system is presented, characterized by the fact that the waveforms carrying the multiplexed information are made up of orthogonal and equal energy polynomial segments. A general expression of the orthonormated polynomials on [0,T] interval and their relations with Legendre polynomials are deduced. By the application of the polynomial signals at the input of a linear system (which corresponds to a bandlimiting channel), there is obtained a weakening of the properties of orthogonality and equal energy of the signals. The cases of limiting the spectrum of the polynomial by an ideal low-pass system, respectively by a causal utterworth system are being considered. On the basis of a group of calculus hypotheses, an upper bound on the probability of error in the presence of intersymbol interference and additive Gaussian noise is evaluated. An experimental model of the presented system is achieved. The optimal characteristic of the multiform M-ary transmission system consists in assuring a minimum probability of error at the detection, in the presence of perturbations; the corresponding hardware can be implemented without difficulties.

SESSION F4

Shannon Theory IV

COMPETITIVE OPTIMALITY OF KELLY-BREIMAN GAMBLING, R.M. Bell and T. Cover (USA). In an attempt to obtain an objective solution to the problem of choosing an optimal portfolio in the absence of any well established optimality criteria, we examine the two-person zero sum game with payoff $E\,\phi(S_1/S_2)$, where ϕ is any monotonic nondecreasing function, and S_1, S_2 are the random capital returns resulting from given portfolio strategies. We compare the answer to this game theoretic problem to the portfolio $\underline{b}^*$ that maximizes $E\,\ln S = E\,\ln \underline{b}^t \underline{X}$, where $\underline{b}$ is a portfolio and $\underline{X}$ is the random vector of stock outcomes. It will be shown that $\underline{b}^*$ is the heart of the solution to all ϕ-games. More specifically, the game with payoff $E\phi(S_1/S_2)$ is solved for either player by first employing fair randomization to the initial capital, where the randomization depends only on the function ϕ, and then distributing the resultant random capital according to $\underline{b}^*$. Consequently, since $E\phi(S_1/S_2)$ can be considered to be the regret of a portfolio manager using portfolio $\underline{b}_1$ instead of $\underline{b}_2$, we see that $\underline{b}^*$ minimizes this regret independently of the subjective choice of the function ϕ. In this sense $\underline{b}^*$ is competitively optimal for all games $O(S_1/S_2)$. When we put this together with the known long-term optimality properties of $\underline{b}^*$ (Kelly and Breiman), we see that $\underline{b}^*$ simultaneously satisfies the three objective criteria: competitive optimality, maximum growth rate, and minimum time to achieve a goal.

SHANNON'S ENTROPY AND SOME DISTRIBUTIONS OF BINOMIAL COEFFICIENTS DEFINED ON PASCAL'S TRIANGLE, N. Cot (France) and T.M. Cover (USA). It is shown that the binomial coefficients along horizontal slopes of Pascal's triangle are unimodal and asymptotically gaussian. We show that this is true for arbitrary slopes through Pascal's triangle. We first identify the peak using a heuristic based on Shannon's entropy. We then derive the critical descriptive parameters shown to be intimately related to generalized Fibonacci numbers and the associated Shannon entropy. Various connections are established with binomial distributions.

ON THE SELECTION OF MEASURES OF DISTANCE BETWEEN PROBABILITY DISTRIBUTIONS, J. Abrahams (USA). Two notions of relative strength and weakness are defined for the comparison of measures of distance between probability distributions and are shown to be appropriate for use in the selection of distances as quasi-optimal design criteria in problems such as signal selection and detector design when the preferred criteria, probability of error and asymptotic relative efficiency, are intractable. Theoretical work involving distances of the Ali-Silvey class and the Bhattacharyya distance is consistent with the experimental findings of previous investigators in showing that the Bhattacharyya distance is stronger than the J-Divergence in an appropriately defined sense.

SCHURCONVEXITY AND MEASURES OF CERTAINTY AND INFORMATION, J.C.A. van der Lubbe and Y. Boxma (The Netherlands). Recently an invited paper of the IEEE Transactions on Information Theory (May 1980) Witsenhausen has pointed out the usefulness of some aspects of convexity with respect to information theory. Among the types of convexity Witsenhausen mentioned the socalled Schurconvexity. In this paper it will be shown that the property of Schurconvexity is important with respect to probabilistic certainty measures, whereas Schurconvexity is fundamental with respect to probabilistic information measures. It will be shown that Schurconvexity functions satisfy properties which can be considered as certainty-like properties and that Schurconcave functions have information- like properties. As an extension to the probability concept we introduce a general class of certainty measures which satisfy the property of Schurconvexity. Based on the relation that intuitively has to exist between certainty and information, we give a characterization theorem which leads to three general classes of information measures. The properties of the three general classes of information measures will be discussed, and their mutual relation will be studied. We also pay some attention to the problem of the choice of the values of the parameters appearing in the information measures.

MINIMIZATION OF DISCRIMINATION MEASURES, N.L. Aggarwal and B. Bouchon (France). By using the generalization of Kullback's directed divergence introduced by Csiszar with the help of a convex function h, we extend a basic inequality of Kullback dealing with the minimum value of a discrimination measure. Let $H_h(Q\,|P)$ denote the h-discrimination relative

to two probability measures P and Q, defined on the same measurable space, with Q<<P. For a given measure P. We exhibit the general form of the measure Q, respecting several constraints, nearest to P in the sense of the minimization of $H_b(Q||P)$. (Groupe de Recherche du C.N.R.S. "Structures de l'Information", Universite Paris VI, Tour 45, 4 Place Jussieu, 75230 Paris Cedex 05, France.)

