AFCRL-70-0655

A STUDY OF PROBLEMS IN INFORMATION PROCESSING

SHU LIN
TADAO KASAMI

CONTRACT NO. F19628-70-C-0082
PROJECT NO. 5632
TASK NO. 563205
WORK UNIT NO. 56320501

FINAL REPORT
1 NOVEMBER 1969--31 OCTOBER 1970

NOVEMBER 20, 1970

CONTRACT MONITOR: VERA S. PLESS
DATA SCIENCES LABORATORY

THIS DOCUMENT HAS BEEN APPROVED FOR PUBLIC RELEASE AND SALE; ITS DISTRIBUTION IS UNLIMITED.

PREPARED FOR
AIR FORCE CAMBRIDGE RESEARCH LABORATORIES
AIR FORCE SYSTEMS COMMAND
UNITED STATES AIR FORCE
BEDFORD, MASSACHUSSETTS 01730

DEPARTMENT OF
ELECTRICAL ENGINEERING
UNIVERSITY OF HAWAII
HONOLULU, HAWAII 96822

AFCRL-70-0655

A STUDY OF PROBLEMS IN INFORMATION PROCESSING

Shu Lin
Tadao Kasami

Department of Electrical Engineering
University of Hawaii
Honolulu, Hawaii 96822

Contract No. F19628-70-C-0082
Project No. 5632
Task No. 563205
Work Unit No. 56320501

FINAL REPORT

Period Covered: 1 November 1969 through 31 Octobe, 1970

November 20, 1970

Contract Monitor: Vera S. Pless
Data Science Laboratory

This document has been approved for public release and sale; its distribution is unlimited.

Prepared
for

AIR FORCE CAMBRIDGE RESEARCH LABORATORIES
AIR FORCE SYSTEMS COMMAND
UNITED STATES AIR FORCE
BEDFORD, MASSACHUSETTS 01730

Abstract

This final report summarizes research for a one-year project. Abstracts for the two scientific reports are given, and some new results are included on reduction of context-free grammars, decoding binary block codes on Q-ary output channels, a procedure for decoding binary product codes, on the minimum weight code words of a certain class of cyclic codes, distance property of the dual codes of polynomial codes and on shortened Reed-Muller codes.

Part One

Summary of Project Research

The purpose of this project is to attain a better understanding of important error-correcting codes and the mathematical theory of languages through research on such topics as

a) Further algebraic properties of polynomial codes.

b) Majority-logic decoding for the dual of polynomial codes.

c) Weight structure of Reed-Muller codes and their related codes.

d) Construction of good convolutional codes for random error correction.

e) Reduction of context-free grammars.

f) Finite automata.

The research on the project over the past year has been reported in two scientific reports, this final report, and three journal papers and two conference presentations. One report deals with majority-logic decoding for the duals of primitive polynomial codes, one with the construction of a class of majority-logic decodable codes. The reports and their abstracts are listed in Appendix A, and papers are listed in Appendix B. This report includes the following new material on research:

Part Two: Reduction of Context-Free Grammars

Part Three: On Decoding Binary Block Codes on Q-ary Output Channels

Part Four: A Procedure for Decoding Binary Product Codes

Part Five: On the Minimum Weight Code Words of a Certain Class of Cyclic Codes

Part Six: An Upper Bound on the Minimum Distance of the Dual Codes of Polynomial Codes

Part Seven: On Shortened Reed-Muller Codes.

Part Two

Reduction of Context-Free Grammars

by

T. Kasami

The following problem has been studied. Given a context-free grammar G, find a context-free grammar with a desirable property among those grammars which are similar to G in structure.

For simplicity, context-free grammar G is assumed to be reduced [1] and to have no ε-rule and cyclic rules. Let $x = A_1 \ldots A_n$ be a sentence of L(G), the context-free language generated by G, and let d denote a derivation tree for x. By phrase $[A_i \ldots A_j]$ of d, we mean a phrase which covers subsequence $A_i \ldots A_j$ exactly. There might be two or more phrases in d which cover $A_i \ldots A_j$ exactly.

We introduce a notion that a context-free grammar G_2 structurally approximates another context-free grammar G_1. By $G_2 \xrightarrow{h} G_1$, we mean that

a) G_1 and G_2 generate the same language, i.e., $L(G_1) = L(G_2)$.

b) For any derivation tree d_1 of a sentence $x = A_1 \ldots A_n$ in G_1, there is a derivation tree d_2 of x in G_2 such that for any phrase $[A_i \ldots A_j]$ of d_1, there is a sequence of phrases $[A_{i_1} \ldots A_{i_2 - 1}]$, $[A_{i_2} \ldots A_{i_3 - 1}]$, . . . , $[A_{i_\ell} \ldots A_j]$ in d_2 with $1 \leq \ell \leq h$ and $i_1 = i$.

By definition, if G_2 is unambiguous, then $G_2 \xrightarrow{1} G_1$ implies that G_1 and G_2 are structurally equivalent [2,3,4], and if G_1 and G_2 are structurally equivalent, then $G_1 \xrightarrow{1} G_2$ and $G_2 \xrightarrow{1} G_1$. The notion of structural equivalence is too restricted for some practical applications. Without affecting the generating power of a grammar, a production rule may be replaced by some separate rules, or some rules are combined into a single rule. However, these elementary transformations do not preserve structural equivalence. On the other hand, if G_2 is derived from G_1 by a set of the elementary transformations stated above, then $G_2 \xrightarrow{h} G_1$ for some h [4].

Theorem 1: Given h, G_1 and G_2, it is decidable whether $G_2 \xrightarrow{h} G_1$.

This theorem is proved by modifying the procedure for deciding "k-structural-equivalence" described in [4].

A context-free grammar G with no two rules having the same right side is called a backwards-deterministic grammar [2].* Two nonterminal symbols X and Y of a backward-deterministic grammar G are equivalent if the grammar derived from G by replacing X and Y by a single new nonterminal symbol is backwards-deterministic and structurally equivalent nonterminal symbols is said to be reduced. A procedure for transforming a given grammar G into a reduced backwards-deterministic grammar structurally equivalent to G is known [2,5]. Two reduced backwards-deterministic grammars are structurally equivalent if and only if they are isomorphic to each other [2].

Theorem 2: Let P be a property of context-free grammars which is preserved by the transformation to a reduced backwards-deterministic grammar.**Then, given G and h, it is decidable whether there is G' with property P such that $G' \xrightarrow{h} G$.

This theorem is proved by presenting a procedure for finding G' if any. The procedure is a generalization of the one described in [5].

Corollary 1: Given G, k, and h, it is decidable whether there exists LR(k) grammar G' such that $G' \xrightarrow{h} G$.