ON THE HIERARCHY OF CODES FOR DMC, T. Hashimoto and S. Arimoto (Japan). It is shown that channel block codes have a fine hierarchical structure with respect to the expurgated exponent in the sense that an optimal code $C_M=\{\underline{X}_1,\underline{X}_2,\ldots,\underline{X}_M\}$ with rate $R_M=(1/N)\log(M)$ is extended to another optimal code $C_{M+1}=\{C_M,\underline{X}_{M+1}\}$ with rate $R_{M+1}=(1/N)\log(M+1)$. The hierarchy is also investigated with respect to the random coding exponent and it is compared with the expurgated exponent for group codes.

THE BEST KNOWN CODES ARE HIGHLY PROBABLE AND CAN BE PRODUCED BY A FEW PERMUTATIONS, R. Ahlswede and G. Dueck (Germany). Two new dimensions are added to the channel coding problem: 1.) We give rather precise double exponentially small bounds on the probabilities that a randomly chosen code fails to meet the random coding or expurgated bound for the discrete memoryless channel. According to these results good codes are hard to miss if selected at random. 2.) It is shown that good codes, even those meeting the random coding and expurgated bound, can be produced with relatively few (linear in the block length) permutations from a single code word. This cutdown in complexity may be of practical importance.

SESSION F5

Image Processing II

*THE EFFECT OF MEDIAN FILTER ON EDGE LOCATION ESTIMATION, G.J. Yang and T.S. Huang (USA). We study the effect of noise reduction preprocessing, specifically median filtering and averaging, on the accuracy of edge location estimation using least-squares. The original edge is either a step of a linear ramp, corrupted by white Gaussian noise or binary symmetrical channel noise, neither median filtering nor averaging improves the estimation accuracy. In the case of binary symmetrical channel noise, median filtering does improve the estimation accuracy for ramp edges which are reasonable models for real-life edges. (This work was supported by the U.S. Army Research Office under Contract No. DAAG 29-79-C-0200.)

SUBPIXEL MEASUREMENT OF EDGE LOCATION, R.O. Mitchell, A.J. Tabatabai and E.J. Delp (USA). A method is presented which finds edges in digitized pictures to sub-pixel locations. The method used is that of fitting an ideal edge while preserving the moments of the input data sequence. The advantage of this method is that a closed form solution for edge location to sub-pixel accuracy is obtained without introducing any interpolation process. Assume $[X_i]$ is a sequence of empirical edge data. The edge is a sequence $[Y_i]$ of one brightness value h_1, followed by a sequence of a second brightness values h_2. Let k be the number of h_1 values in $[Y_i]$ and N-k be the number of h_2 values. Since we have three unknowns, k, h_1, h_2, we set the first three sample moments of $[X_i]$ equal to those of $[Y_i]$. The resulting k may be a non-integer, implying that the edge need not be located at a sample point. The moment preserving problem can be formulated as a quantization scheme that is related to the Gauss-Jacobi mechanical quadrature where the edge locations are related to the so-called Christoffel numbers. This method has been shown empirically to be relatively robust to change in sequence length and to effects of additive white noise. The method requires little computation.

ON IMPROVING THE EFFICIENCY OF CHAIN ENCODED LINE DRAWINGS, J. Koplowitz (USA). We consider the problem of compressing chain encoded line drawn pictorial data. Chain encoding consists of using points on a square grid to approximate the original curve. Each element of the "chain" consists of designating the next point from among the 8 possible ones which surround the present point. Different encoding schemes yield different points on the grid. In previous work we considered a general class of encoding schemes. By determining the distribution of the chain elements we obtained the efficiency of the encoding schemes. Here, the correlation of the chain elements is examined for the purpose of using differential encoding, i.e., designating the change in direction of the elements. It is shown that by considering first and sometimes second order correlations one can significantly reduce the required bits for element by element encoding.

TWO-DIMENSIONAL SEQUENTIAL ALGORITHM FOR IMAGE RESTORATION, J.A. Ponnusamy and M.D. Srinath (USA). This paper considers the estimation of a discrete two-dimensional (2-D) image field modeled by a non-symmetric half-plane (NSHP) model. A two-dimensional sequential minimum variance estimation algorithm is obtained using the innovations process. A modification of the algorithm which will facilitate inplace computation and reduce the number of computations involved is presented. The computational complexity and storage requirements for the inplace estimation algorithm are discussed. Suboptimal implementations with further reduction in computations, suitable for large images are also presented. To illustrate the validity of the 2-D optimal estimation algorithm and its suboptimal approximations, the algorithms are applied to restore several monochromatic images modeled by a symmetric (1,1) NSHP model and corrupted by white additive white noise. The performance of the algorithms in terms of computation time and signal-to-noise ratio improvement is also presented.

ADVANCED MAP RESTORATION - FILTERING TECHNIQUES WITH APPLICATION TO IMAGE PROCESSING, V. Cappellini, E. Del Re, G. Francolini, and S. Taiuti (Italy). MAP restoration techniques based on the maximization of a posteriori probability, are considered for noisy image processing. In particular MAP sectioned algorithms, as introduced by Hunt and Trussell, are developed in details with special reference to the parameters involved that can be adapted to the local properties of the images. Modifications in these algorithms

and methods are described, based on the efficient control of the iterative procedure in connection with the degradation degree in the different image parts. The use of 2-D low-pass digital filters is proposed, before or after the MAP restoration, to improve the efficiency of noisy image processing especially at low S/N values. Results obtained in processing test images and real images in biomedical and remote sensing areas are presented. Considerations on the practical application of the described techniques by means of minicomputers are finally given regarding the obtainable restoration quality in correspondence with the noise levels in the examined image.

SPECKLE ANALYSIS AND SMOOTHING OF SYNTHETIC APERTURE RADAR IMAGES, J-S. Lee (USA). Coherent processing of synthetic aperture radar (SAR) data makes images susceptible to speckles. Basically, the speckles are signal-dependent and, therefore, act like multiplicative noise. This paper develops a statistical technique to define a noise model, and then successfully applies a local statistics noise filtering algorithm to a set of actual SEASAT SAR images. The smoothed images permit observers to resolve fine detail with an enhanced edge effect. Several SEASAT SAR images are used for demonstration.