* Two or more initial symbols are admitted.

** We assume that it is decidable whether a context-free grammar has property P.

A procedure for finding such G if any has been devised. Also, the procedure described in [5] can be generalized to one for finding a grammar with the minimum number of nonterminal symbols or production rules among those grammars which h-approximate a given grammar in structure for given h.

References

1. Ginsburg, S. (1966), "The Mathematical Theory of Context-Free Languages," McGraw-Hill, New York.

2. McNaughton, R. (1967), Parenthesis grammars, J. Assoc. Comput. Mach. 14, pp. 490-500.

3. Paul, M. C. and Unger, S. H. (1968), Structural equivalence of context-free grammars, J. Computer and System Sci. 2, pp. 427-463.

4. Fujii, M. and Kasami, T. (1968), Some structural equivalence relations and well transformations of context-free grammars, Papers of Tecn. Group on Automaton, I.E.C.E., Japan.

5. Taniguchi, K. and Kasami, T. (1970), Reduction of context-free grammars, Information and Control, 17, No. 2.

Part Three

Decoding Binary Block Codes on Q-ary Output Channels*

by

E. J. Weldon, Jr.

1. Introduction

In many communication systems the demodulator must make a "hard" binary decision after examining the received waveform. This hard decision causes a loss in channel capacity and, more importantly, a reduction in the error exponent at all rates below capacity. However, in systems using coding to improve reliability, decoding is considerably simpler if the decoder processes only binary digits. In practical situations this can more than compensate for the increased probability of error.

This paper presents a technique for decoding binary block codes in situations where the demodulator quantizes the received signal space into $Q > 2$ regions. The method, referred to as Weighted Erasure Decoding, is applicable in principle to any block code for which a binary decoding procedure is known.

In section 1 of this paper, Weighted Erasure Decoding is introduced. In section 2 two practical methods of implementing this decoding procedure are described. In section 3 we examine the performance of the (23, 12) Golay code used on the additive white Gaussian noise channel and decoded with Weighted Erasure Decoding for various values of Q. It is shown, as expected, that even small values of Q yield substantial improvements over strictly binary decoding.

It is interesting to observe that all three of the practical decoding procedures for convolutional codes -- sequential decoding, threshold

* This part was supported in part by NASA grant NGL-12-004-046 and by AFCRL contract F19623-70-C-0082.

decoding and Viterbi decoding -- are readily adapted to Q-ary output channels. Because of its simplicity, Weighted Erasure Decoding may permit block codes to be competitive with convolutional codes on some soft-quantized channels.

2. Code Structure

Assume that a binary (n,k) code with minimum Hamming distance d is used on a memoryless channel whose output can assume any one of Q possible values. We wish to devise a procedure for decoding this code which will take into account the probabilities of the different output symbols.

Consider the memoryless channel whose transition diagram is shown in Figure 1. The Q levels are ordered according to their likelihood ratios; that is

$$\frac{\Pr(0/L_i)}{\Pr(1/L_i)} > \frac{\Pr(0/L_{i+1})}{\Pr(1/L_{i+1})}$$

for $i = 0, 1, \ldots, Q-1$.

We will associate with each of the channel transitions a positive real number called the w-weight as follows:

Transitions	w-weight
$1 \rightarrow L_{Q-1}$, $0 \rightarrow L_0$	w_0
$1 \rightarrow L_{Q-2}$, $0 \rightarrow L_1$	w_1
⋮	
$1 \rightarrow L_1$, $0 \rightarrow L_{Q-2}$	w_{Q-2}
$1 \rightarrow L_0$, $0 \rightarrow L_{Q-1}$	w_{Q-1}

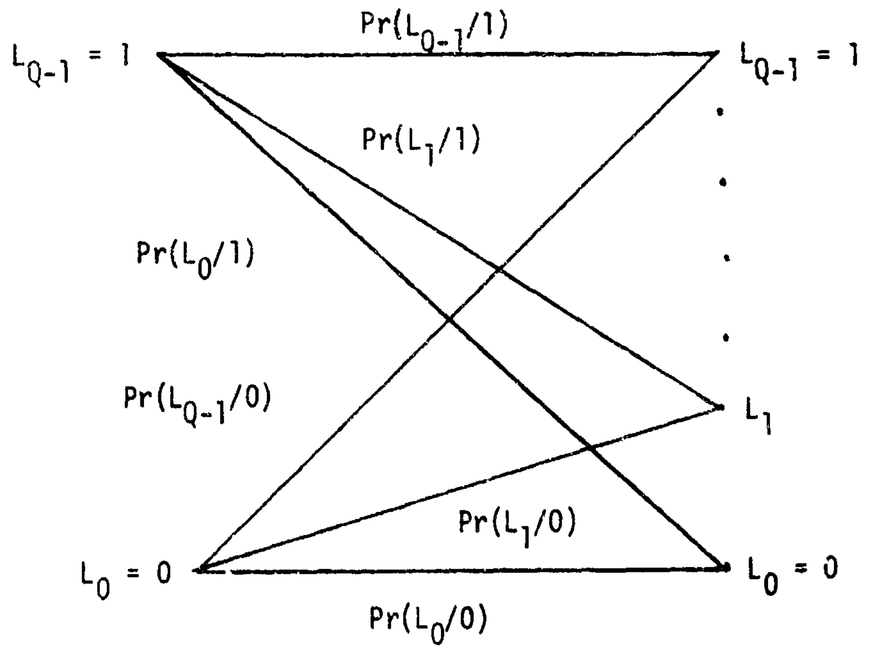

Figure 1. Transition diagram of a memoryless channel with two inputs and Q outputs.

To permit maximum likelihood decoding with equiprobable inputs, it is necessary to choose the weights w_i to be proportional to

$$-\log \Pr(L_i \mid 0) \qquad (1)$$

However, in the decoding procedure presented in this paper certain constraints are necessarily placed on the w_i. First of all, it is necessary to choose $w_0 = 0$. Secondly, for notational convenience we choose $w_{Q-1} = 1$. These constraints and Eq. (1) then suggest the restriction that

$$0 = w_0 \leq w_1 \leq \cdots \leq w_{Q-2} \leq w_{Q-1} = 1 \qquad (2)$$

The final restriction, necessary for Weighted Erasure Decoding, is

$$w_i + w_{Q-1-i} = 1 \qquad (3)$$

This last restriction may preclude choosing the w_i according to Eq. 2.

Because of these restrictions, Weighted Erasure Decoding will always be inferior to maximum likelihood decoding, although perhaps not significantly so. In order to minimize the magnitude of the resulting degradation, it seems desirable to choose the w_i to be close to the values given by Eq. 2.