IMAGE ENHANCEMENT AND RECOGNITION OF MOVING OBJECTS IN CLUTTERED BACKGROUND, N.C. Mohanty, K. Taylor and J. Pasek (USA). By taking the absolute difference of consecutive video fields, the signal to noise ratio of moving ships is increased and the ability to recognize ships on the ocean by a matched filter is significantly improved. Both analytical and computer processing results of the forward looking infrared images support the superiority of the method. The filter performs better even when the filter size does not exactly match the size of the moving objects.

DIGITAL HALFTONES AND IMAGE CODING, E.S. Angel (USA). Digital halftones have been used for a number of years to display gray scale imagry on binary devices such as electrostatic printers and graphics tubes. In this paper we will explore the use of halftones as image coders. Typical dithering algorithms will produce 8:1 compression ratios. Success

of the coding will depend on the design of a reconstruction unit other than the human visual system on the receiver end. Two types of algorithms will be introduced. The first uses statistical image information to derive optimal estimators based on the received halftone. The second type of algorithm in addition assumes the receiver has knowledge of the pseudorandom sequence used to generate the halftone. Since each received bit has different statistics associated with it which can now be used in the reconstruction process, this leads to a new type of algorithm. It will be argued that these methods lead to a type of interpolative coder without the usual difficulties associated with interpolation methods.

SESSION G1

Communication Systems IV

ERROR BOUNDS FOR MULTI-h PHASE CODES, S.G. Wilson, C-D Hsu and J.H. Highfill (USA). Multi-h phase codes, described by Anderson and Taylor, represent a class of constant envelope signal designs providing attractive gains in the power/bandwidth tradeoff, relative to MSK and QPSK. Time-variation of the transmitter deviation parameter among a small set of rational numbers provides for delayed remergers in the phase trellis, and this in turn may be exploited by a maximum likelihood sequence estimator to provide increased minimum distance between signals, enhancing energy efficiency. Error analysis thus far for these signals has concentrated on minimum distance calculations to yield asymptotic behavior, or on receiver simulation.

We develop upper and lower bounds to symbol error probability for this class of signals, including M-ary designs with nonlinear phase trajectories. The signals may be represented with a (time-varying) finite-state trellis, and we thus apply the union bound/transfer function approach to upper bounds developed earlier for linear convolutional codes. One extension necessary is to incorporate the time-varying nature of the trellis, and it is shown that the desired bound is a simple average of bounds obtained with the various trellis starting conditions implied by the multi-h code. Also, the codes do not possess the usual and convenient group property, and we invoke the concept of difference states and trellises due to Aulin to simplify the development.

Lower bounds are similarly obtained as an average of lower bounds, each dependent only on minimum distance experienced with the various starting conditions. The upper and lower bounds are asymptotically tight, and appear to be close for P_s as high as 10^{-3}.

We also obtain similar results for the case where decoder memory is not arbitrarily large, and error events due to unmerged trellis paths become significant. The bounds provide a numerical means of determining the necessary decoder memory.

The expressions developed may be simply evaluated using matrix operations. The only code-specific step is determination of the matrix of path gains in the signal flow graph; the size of this matrix and its entries depend on the

modulation indices and the form of the phase trajectory. Application of the bounds is illustrated with the simple binary linear phase codes of interest, and computer simulation results are provided for comparison.

ERROR PROBABILITY BOUNDS FOR VITERBI DETECTED CONTINUOUS PHASE MODULATED SIGNALS, T. Aulin (Sweden). The necessary conditions for a CPM signal to be coherently Viterbi detected are given, and the Viterbi detector is derived. It is shown that the metrics can be obtained from matched filters and samplers.

To be able to predict the performance when Gaussian channels are used, a new method for obtaining upper bounds on the probability of error event and symbol error, has been developed. Tight bounds are achieved and the method is useful for Viterbi decoding of non-linear trellis codes. By also using lower bounds it is possible to conclude that the performance of the detector is approximately determined by the minimum Euclidean distance for symbol error probabilities smaller than $10^{-2} - 10^{-4}$.

ON A TIGHT ERROR PROBABILITY BOUND FOR A QUANTIZED DETECTOR, S. Reisenfeld and K. Yao (USA). A binary signal, $s(t)=\pm A$, $0<t<T$ in additive Gaussian noise with zero mean, is detected using digital signal processing. The signal-plus-noise waveform is low-pass filtered, sampled and quantized. The quantized samples are summed to form a detection statistic and this statistic is compared to a zero threshold. The quantizer represents the analog-to-digital converter which would be present in systems in which the detection filter is implemented using digital arithmetic. This quantization error causes a degradation from the ideal error probability performance.

The Chernoff bound is too loose to be of much value in this quantized detection problem, where the quantization errors cause a relatively small degradation in performance. A tight upper bound on P_e is introduced which depends upon a synthesized function which upper-bounds the unit step function over a finite region. This function yields a tighter upper bound as compared to the exponential function used in the Chernoff bounding approach. This function is obtained by amplitude scaling and time shifting the finite Fourier Series approximation of the periodic extension of the truncated unit step function. The error probability is

then upper bounded by taking the expectation of the synthesized function, with the argument being the summation of the quantized observations. The final form of the upper bound is readily available in terms of the characteristic function of a quantized observation.

Various numerical examples will be given for the error performance of the quantized detection problem. The new bound will be compared with the Chernoff Bound and the actual error probability.