We now define the w-distance between two levels as follows.

$$d_w(L_i, L_0) = d_w(L_0, L_i) = w_i \qquad (4a)$$

$$d_w(L_i, L_{Q-1}) = d_w(L_{Q-1}, L_i) = w_{Q-1-i} \qquad (4b)$$

for all i. The other distances, $d_w(L_j,L_i)$, $j \neq 0$ or Q-1, are unimportant in this paper; however for compl?eteness we can define

$$d_w(L_i,L_j) = |w_i - w_j| \tag{4c}$$

Now Eqs. 4b and 4c can be combined to give Eq. 3, explaining in part the need for this constraint. As defined, w-distance is a true metric, satisfying, symmetry, reflexivity, and the triangle inequality. In fact, for all i,

$$d_w(L_0,L_{Q-1}) = d_w(L_0,L_i) + d_w(L_i,L_{Q-1}) \tag{5}$$

The w-weight of the error in the ν^{th} transmitted digit, $0 \leq \nu \leq n-1$, will be denoted e_ν. The following theorem characterizes the error-correcting capability of binary codes on this channel:

Theorem 1: A binary (n,k) code with minimum Hamming distance d can correct any error pattern such that

$$\sum_{\nu=0}^{n-1} e_\nu = E < d/2$$

Proof: The w-distance between code words is at least d, the minimum Hamming distance of the code. If an error pattern of w-weight $E < d/2$ occurs, the received vector is w-distance E from the transmitted code word. Now assume that another code word is w-distance $E' \leq E$ from the received word. By Eq. 5 this would imply that the distance between this code word and the transmitted one is $E + E' < d$. But this is impossible, so there exists no code word closer to the received vector than the transmitted word, and the theorem is proved.

Let N_i denote the number of error digits of weight w_i.

Corollary Any error pattern is correctable provided

$$\sum_{i=1}^{Q-1} N_i w_i < d/2 \tag{7}$$

Example: For Q=3, the three outputs of the channel can be taken as 1, 0 and erasure. In this case the only possible choice for the w_i, subject to the constraints of Equations 2 and 3, are $w_0=0$. $w_1=.5$, and $w_2=1$. Then

$$\sum_{\nu=0}^{n-1} e_\nu = 2N_2 + N_1 < d$$

This is the well-known result for the binary symmetric erasure channel. It is interesting to note that for all larger values of Q, the constraints of Eqs. 2 and 3 do not completely specify the w_i.

Forney[11] has proved Theorem 1 and its corollary in a more general form; in particular, the constraint of Eq. 3 is not employed in his proof. We use the constraint here because it is necessary in the sequel and results in a somewhat simpler theorem and proof.

Error correction procedures which employ the w-distance metric are referred to in this paper as Weighted Erasure Decoding. In the next section we present two practical methods of implementing Weighted Erasure Decoding which permit the correction of all error patterns of w-weight less than $d/2$ and many of higher weight.

3. Implementation

For any choice of the w_i it is possible to find a set of $r \leq (Q+1)/2$ positive real numbers $v_1, v_2, \ldots, v_r$ such that for all i

$$w_i = A_{ri}\, v_r + A_{(r-1)i}\, v_{r-1} + \cdots + A_{1i}\, v_1 \tag{8}$$

and such that

$$\sum_{\sigma=1}^{r} v_\sigma = w_{Q-1} = 1$$

The A's are binary digits.

For the ν^{th} digit of the received vector the demodulator output will consist of r binary digits $a_{r\nu}, a_{(r-1)\nu}, \ldots, a_{1\nu}$ and the received word can be represented as an $r \times n$ array of binary digits as shown in Figure 2. Since this array must be stored by the decoder, for a given value of Q it is advantageous to choose r to be as small as possible.

3.1. In the General Case

Given that a binary decoding technique capable of correcting all error patterns of Hamming weight less than $d/2$ and perhaps others is available, decoding for the Q-ary channel can be accomplished as follows. Decode each of the rows of Figure 2 using the decoder for the binary code. For the

σ^{th} row record F_σ, the number of changes made in this row. The quantity F_σ is related to the number of bit errors in the σ^{th} row, E_σ as follows:

$$\begin{aligned} F_\sigma &= E_\sigma \quad ; \quad E_\sigma < \frac{d}{2} \\ F_\sigma &= E_\sigma \quad ; \quad \text{(correct decoding)} \quad E_\sigma \geq \frac{d}{2} \\ E_\sigma \geq F_\sigma &\geq d-E_\sigma \quad ; \quad \text{(incorrect decoding)} \quad E_\sigma \geq \frac{d}{2} \end{aligned} \tag{10}$$

Note that the total w-weight of the error pattern is

$$E = \sum_{\nu=0}^{n-1} e_\nu = \sum_{\sigma=1}^{r} v_\sigma E_\sigma \tag{11}$$

				Relative Weight
$a_{r(n-1)}$	$a_{r(n-2)}$		a_{r0}	v_r
$a_{(r-1)(n-1)}$	$a_{(r-1)(n-2)}$	. . .	$a_{(r-1)0}$	v_{r-1}
	. . .			
$a_{1(n-1)}$	$a_{1(n-2)}$		a_{10}	v_1

Figure 2. Representation of a received word.

Now following Reddy[10] we assign to each row a Reliability Indicator

$$R_\sigma = d - 2F_\sigma \tag{12}$$

Consider the tentatively decoded digits of the first column of the array of Figure 2. Certain of these digits are 1's, the others are 0's. Let S_1 and S_0 denote the index set of the rows corresponding to 1's and 0's, respectively, in the first column of the tentatively decoded array.

The decoding rule can now be stated. Choose the first information digit to be a 0 if

$$\sum_{S_0} R_\sigma v_\sigma > \sum_{S_1} R_\sigma v_\sigma \tag{13}$$

Otherwise choose this digit to be a 1. It must now be shown that this rule guarantees the correction of all error patterns of w-weight $E < d/2$.

Assume a code word C is transmitted and denote the first bit of this word as the binary digit c. Now in the absence of errors the demodulator output r-tuple will consist of r c's, since L_0 corresponds to the all-zero and L_{Q-1} to the all-ones r-tuple. (See Eqs. 8 and 9) In this case

$$\sum_{S_c} R_\sigma v_\sigma = d$$

and

$$\sum_{S_{\bar{c}}} R_\sigma v_\sigma = 0$$

where $\bar{c}$ denotes the complement of the binary digit c.

If an error pattern of w-weight less than d/2 occurs, then

$$\sum_{S_c} R_\sigma v_\sigma = \sum_{S_c} v_\sigma(d - 2F_\sigma)$$

$$\geq d \sum_{S_c} v_\sigma - 2 \sum_{S_c} v_\sigma E_\sigma \tag{14}$$

Some rows are decodec incorrectly and result in the first bit being $\bar{c}$. Thus

$$\sum_{S_{\bar{c}}} R_\sigma v_\sigma = \sum_{S_{\bar{c}}} v_\sigma(d - 2F_\sigma)$$

$$\leq d \sum_{S_{\bar{c}}} v_\sigma - 2 \sum_{S_{\bar{c}}} v_\sigma(d - E_\sigma)$$

$$= -d \sum_{S_{\bar{c}}} v_\sigma + 2 \sum_{S_{\bar{c}}} v_\sigma E_\sigma \tag{15}$$

Then Equations 14 and 15 give

$$\sum_{S_c} R_\sigma v_\sigma - \sum_{S_{\bar{c}}} R_\sigma v_\sigma \geq d \sum_{\sigma=1}^{r} v_\sigma - 2 \sum_{\sigma=1}^{r} v_\sigma E_\sigma \tag{16}$$

From Eqs. 9 and 11 we have

$$\sum_{S_c} R_\sigma v_\sigma - \sum_{S_{\bar{c}}} R_\sigma v_\sigma \geq dw_{Q-1} - 2E \tag{17}$$

If the error pattern weight, $E \leq (dw_{Q-1} - 1)/2$, then $\sum\limits_{S_c} R_\sigma v_\sigma -- \sum\limits_{S_{\bar{c}}} R_\sigma v_\sigma$ and the decoder correctly decodes the first information digit. All other digits can be correctly decoded in a similar manner.

In situations where only a bounded distance decoder is available for the binary code it is advantageous to define $R_\sigma = 0$ if an error pattern of Hamming weight $d/2$ or greater is detected in the σ^{th} row by the binary decoder. It can be shown that all error patterns of w-weight $E < d/2$ are also correctable with this modified Reliability Indicator; since rows with $R = 0$ are ignored by the decoder, the proof above can be carried through considering only rows with $R > 0$.

3.2. When the Code is Majority-Logic Decodable

For simplicity the binary (n,k) code will be taken to be completely orthogonalizable in one step. That is, we assume that it is possible to construct exactly d orthogonal estimates of any code digit. The extension to L-step decodable codes is not difficult.

The decoder for a majority-logic decodable binary cyclic code used on an Q-ary output channel is shown in Figure 3. Basically it consists of r binary decoders and a single majority gate. The majority gate has rd inputs; d have weight v_r, d have weight v_{r-1}, ... , d have weight v_2 and d have weight v_1.

In Figure 3 each of the r Syndrome Registers is a circuit which divides by g(X), the generator polynomial of the code. The inputs to the σ^{th} register are the n binary digits

$$a_{\sigma(n-1)}, a_{\sigma(n-2)}, \cdots, a_{\sigma 1}, a_{\sigma 0} \tag{18}$$

Similarly the σ^{th} Information Register stores the k "information" symbols

$$a_{\sigma(n-1)}, a_{\sigma(n-2)}, \cdots, a_{\sigma(n-k)}$$

The n-tuple (18) is treated as a possibly erroneous word in the (n,k) code. Its syndrome is calculated and the d orthogonal estimates of $a_{\sigma(n-1)}$ are formed. These are used as inputs to the majority gate where each is weighted by the factor v_σ. The ru binary adding circuits which may be needed to form the inputs to the majority gate have been omitted from Figure 3 to simplify the drawing.

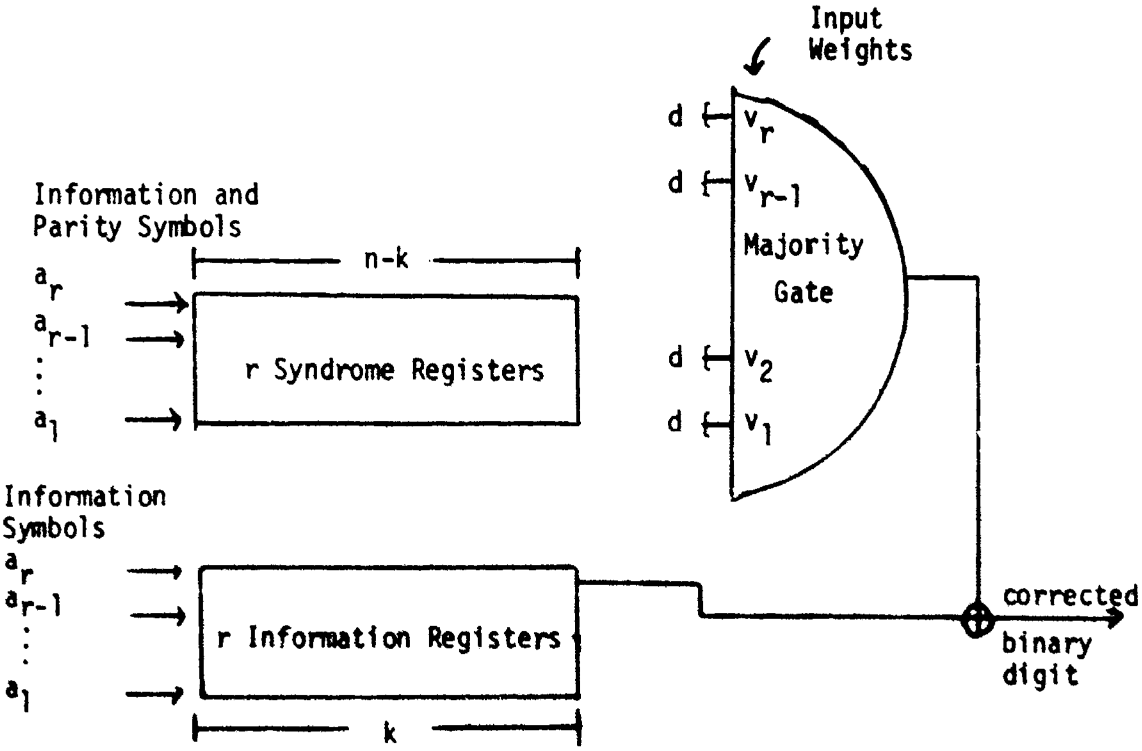

Figure 3. Block diagram representation of a majority logic decoder for a Q-ary output channel.

We now consider the error-correcting capability of the decoder of Figure 3.

Theorem 2: An (n,k) code completely orthogonalizable in one-step with minimum Hamming distance d used on a Q-ary output channel can correct all error patterns of w-weight less than d/2 using a one-step majority logic decoder. (Figure 3)

Proof: Assume that an error pattern of w-weight E less than d/2 occurs. Let c denote the value of the first information bit. We wish to show that the output of the majority gate gives the correct value of this bit regardless of the location of the errors.