THE USE OF MOMENT SPACE BOUNDS FOR EVALUATING THE PERFORMANCE OF NONLINEAR DIGITAL COMMUNICATION SYSTEMS, K. Yao and L.B. Milstein (USA). This paper considers the performance of a two-link frequency-translating satellite system with an uplink to the satellite, a bandpass limiter on the satellite and a downlink to a coherent matched filter detector. On both uplink and downlink channels, independent narrow-bandlimited white Gaussian noise is added to a binary PSK signal of duration T seconds. The output of the matched filter can be expressed as the sum of two integrals, $g(T) + h(T)$, where $g(T)$ is the response to the inphase component of the downlink Gaussian noise, and $h(T)$ is the response to the output of the bandpass limiter. It is well known that $h(T)$ is a random variable whose density function is generally intractable. One approximates this integral by a finite sum of $N=2BT$ independent samples, $a(i)$, where $2B$ is the RF bandwidth of the system. Since $g(T)$ is a Gaussian r.v. of variance σ^2, then the probability of error can be expressed as $P(e) = E\{Q(a(1)+\ldots+a(n))/\sigma)\}$, when $E\{\cdot\}$ denotes expectation. $P(e)$ can be bounded by using the moment space technique. Specifically, the isomorphism theorem establishes an equivalence between the convex hull of a curve generated by an arbitrary set of continuous kernel functions and the convex body generated by the generalized moments of these kernels. By proper selection of these kernels, $P(e)$ can be taken as one of the moments, while other moments of $a(i)$ can be chosen such that they can be evaluated easily. Detailed numerical examples are given.

OPTIMIZATION AND COMPARATIVE PERFORMANCE OF SELECTION DIVERSITY RECEIVERS FOR THE RICIAN AND LOGNORMAL CHANNELS, M.A. Blanco (USA). The optimization of simple switched diversity receivers for the detection of signals in a Rician, or lognormal, fading environment is considered. The one-dimensional distribution and probability density

functions of the envelope of the received signal are obtained for two different switching strategies. This information is used to obtain the average probability of bit error for the case of noncoherent detection of binary FSK signals with Rician, or lognormal, fading envelopes and additive white Gaussian noise. The optimization of these switching strategies is then considered, and it is shown that by proper selection of switching thresholds, the average probability of error during detection can be minimized. The performance of these optimized switched diversity receivers is then examined in more detail for the cases of Rician and lognormal fading for typical parameters of interest, and it is compared against that corresponding to the Rayleigh fading case. It is also shown that these optimized switching strategies yield a significant improvement in performance over nondiversity receivers and can approach asymptotically the performance of more complex receivers such as maximal ratio combining.

LEAST SQUARE APPROXIMATION TO ERROR PROBABILITIES USING GENERALIZED GRAM-CHARLIER EXPANSIONS, R.S. Freedman (USA). The three Gram-Charlier expansions (in the sense of Gram) can be used to provide a least square estimate of probability density functions or cumulative distribution functions from sampled data without evaluating higher order moments. A method has been developed and applied to the estimation of an outage probability of a changing communication environment. Gram-Charlier approximations of the distribution function in Gaussian and beta series have been evaluated and compared.

A FAST EVALUATION OF THE ERROR RATE OF CPSK SYSTEM WITH INTERSYMBOL AND MULTIPLE CO-CHANNEL INTERFERENCES BY MEANS OF LOCAL APPROXIMATIONS OF THE ERROR FUNCTION, P. Amadesi (Italy). A computational technique for the approximate evaluation of the average error rate of CPSK systems is presented. The complementary error function erfc(x) is substituted by a suitable exponential function that approximates it at best in the limited interval of the x argument involved in the averaging operation. With this assumption the error rate in the presence of intersymbol interference and multiple interferences from other channels is assessed by simplified expressions allowing fast computation to be performed. The validity of the approximation is tested by comparing the approximate error rate curves with the exact ones obtained by simulation, for

various interfering environments. The theoretical lower and upper bounds derived by Yao and by Rosenbaum and Glave are also evaluated and compared with the new technique results. The local exponential approximation appears surprisingly reliable even in rather critical situations and can be reasonably adopted as a design tool.

SESSION G2

Estimation II

OPTIMAL FILTER BASED ON THE MUTUAL INFORMATION, S. Omatu and T. Soeda (Japan). In this paper we derive the optimal filter for a continuous-time linear system based on the mutual information principle. We consider the three problems, (i) the optimal filtering problem which maximizes the mutual information between the state and the estimated values, (ii) the optimal filtering problem which maximizes the mutual information stated in (i) and possesses the unbiased property, and (iii) the optimal reduced filtering problem which maximizes the mutual information stated in (i). For these problems, we derive the optimal filter and make clear the interrelations between the optimal filtering theory and the rate distortion theory. Finally, we show the numerical examples to illustrate the validity of the theoretical results about the optimal filter based on the mutual information theory.

MAXIMUM LIKELIHOOD ESTIMATES OF THE MEAN AND COVARIANCE BASED ON A SET OF NONLINEAR OBSERVATIONS, F-K. Sun (USA). An interative procedure is presented for computing the maximum likelihood estimates of the mean μ and covariance Σ of $\underline{x}_i$ when the observation is modeled by $\underline{y}_i = \underline{g}(\underline{x}_i) + \underline{E}_i$. The procedure is derived from the general theory of the E-M algorithm due to Dempster et al.. It is shown that the evaluation of the first and second partials of all $\underline{y}_i$'s, which is required by most existing numerical techniques, is not necessary for the proposed procedure.

ON OPTIMAL REDUCTION OF OBSERVATIONS FOR ESTIMATION, B. Picinbono and M. Benidir (France). It is well known in statistical pattern recognition that feature selection is necessary to simplify the procedure and the classical way to achieve this selection is to use the Karhunen-Loeve expansion. The same kind of problem can appear in estimation. More precisely let us suppose that we have to estimate a random variable x in terms of observations $y_1, y_2, \ldots y_n$ by using the linear least square method. For large values of n it is often difficult to use all the

variables y_i in order to estimate x. Then arises the problem of the optimal choice of m variables y_i, $m<n$, in such a way that the quadratic mean error is minimum. For $m=1$ the solution is obviously to select the observation y_i which is the most correlated with x. We give a recursive solution of this problem and we discuss its application in some examples of signal processing problems. Moreover we show that this recursive solution is not necessarily optimal if the condition of recursivity is not imposed, and we compare in some cases the results obtained by recursive and non-recursive methods.