An error of magnitude e_ν in position ν is represented as

$$e_\nu = e_{r\nu}v_r + e_{(r-1)\nu}v_{r-1} + \cdots + e_{1\nu}v_1 \tag{19}$$

where the e's are binary digits. Then

$$\sum_{\nu=0}^{n-1} e_\nu = v_r \sum_{\nu=0}^{n-1} e_{r\nu} + \ldots + v_1 \sum_{\nu=0}^{n-1} e_{1\nu}$$

$$= E_r v_r + E_{r-1} v_{r-1} + \ldots + E_1 v_1 = E < d/2 \tag{20}$$

where E_σ is the number of binary errors in the σ^{th} row of the array of Figure 3.

Now consider this σ^{th} row. Because the code is completely orthogonalizable it is possible to construct d orthogonal estimates of the first bit of this word; these are also estimates of the first information bit. At most E_σ of these estimates will have value $\bar{c}$; the others have value c.

These are each weighted by the factor v_σ by the majority gate. Summing on σ gives an upper bound on the total number of incorrect estimates of the first information digit:

$$\sum_{\sigma=1}^{r} E_\sigma v_\sigma = E$$

But by hypotheses,

$$E < d/2$$

so strictly less than half of the weighted inputs to the majority gate give value $\bar{c}$. Therefore the value of this output is c and the first information symbol is decoded correctly. If d orthogonal estimates of each information bit can be formed, as in a cyclic code, the entire code word can be decoded correctly.

The above procedure is closely related to Massey's APP decoding.[2] It differs in that restriction [3] will cause some degradation in performance; on the other hand the circuitry required to form the inputs to the majority gate will be simpler. Also, this procedure extends in a straightforward way to L-step decoding. After the first step all check sums required in the second step will be correctly determined provided that decoding is performed as above and that the error pattern has weight less than d/2. Subsequent steps can be identical to binary-output majority-logic decoding.

4. Evaluation of Weighted Erasure Decoding

It does not seem to be possible to calculate the probability of erroneous decoding for interesting codes. The alternative, simulation, is being performed; unfortunately no results are available at this writing.

In order to give some idea of the capabilities of this decoding procedure however, we present in Figure 4 performance curves for maximum likelihood Weighted Erasure Decoding. The channel is the standard time-discrete channel afflicted by zero-mean additive white Gaussian noise; the equally likely antipodal signals have energy E_s and the noise has variance $N_0/2$. The code employed is the (23,12) Golay code and so the energy per information bit, E_b, equals $F_s(23/12)$.

The curves are all strict upper bounds on performance with the exception of the Q=2 curve, which is exact. The Q=3, 4 and 8 curves are somewhat crudely optimized on the weights w_i and threshold settings. Interestingly enough, nearly optimal performance is obtained in all cases with evenly spaced thresholds and weights $w_i = i/(Q-1)$.

It can be shown that for long codes decoded with the procedures of Section 2, the Q=3 curve is roughly 1.4 db better than the Q=2 curve, tne Q=4 curve is 1.9 db better, the Q=8 curve is 2.6 db better, while correlation decoding is 3.0 db better. Forney[11] and Cahn[14] have obtained identical results for the cases of Q=3 and 4, respectively, using Generalized Minimum Distance decoding. This indicates that Weighted Erasure Decoding is asymptotically as good as maximum likelihood decoding.

For moderate signal-to-noise ratios, i.e., such that $p \approx d/2$ where p is the binary symmetric channel crossover probability, Forney[11] has shown that Generalized Minimum Distance decoding offers no improvement over binary decoding. Weighted Erasure Decoding corrects some error patterns of w-weight greater than d/2 and so may in fact improve on binary decoding in this range; it seems doubtful to the author that any such improvements will be significant, however. This will be the first question answered by our simulation.