INVARIANT IMBEDDING APPROACH TO THE SOLUTION OF LINEAR LEAST-SQUARES ESTIMATION PROBLEM WITH DEGENERATE COVARIANCE, S. Ueno (Japan). On making use of an invariant imbedding, an initial-value solution of linear least-squares filtering problem in the stationary case is presented for the recursive Hopf type integral equation with degenerate kernel. It is shown that, via the Bellman-Krein-Sobolev like relation, the impulse response function is expressed in terms of the auxiliary function, whose initial condition is given by R-function, satisfying the Riccati-type differential equation. Furthermore, it is stated that the real-time solution of the optimal estimate is reduced to a Cauchy system for an integral of the stochastic process weighted with an auxiliary function.

LINEAR PREDICTION IN CASE OF NON POSITIVE DEFINITE COVARIANCE MATRICES, C. Gueguen (France). Linear prediction has received considerable attention and has been successfully applied to a large variety of signals, but its nice properties have been established for a well behaved positive definite sample covariance (pxp) matrix R_p. In many practical cases, however, this matrix is experimentally found to be singular or even negative. Another important case where this difficulty is met is the identification of sine waves merged in noise. The corresponding correlation matrix is singular (at least for a large enough p) in the noise-free case and most noise cancelling techniques (such as Pisarenko's) consequently raise the problem of solving the normal equation in the critical case. Finally, a related problem is the computation of eigenvectors of correlation matrices now of interest in many fields (array processing, lossless, eigen models...). An efficient computation of

these vectors also requires a better understanding of the standard Levinson algorithm in the case of singular correlation matrix (by construction). This paper analyzes what happens in this critical case and gives various ways to cope with the difficulty.

Linear prediction can be generalized without difficulty to the case where the covariance matrix is non-positive. The physical interpretation is lost (negative energy of the residuals) but still the minimization problem makes sense. The critical case is met when one of the principal minors of R_p has a zero determinant.

The Cholesky decomposition (or equivalently Gauss elimination) which underlies the efficient Levinson algorithm fail to be applicable. This may happen for a nxn minor R_n while the pxp correlation matrix R_p is non singular.

The paper includes the following results: 1. The limit of the traditional L.P. solution when det $R_n \to 0$ is studied. It is shown that this limit (after blowing up to infinity) is no longer in simple relationship with the L.P. of previous order. 2. There is another choice of linear prediction models (basically lossless) that remain finite when passing the critical value n. Some new reflexion coefficients are then defined but they "reflect" between the modified models. A lossless lattice filter preserving robustness properties in the critical case is consequently proposed. 3. Based on the previous analysis, a generalization of Cholesky decomposition is then offered. This extension is based on the one and two step ahead linear predictors producing a 2x2 block artifact. The corresponding decomposition is no longer unique by attributing the outlier block to one of the factors.

ANALYSIS OF PERFORMANCE OF THE LMS ALGORITHM FOR ADAPTIVE ESTIMATION IN A NONSTATIONARY ENVIRONMENT, W.A. Gardner and M. Hajivandi (USA). Upper and lower bounding, first-order, linear recursions for the mean-squared error realized with the LMS algorithm operating in a nonstationary environment are described. Resultant general formulae for steady state misadjustment are used to optimize the adjustment step-size for minimum misadjustment for several specific problems including system identification, noise cancellation, signal prediction, and channel equalization. Sensitivity of misadjustment to deviations from optimum step-size is discussed.

IMPROVEMENTS OF ADAPTIVE LINEAR PREDICTION BY NON-LINEAR METHODS, T. Denker and D. Wolf (Germany). In order to adapt a linear prediction error filter A_N to a "short" data sequence several methods have been developed. Two of them are: (i) Evaluating the autocorrelation function from the data after optional windowing and calculating the predictor coefficients, e.g. by Levinson's algorithm. (ii) Correlating forward and backward prediction error signals in a PARCOR lattice structure realization of $A_N(z)$.

In this paper we propose the introduction of some nonlinear variations in the adaption algorithm which may affect the pole configuration but not the stability of the model. One of the methods applied is substitution of the standard correlation PARCOR coefficients

$$k_2 = -E\{\eta_2 \cdot \xi_2\} \cdot (E\{\eta_2^2\} E\{\xi_2^2\})^{1/2}$$

where and are the forward and backward prediction error signals of the th-order predictor, by polarity correlation coefficients.

a) $k_\nu^a = -E\{\eta_\nu \operatorname{sgn}(\xi_\nu) + \operatorname{sgn}(\eta_\nu) \cdot \xi_\nu\} / E\{|\eta_\nu| + |\xi_\nu|\}$ or

b) $k_\nu^b = -\sin(\frac{\pi}{2} \cdot E\{\operatorname{sgn}(\eta_\nu) \cdot \operatorname{sgn}(\xi_\nu)\})$.

These modified PARCOR coefficients will work optimally when η_ν and ξ_ν may be considered to be realizations of spherical invariant random process. In this case employing k_ν^a or k_ν^b will not only reduce the necessary number of multiplications but can also improve the spectral fit of the model - especially when reflection coefficients of large absolute value have to be estimated. The effect is based on the reduction of the estimation error by polarity correlation in the case of strong correlation.

Another method employed is a mapping to a slightly modified set of PARCOR-coefficients k_ν, subject to the conditions $|k_\nu| \leq |k_\nu'| < 1$ which guarantee stability and a kind of pole-enhancement.