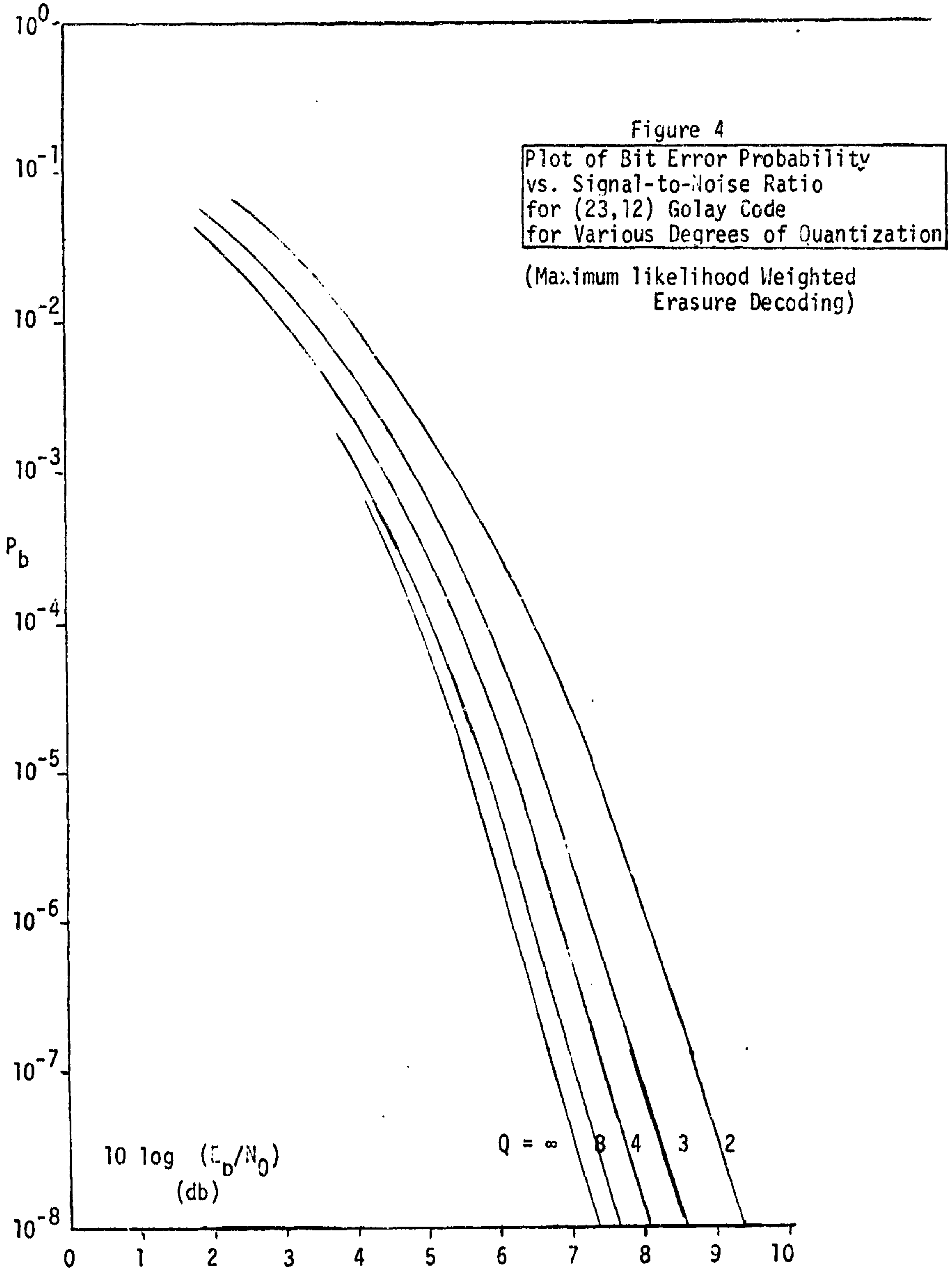

Figure 4

Plot of Bit Error Probability vs. Signal-to-Noise Ratio for (23,12) Golay Code for Various Degrees of Quantization

(Maximum likelihood Weighted Erasure Decoding)

5. Summary and Conclusions

The decoding procedure described in this paper is applicable, in principle, to any binary block code. Both of the two means of implementing this procedure correct all error patterns guaranteed correctable by the minimum distance of the code, as well as some patterns of higher weight. It seems likely, however, that the fractions of these high weight patterns which are correctable with these practically implementable decoding techniques are less than the fraction correctable with maximum-likelihood Weighted Erasure Decoding.

Performance curves for the Golay code decoded with maximum-likelihood Weighted Erasure Decoding have been presented; these show that as expected, substantial improvements over hard-decision decoding are possible. The efficacy of the two practical Weighted Erasure Decoding procedures has yet to be demonstrated, however.

References

1. Wozencraft, J. M., and I. M. Jacobs, *Principles of Communication Engineering*, John Wiley & Sons, Inc., New York (1965).

2. Massey, J. L., *Threshold Decoding*, The M.I.T. Press, Cambridge, Massachusetts (1963).

3. Viterbi, A. J., "Error Bounds for Convolutional Codes and an Asymptotically Optimum Decoding Algorithm," *IEEE Trans.*, *IT-13*, 260-269 (1967).

4. Burton, H. O., and E. J. Weldon, Jr., "Cyclic Product Codes," *IEEE Trans.*, *IT-11*, 433-439 (1965).

5. Mitchell, M. E., et. al., *Coding and Decoding Operations Research*, G.E. Advanced Electronics Final Report on Contract AF 19(604)-6183, Air Force Cambridge Research Labs (1961).

6. Kasami, T., "A Decoding Procedure for Multiple Error-Correcting Cyclic Codes," *IEEE Trans.*, *IT-10*, 134-139 (1964).

7. Lin, S., and E. J. Weldon, Jr., "Further Results on Cyclic Product Codes," *IEEE Trans.*, *IT-16* (1970).

8. Weldon, E. J., Jr., "Difference-Set Cyclic Codes," BSTJ, 45, 1045-1055 (1966).

9. Peterson, W. W., and E. J. Weldon, Jr., *Error-Correcting Codes* Edition 2, M.I.T. Press, in press.

10. Reddy, S. M., "On Decoding Iterated Codes," to appear, *IEEE Trans.*, *IT-16* (1970).

11. Forney, G. D., Jr., "Generalized Minimum Distance Decoding," *IEEE Trans.*, *IT-12*, p. 125 (1966).

12. Fein, A. E., R. M. Heller, C. W. Helstrom, "Analog Coding," Technical Report RADC-TR-65-311, Clearinghouse #AD626388 (1965).

13. Forney, G. D., Jr., "Study of [illegible]ation Coding," Technical Report RADC-TR-67-410, Clearinghouse #AD822160 (1967).

14. Cahn, C. R., "Binary Decoding Extended to Nonbinary Demodulation of Phase Shift Keying," IEEE Trans., COM-17, No. 5 (1969).

Part Four

A Procedure for Decoding Binary Product Codes*

by

E. J. Weldon, Jr.

1. Introduction

Product (iterated) codes, despite their relatively poor random-error-correcting capabilities, have been much studied. For one thing the codes are structurally interesting, and this structure has suggested several effective and easily implemented decoding procedures applicable only to these codes.

These methods are summarized briefly below for a 2-dimensional product code:

1) (Elias[1], Abramson[2]) The row code words are decoded independently; then the column words are decoded. This process can be repeated a number of times until no further corrections are possible.
2) (Lin and Weldon[3], Gore[4]) When the row and column codes are majority logic decodable, the product code is majority logic decodable.
3) (Reddy[5]) If either factor (component) code is majority-logic decodable, then the product code can be decoded using the decoders for the factor codes.

All of these procedures have the highly desirable property that the decoder(s) for the factor codes are used to decode the much longer product code. However, Method 1 fails to correct many error patterns of weight less than or equal to t where

* This research was supported in part by NASA grant NGL-12-001-046 and by AFCRL Contract F19628-70-C-0082.

$$t = \frac{d_1 d_2 - 1}{2} . \qquad (1)$$

the error-correcting capability of the code. Methods 2 and 3 correct all patterns of weight t or less and many of higher weight but are applicable to relatively few product codes.

In this paper we present a decoding procedure for product codes which corrects all error patterns of weight $(d_1 d_2 - 1)/2$ or less (as well as some of higher weight), is applicable to all binary product codes, and uses the factor-code decoders in a simple way to decode the product code. The procedure is similar in concept to Reddy's decoding technique[5] and draws heavily on the results of Reference 6. Because of the limitations of this latter reference, the present result applies only to binary codes.

2. The Decoding Procedure

Consider the product of an (n_1,k_1) row code with minimum Hamming distance d_1 and an (n_2,k_2) column code with distance d_2. Let E_γ denote the number of bit errors in the γ^{th} row. Decoding can be accomplished in 2 steps:

1) Decode the γ^{th} row word; compute and record F_γ, the number of changes made in decoding this row, $\gamma = 1, 2, \ldots, n_2$.
2) Decode the ν^{th} column word using Weighted Erasure Decoding[6] as explained below.

To simplify the presentation we will take d_1 to be odd i.e. $d_1 = 2t_1 + 1$; the column decoder operates on a binary-input, $(d_1 + 2)$-ary output channel. If $F \leq t_1$, the digit in the γ^{th} row and the ν^{th} column, $a_{\gamma\nu}$, will be taken to have value L_F if the binary symbol in this position is a 0 and value L_{d_1+1-F} if the binary symbol is a 1 . If $F > t_1$, the output symbol is L_{t_1+1} regardless of the associated binary digit.