The efficiency of the proposed methods has been evaluated in computer simulations. From white Gaussian noise data sequences, filtered by an all-pole filter $1/A'_{N'}(z)$, a linear prediction error filter $A_N(z)$ has been estimated after applying a window of length m. The estimation error is measured by the average $\bar{d}(S,S')$ of the spectral distance measure

$$d(S,S') = \int_{-\pi}^{\pi} \log^2\left[\frac{S'(\omega)}{S(\omega)}\right] d\omega.$$

The influence of parameters like the pole structure of $1/A'_N(z)$, the window length and type, the different correlation techniques and the reflection coefficient mappings as well as the influence of different joint densities have been analyzed in detail. The results show a significant improvement of the reconstruction of the all-pole source spectrum which in many cases is more substantial than that by other known techniques. From a more general point of view it is demonstrated that the knowledge of the joint distribution densities of a random process is required for more efficient adaptive filtering concepts.

MAXIMUM VARIANCE STOCHASTIC REALIZATIONS, F. Perez, T. Kailath and A. El Gamal (USA). The stochastic realization problem as recently studied in estimation and system theory is the following: given a factored representation of the covariance function of a a finite-dimensional process, find a Markovian model for the process, i.e., a finite-dimensional state-space model driven by white noise whose output has covariance equal to that of the given process.

There is by now an extensive body of results on this problem. Even more recently, Lindquist and Picci and Ruckebusch have focused on an abstract geometric viewpoint, encompassing also infinite-dimensional processes. Lindquist and Picci have emphasized the preservation of sample path as well as covariance properties in going between different models (stochastic realizations) of a process.

Among the different possible models, a particular role is played by models that have the minimum and maximum possible state variances. It was shown by Kailath and Geesey that the minimum-variance models could be obtained by rewriting the Kalman-Bucy filter for any given model. Later Ruckebush and Faurre, Clerget and Gramian used a time-reversal duality to compute the maximum-variance model via a Kalman-Bucy filter of a backwards Markovian model associated with a given state-space model. This construction was later also presented by Lindquist and Picci. This route via duality and a backwards model makes the specification of the maximum-variance model less explicit than it can be, at least for modeling over finite time intervals. For stationary processes over finite intervals, the minimum and maximum variance models correspond to those with minimum and maximum phase transfer functions, respectively.

In this paper, we shall present an explicit description of maximum variance models, without any reference to backwards

models. The maximum state variance, Σ^* will be given by the formula

$$\Sigma^*(t) = \Sigma_*(t) + \theta_K^{-1}(t),$$

where $\Sigma_*(t)$ is the variance of the state of Kalman-Bucy filter of any given model and $\theta_k(t)$ is the observability of Gramian of this filter. Both $\Sigma_*(\cdot)$ and $\theta_k(\cdot,\cdot)$ depend only upon the covariance function of the process, and not upon any particular assumed model (subject to certain basis constraints required to make the stochastic realization problem meaningful). Moreover, our derivation of the maximum variance model is in many ways a natural extension of the Kalman-filter-based derivation of the minimum variance model. [illegible] brings out the adjoint variable of the Hamiltonian equations for the smoothing problem. Furthermore, some illuminating interpretations and connections can be made with the Lax-Phillips and Redheffer scattering theories.

SESSION G3

Shannon Theory V

ABOUT LATTICES AND THE RANDOM CODING THEOREM, R. de Buda and W. Kassem (Canada). The Random Coding theorem is derived in a way, in which the random coding argument itself is avoided, and its place taken by a theorem from the Geometry of Numbers. The proof also demonstrates the existence of an optimal code which is not random, but has a structure which is derived from a lattice.

A NEW LOOK AT THE VITERBI ALGORITHM AND TRELLISES, F.E. Othmer (Germany). It is shown that a variety of problems including all the well-known discrete optimization problems to which the Viterbi algorithm (VA) is a recursive optimal solution can be formulated in terms of a general summation problem where the addition operation is defined on a semimodule. A general approach to the construction of a weighted trellis each branch of which is associated with an additive operator on the semimodule is presented and it is shown that if the weighted trellis is interpreted as a signal-flow graph, then the corresponding linear, causal relationships between the node variables represent a recursive solution to the summation problem. In case of the well-known discrete optimization problems this recursion algorithm is formally identical to the VA.

OPTIMAL METRIC-FIRST CODE TREE SEARCH ALGORITHMS, S. Mohan (USA) and J.B. Anderson (Canada). Two metric-first code tree search algorithms are proposed that reduce the number of accesses to storage per branch extended from O(S) for the stack algorithm to O(log S), where S refers to the number of code tree paths retained. The first one, the generalized merge algorithm, uses a main list and an arbitrary number of successively smaller auxiliary lists to store paths. This algorithm extends the best metric path at any time (hence the name metric-first), and orders them into a succession of auxiliary lists which are later merged with the main list. The second algorithm uses a class of height-balanced binary trees, known as AVL trees, to store paths. Each node of the AVL data tree is assigned a path, with the leftmost node

being the best metric path and the rightmost node the worst. Paths are extended from the leftmost node of the data tree, and, as new paths are inserted into the data tree, worst paths are dropped off the rightmost node. The generalized merge and the AVL-tree-based algorithms achieve the least cost possible for metric-first search algorithms.

AN INFORMATION THEORETIC APPROACH TO THE CONSTRUCTION OF EFFICIENT DECISION TREES, J.M. De Faria, Jr. (Brazil), C.R.P. Hartmann, C.L. Gerberich and P.K. Varshney (USA). This paper treats the problem of construction of efficient decision trees. Construction of optimal decision trees is, in general, an NP-complete problem and, therefore, a heuristic approach for the design of efficient decision trees is considered. The approach is based on information theoretic concepts and the proposed algorithm provides us with a systematic procedure for the construction of near-optimal decision trees. First, we derive an upper bound on the average cost, C, of the algorithm. The algorithm is constructed by minimizing the upper bound at each step of its construction. The same approach was used by Massey in the derivation of his first-order optimal algorithm. The computational complexity of the construction of the algorithm is presented. The systematic procedure presented in this paper provides us with a trade-off between the complexity of the construction of the decision tree and the upper bound C. In other words, a smaller upper bound on C may be achieved by increasing the complexity of the construction of the algorithm. The construction of the algorithm is illustrated by means of examples.