The table below assumes that the all-zero word is transmitted. The γ^{th} row originally contains E_γ errors; the row decoder makes F_γ changes. Of course, if $E_\gamma \leq t_1$, these changes are corrections; if $E_\gamma \leq t_1+1$, correction of all errors may or may not occur.

E_γ	F_γ	Output symbol $a_{\gamma\nu}$		w-weight of error e_γ	
no. of bit errors in row γ	no. of changes made in row γ	Associated Binary digit		Associated Binary digit	
		0	1	0	1
0	0	L_0	-	0	0
1	1	L_1	-	1	1
2	2	L_2	-	2	2
⋮					
t_1	t_1	L_{t_1}	-	t_1	t_1
$\geq t_1 + 1$	$\geq t_1 + 1$	L_{t_1+1}	L_{t_1+1}	$t_1 + \frac{1}{2}$*	$t_1 + \frac{1}{2}$*
$\geq t_1 + 1$	t_1	L_{t_1}	L_{t_1+2}	t_1	$t_1 + 1$
	⋮				
$\geq d_1 - 2$	2	L_2	L_{d_1-1}	2	$d_1 - 2$
$\geq d_1 - 1$	1	L_1	L_{d_1}	1	$d_1 - 1$
$\geq d_1$	0	L_0	L_{d_1+1}	0	d_1

* In Reference 6 the e_γ are restricted to be integers. This is not strictly necessary but multiplying the e_γ here by a factor of 2 gives integral weights and leaves the proof unchanged.

It now remains to show that the column decoder decodes correctly provided that t or fewer errors occurred in the product code worা. To prove that this is so, assume that the all-zero code word is transmitted and consider the decoding of a particular column, the ν^{th}.

The worst case occurs when the row decoder corrects no errors. Let e_γ denote the w-weight of the erro: in the γ^{th} digit. Then either

1) The γ^{th} row contained no errors, hence no changes were made by the row decoder and $e_\gamma = 0$, or

2) The γ^{th} row contained E_γ errors where

$$E_\gamma \geq t_1 + 1$$

In this latter case,

$$e_\gamma \leq E_\gamma \tag{2}$$

Now since t or fewer bit errors occurred in the product code word

$$\sum_{\gamma=1}^{n_2} E_\gamma \leq t \tag{3}$$

Therefore, from Eq. 2,

$$\sum_{\gamma=1}^{n_2} e_\gamma \leq t \tag{4}$$

But by Theorem 1 of Reference 6, this is precisely the necessary condition for correctly decoding the ν^{th} column. Therefore all error patterns of Hamming weight $\leq [(d_1 d_2 - 1)/2]$ are correctable.

Example. Consider the product of two binary codes with minimum Hamming distance 3. The product code has distance 9 and so can correct any error pattern of weight ≤ 4 -- including a pattern of 4 errors which form a rectangle in the usual 2-dimensional representation of the product code word. Again assume the all-zero word is sent.

After Step 1 of decoding, all rows except the γ_1th and γ_2th have $e_\gamma = 0$, $F_\gamma = 0$ and contain no errors. The other two rows have $e_\gamma = 2$, $F_\gamma = 1$ (the row decoder introduces an error) and contain 3 binary errors each after the first step.

In Step 2 of decoding, for all columns except ν_1, ν_2 and ν_3, the γ_1th and γ_2th bits are 0 with $F = 1$ and all other bits are 0 with $F = 0$. Thus for these columns,

$$\sum_{\gamma=1}^{n_2} e_\gamma = 2 \leq t$$

and correct column decoding results. For the ν_1th, ν_2th and ν_3th columns, the γ_1th and γ_2th bits are 1 with $F = 1$, while all other bits are 0 with $F = 0$. Hence

$$\sum_{\gamma=1}^{n_2} e_\gamma = 4$$

and correct decoding results.

In conclusion, it should be remarked that since only the F_γ must be stored after each row decoding, and since $F_\gamma \leq t_1+1$, the storage requirements beyond storing the array itself are minimal. Also since the complexity of Weighted Erasure Decoding increases with the number of output symbols, it makes sense to treat the code with the smaller minimum distance as the row code.

REFERENCES

1. Elias, P., "Error Free Coding," IRE Trans., PGIT-4, pp. 29-37, 1954.

2. Abramson, N., "Cascade Decoding of Cyclic Product Codes," IEEE Trans., COM-16, pp. 398-402, 1968.

3. Lin, S., and E. J. Weldon, Jr., "Further Results on Cyclic Product Codes," IEEE Trans., IT-16, 1970.

4. Gore, W., "Further Results on Product Codes," submitted to IEEE Trans., IT-16, 1970.

5. Reddy, S. M., "On Decoding Iterated Codes," IEEE Trans., IT-16, 1970.

6. Weldon, E. J., "Encoding and Decoding for Binary-Input Q-ary Output Channels," submitted to IEEE Trans., IT-17, 1971.

Part Five

A Remark on the Minimum Weight Code Words of a Certain Class of Cyclic Codes

by

T. Kasami

Very little is known on the weight structure of subcodes of the 3rd or high order Reed-Muller code (or supercodes of the (m-4)th or lower order Reed-Muller code). The following theorem on the minimum weight code-words is a strengthened version of Theorem 11 in (Kasami-Lin-Peterson, 1968). Let p be a prime. $W_{p^s}(i)$ denote the sum of the coefficients of the radix-p^s form of i.

<u>Theorem</u>: Let C be a p-ary cyclic code of length $p^{ms}-1$ with generator polynomial g(X), let β be a primitive element of GF(p^{ms}), and let $1 \leq c < m$. If $g(\beta^i) = 0$ for every i such that

$$0 < i < 2(p^{(m-c)s}-1) ,$$

$$W_{p^s}(i) < (m-c)(p^s-1) ,$$

then any code-word of minimum weight $p^{(m-c)s}-1$ is a scalar multiple of the incidence vector* of an (m-c)-flat through the origin in EG(m,p^s).

This theorem is proved by showing that the reciprocal of the locator polynomial of a code-word of weight $p^{(m-c)s}-1$ is an affine polynomial. For the detail, refer to the proof of Theorem 11 in (Kasami-Lin-Peterson, 1968). If C in Theorem is a proper supercode

* The component corresponding to the origin is deleted.

of the code spanned by the dual of the (m-c-1)-th order Euclidean Geometry code over EG(m,p^s) and the all one vector, then a vector v is a minimum weight code-word if and only if v is a nonzero scalar multiple of the incident vector of an (m-c)-flat through the origin in EG(m,p^s). The minimum weight code-words do not span code C.