ALGORITHM OF STORAGE REDUCTION FOR CODINGS WITH THE USE OF CODE TREES, B. Fitingof (Germany). An algorithm is suggested for reducing the storage required for any variable-to-variable-length coding and decoding with use of a code tree (it is termed the "fusion algorithm"). It is proved that for Tunstall's variable-to-fix-length method of coding of a stationary source of independent letters the fusion algorithm reduces the storage required from M to $C \ln_m M$ where C is a constant and m is the number of symbols in the source alphabet. Some other properties of the algorithm are proved. The fusion algorithm is based on merging those nodes of code tree that issue identical subtrees.

SESSION G4

Speech Compression II

*AN 800 BPS SPEECH COMPRESSION SYSTEM BASED ON VECTOR QUANTIZATION, D.Y. Wong, B.H. Juang, and A.H. Gray,Jr. (USA). Recent developments in vector quantization since its first application to LPC speech compression have allowed significant reductions in the bit rate of LPC vocoders. A 2400 bps LPC vocoder is being modified to operate at 800 bps while retaining acceptable intelligibility and naturalness in quality.

Due to practical considerations in computation, storage requirements and speech quality, the optimal approach is replaced with a gain separated sub-optimal approach. Several other new features are also introduced to maximize the speech quality as well as minimize the complexity of the system. The design of such a speech compression system is discussed, and formal performance evaluation is presented and compared with existing LPC systems. (This research is supported by the Naval Electronic Systems Command under contract N00039-79-C-0450.)

*VECTOR CODING: A NEW APPROACH TO MEDIUM-BAND SPEECH CODING, P. Mabilleau and J-P. Adoul (Canada). Digital representation of speech in the range of 4 to 8 kbits/sec is of considerable practical interest due to the possibility of transmitting that information via modems sets through the switched telephone network itself thereby enabling encryption, statistical multiplexing with digital data, digital delay, storing, processing, etc. In that range of bit rates the speech representation uses less than one bit per sample as the Nyquist rate is usually taken around 8k samples per second.

Successful attempts at coding in that range comprise techniques called Code Excited LPC (Linear Predictive Coding), Subband Coding, Tree Coding, etc., while classical delta modulation and DPCM approaches break down.

The approach presented in the paper centers around the idea of using a dictionary of N indexed waveforms of fixed duration T (where T lies between 1 and 8 ms). The incoming signal to be encoded is then broken down into segments of duration T. For each segment we search in the dictionary for

that prototype waveform which is, with respect to some distance measure, the closest to the segment. The digital representation of the signal is thereafter the index of the prototype. The success of this approach hinges upon the judicious choice of distance measures and the ability to design a good dictionary. Furthermore, implementation considerations favor measures that are tractable and dictionaries with properties that speed up the search procedure. The paper formalizes the problem and addresses these questions in a number of situations. The basic tool for the design of the dictionary uses an iterative algorithm used in clustering and recently applied successfully to block (or vector) quantization.

The first situation is concerned with the direct encoding of the normalized speech segments composed of 8 to 16 samples using the mean square criteria and an N(=256) prototype dictionary. The second situation is concerned with the coding of the residual resulting from inverse filtering of the speech. In the third situation the speech is first divided into two subbands where the lower frequencies are dictionary encoded with a mean square error criteria in the time domain while the upper band is "dictionary encoded" using a mean square criteria on the discrete Fourier magnitudes. In the fourth situation the dictionary contains N residual prototype waveforms and a set of L linear filters obtained. The appropriate filter used in coding a specific speech segment is selected on the basis of the autocorrelation coefficients and initialized with the previously transmitted segment. The distance is then defined in the signal space, that is: the dictionary is "seen through" the coloring filter.

Subjective results in the form of simulation recordings will be presented along with signal-to-noise ratio and other objectives criteria. This study contributes a better understanding of the relationship between objective measures and subjective results and should prove itself useful in formulating a rate distortion function more relevant to speech coding. The paper also contributes new algorithms for the design of waveform dictionaries which incorporate several useful features such as minimax error constraints. These algorithms have also been designed to operate on a continuous data flow (speech samples) as opposed to the more conventional procedure consisting of iterating on the same training data.

VECTOR QUANTIZATION APPLIED TO SPEECH CODING, G. Rebolledo and R.M. Gray (USA). A recently developed family of algorithms for speech coding based on vector quantization is

described from an information theory viewpoint. The technique consists of mapping frames of a sampled speech waveform into a finite set of Linear Predictive Coded (LPC) all pole or autoregressive models so as to minimize a distortion measure that is itself a Kullback minimum discrimination information.

Recent tapes of compressed speech at rates of under 1000 bits per second will be played and the system compared quantitatively and subjectively with other very low rate systems.

VECTOR QUANTIZATION OF SPEECH AND SPEECH-LIKE WAVEFORMS, H. Abut, R.M. Gray, and G. Rebolledo (USA). Distortion-rate and asymptotically optimum block quantizer bounds for "fake speech" produced by autoregressive models of speech are obtained. Performance of locally optimum vector quantizers using Linde, Buzo, and Gray algorithm are compared with the derived theoretical bounds. The experiments have included both real speech and the "fake speech" generated by the assumed all-pole model source at rates of one bit/sample (for dimensions of k=1 to 8) and two bits/sample (for dimensions of k=1 to 4). Quality of reconstructed speech was significantly better for larger dimensions considered. Vector quantizers for real speech consistently yielded lower distortion than those of the all-pole models indicating the larger memory content in real speech.

A FAST METHOD FOR OPTIMAL ADAPTIVE DATA COMPRESSION, J. Karhunen and E. Oja (Finland). In multidimensional data compression, linear transforms are widely used. It is well-known that the Karhunen-Loeve expansion is the optimal transform in the mean-square sense. The drawback of this method, greatly diminishing its practical value, is the large amount of computations needed to first estimate the covariance matrix and then compute its eigendata. A fast algorithm is presented here that produces estimates for an arbitrary number of largest eigenvalues with their corresponding eigenvectors, without computing the covariance matrix at all, using the data samples directly. The method can be applied both to stationary and nonstationary streams of multicomponent data vectors. As the practical data base for computer simulations, over one thousand 30-component spectral vectors representing phoneme /a/ are used. The present method is considerably faster than conventional methods based on covariance matrix estimates.

SESSION G5

Coding VI

ON FINDING THE ROOTS OF POLYNOMIALS OVER FINITE FIELDS, C.L. Chen (USA). A technique is used to derive formulas for direct computation of the roots of polynomials over the finite field $GF(2^m)$. Formulas for the roots of polynomials with degrees less than or equal to 4 are discussed.

VORONOI REGIONS OF LATTICES, 2ND MOMENTS OF POLYTOPES, AND QUANTIZATION, J.H. Conway (England) and N.J.A. Sloane (USA). If a point is picked at random inside a regular simplex, octahedron, 600-cell, or other polytope, how far is it from the centroid? If a point is picked at random in n-dimensional space, how far is it from the closest point of the lattice A_n (or D_n, E_n, A_n^* or D_n^*)?

The answers are given here as well as fast algorithms for finding the closest lattice point. The results have application to quantization and to the design of signals for the Gaussian channel. For example, a quantizer based on the eight-dimensional lattice E_8 has a mean square error per symbol of 0.0717..., compared to 0.0833... for the best one-dimensional quantizer.

ON THE RADIUS OF BINARY LINEAR CODES, M. Karpovsky (USA). A method is presented for the computation of a radius of a binary (n,k) code. For $n \to \infty$ this method requires at most $2^{n-k}(n,k)\log_2(n-k-n\,H^{-1}(\frac{n-k}{n}))$ arithmetical operations where H^{-1} is the inverse function for the binary entropy. Similar complexity estimations are given for BCH codes and codes which asymptotically meet Varshamov-Gilbert bound.

SOME GENERALIZATIONS OF PERFECT CODES, G. Cohen, M. Deza, and P. Frankl (France). Perfect (n,e) codes are partitions of the n-dimensional binary vector space F_2^n with Hamming spheres of radius e, the centers of which are the codewords.

The problem of their characterization has already been solved and some extensions, e.g. uniformly packed codes, studied. We consider here the following generalizations: 1) the spheres have different radii. 2) the spheres are replaced by L-spheres, defined, for any c in F_n, by $L(c)=\{xEF_n, d(x,c)EL\}$, where d is the Hamming distance and L a subset of $\{1,2,...n\}$. 3) $(n,\{L_i\})$ perfect codes, where 1) and 2) are combined. We give necessary conditions of existence, examples of such codes and conjectures. These codes can be applied to simultaneous control of failures in networks and random errors.

(n,k,t)-COVERING SYSTEMS AND ERROR-TRAPPING DECODING, A.H. Chan and R.A. Games (USA). The technique of error-trapping decoding for algebraic codes is studied in combinatorial terms of covering systems. Let n,k and t be positive integers such that $n>k>t>0$. An (n,k,t)-covering system is a pair (X,β), where X is a set of size n, β a collection of subsets of X, each of size k, such that for all $T \subseteq X$ of size t, there exists at least one $B\epsilon\beta$ with $T \subseteq B$. Let b(n,k,t) denote the smallest size of such that (X,β) is an (n,k,t)-covering system. It is shown in this paper that the complexity of an error-trapping decoding technique is bounded by b(n,k,t) from below. Four methods for constructing small (n,k,t)-covering systems, the Cartesian Product Method, the Recursive Method, the Algorithmic Method and the Difference Family Method are given. (This work was accomplished as part of the MITRE Corporation's Independent Research and Development program.)

ON DETERMINING THE INDEPENDENT POINT SET FOR DOUBLY PERIODIC ARRAYS AND ENCODING TWO-DIMENSIONAL CYCLIC CODES AND THEIR DUALS, S. Sakata (Japan). For the purpose of encoding two-dimensional cyclic (TDC) codes, an effective algorithm for finding the independent point set of an arbitrary module of doubly periodic (DP) arrays is proposed. In addition, a method for determining the characteristic ideal of a given set of DP arrays is exhibited. With the aid of these methods it is possible to specify the structure of the generator and check ideals of TDC codes. By applying this algorithm to non-semisimple binary TDC codes with small areas, several optimal linear codes have been found and their before-unknown TDC structure exhibited.

GOPPA CODES RELATED QUASIPERFECT DOUBLE ERROR CORRECTING CODES, O. Moreno (Puerto Rico). In this paper we prove that if m m_m is odd the binary Goppa code with parameters $(2^m, 2^m-2m, 5)$ are quasiperfect. If m is even, the cyclic codes with parameters $(2^m+1, 2^m+1-2m, 5)$ are quasiperfect.

A BERLEKAMP-MASSEY TYPE PROCEDURE FOR THE SOLUTION OF THE PADE APPROXIMATION PROBLEM FOR SCALAR RATIONAL SEQUENCES, J. Conan (Canada). In this paper we consider a recursive algorithm for the solution of the classical Pade approximation of any scalar rational sequence based on the use of a variant of the Berlekamp-Massey algorithm. The approach taken here parallels directly the derivation of the original Berlekamp-Massey algorithm, shedding more light into the close relationship between this procedure and a more general algorithm introduced recently by Dickinson, Morf and Kailath. Based on the known numerical efficiency of the original Berlekamp-Massey procedure as applied, for example, to the decoding problem of Bose-Chaudhuri-Hocquenghem block codes; it is believed that such a scheme constitutes probably the most efficient procedure for the solution of the problem associated with the recursive approximation of longer portions of any scalar rational sequence.