References

1. Kasami, T., Lin, S. and Peterson, W. W. (1968), "New Generalizations of the Reed-Muller Codes-Part I: Primitive Codes," IEEE Transactions on Information Theory, Vol. IT-14, No. 2, 189-198.

Part Six

An Upper Bound on the Minimum Distance of Dual Codes of Primitive Polynomial Codes

by

T. Kasami and S. Lin

1. Introduction

In this part of the report, an upper bound on the minimum distance of dual codes of primitive polynomial codes [1] is derived. For several cases, this upper bound is tight and is equal to the BCH lower bound for the same class of codes [2,3]. This upper bound can be applied to establish the exact minimum distance of a subclass of binary primitive BCH codes.

2. A Brief Review of Polynomial Codes

Let $GF(q^{ms})$ be the extension field of $GF(q^s)$ where q is a power of a prime p. Let α be a primitive element of $GF(q^{ms})$. Then, any nonzero element α^j in $GF(q^{ms})$ can be expressed as

$$\alpha^j = a_{1j} + a_{2j}\alpha^1 + a_{3j}\alpha^2 + \dots + a_{mj}\alpha^{m-1} \qquad (1)$$

for $0 \leq j < q^{ms}-1$, where a_{ij} is in $GF(q^s)$. There is one-to-one correspondence between α^j and the m-tuple $\overline{A} = (a_{1j}, a_{2j}, \dots, a_{mj})$. We call $\overline{A} = (a_{1j}, a_{2j}, \dots, a_{mj})$ the coordinate vector of α^j.

Let $\overline{X} = (X_1, X_2, \dots, X_m)$ where X_i is a variable over $GF(q^s)$. Define $Q_m(\mu)$ as a set of the following polynomials of m variables:

$$f(\overline{X}) = \sum C_{\nu_1\nu_2\dots\nu_m} X_1^{\nu_1} X_2^{\nu_2} \dots X_m^{\nu_m} \qquad (2)$$

such that

(1) $C_{\nu_1\nu_2\cdots\nu_m} \varepsilon \mathrm{GF}(q^s)$,

(2) $0 \le \nu_i < q^s$ for $1 \le i \le m$,

(3) $\sum_{i=1}^{m} \nu_i \le \mu$

(4) $f(a_{1j}, a_{2j}, \ldots , a_{mj}) \varepsilon \mathrm{GF}(q)$ for $0 \le j < q^{ms} - 1$,

where $(a_{1j}, a_{2j}, \ldots , a_{mj})$ is the coordinate vector of α^j.

For each polynomial $f(\overline{X})$ in $Q_m(\mu)$, a vector $\nu(f)$ is defined as follows:

$$\nu(f) = (\nu_0, \nu_1, \nu_2, \ldots , \nu_{q^{ms}-2}) \tag{3}$$

where the j^th component

$$\nu_j = f(a_{1j}, {}_{2j}, \ldots , a_{mj}) \tag{4}$$

for $0 \le j \le q^{ms}-2$. Thus, $\nu(f)$ is a vector over GF(q).

<u>Definition</u>[1] A μ-th order q-ary polynomial code of length $q^{ms}-1$ is defined as the following set of vectors:

$$C_m(\mu) = \{\nu(f) \mid f(\overline{X}) \varepsilon Q_m(\mu)\} \quad . \tag{5}$$

Let Q_0 and R_0 be the quotient and remainder resulting from dividing $(\mu+1)$ by (q^s-1), i.e.,

$$\mu+1 = Q_0(q^s-1) + R_0 \tag{6}$$

with $0 \leq R_0 < q^s-1$. Let j be the largest integer such that

$$q^j \leqq q^s - R_0 \tag{7}$$

Dividing q^s-R_0 by q^j, we obtain

$$q^s - R_0 = \sigma_j q^j + r_j \tag{8}$$

where $1 < \sigma_j < q$ and $0 \leq r_j < q^j$. Define the following two integers,

$$\begin{aligned} A &= R_0 - 1 + \sigma_j q^j \\ B &= q^s - \sigma_j q^j \ . \end{aligned} \tag{9}$$

Let A_0 and B_0 be two non-negative integers less than or equal to q^s-1 which are defined as follows:

$$\begin{cases} A_0 \equiv A q^{s-j} \pmod{q^s-1} & \text{for } A \neq q^s-1 \\ A_0 \equiv A & \text{for } A = q^s-1 \ , \end{cases}$$

$$\begin{cases} B_0 \equiv B q^{s-j} \pmod{q^s-1} & \text{for } B \neq q^s-1 \\ B_0 \equiv B & \text{for } B = q^s-1 \\ B_0 \equiv Bq \pmod{q^s-1} & \text{for } j = 0 \ . \end{cases} \tag{10}$$

Now, we construct h_0 as follows:

$$\begin{aligned} h_0 &= (q^s-1) + (q^s-1)q^s + \ldots + (q^s-1)q^{(Q_0-2)s} \\ &\quad + A_0 q^{(Q_0-1)s} + B_0 q^{Q_0 s} \\ &= B_0 q^{Q_0 s} + (A_0+1)q^{(Q_0-1)s} - 1 \ . \end{aligned} \tag{11}$$

Let $D_m(\mu)$ be the q-ary dual code of the μ-th order polynomial code $C_m(\mu)$. It has been shown in Ref. 2 and 3 that the code $D_m(\mu)$ has minimum distance d_{min} at least equal to

$$h_0 + 1 = B_0 q^{Q_0 s} + (A_0 + 1) q^{(Q_0 - 1)s} \tag{12}$$

i.e.

$$d_{min} \geqq h_0 + 1 .$$

3. An Upper Bound on the Minimum Distance of $D_m(\mu)$

Consider $x_1^{\nu_1} x_2^{\nu_2} \ldots x_m^{\nu_m}$ with $0 \leqq \nu_i \leqq q^s - 1$ for $1 \leqq i \leqq m$. It has been proved that

$$\sum_{\substack{x_i \varepsilon GF(q^s) \\ 1 \leqq i \leqq m}} x_1^{\nu_1} x_2^{\nu_2} \ldots x_m^{\nu_m} = 0 \tag{13}$$

unless $\nu_1 = \nu_2 = \ldots = \nu_m = q^s - 1$ [1] .

Now, consider the μ-th order primitive q-ary polynomial code $C_m(\mu)$ with

$$\mu = Q_0(q^s - 1) + R_0 - 1 \tag{14}$$

where $0 \leqq R_0 < q^s - 1$. Define the following polynomial:

$$p(\bar{X}) = \prod_{i=1}^{m-Q_0-1} (X_i^{q^s-1} - 1) \{ X_{m-Q_0} \prod_{j=1}^{q^s-R_0-2} (X_{m-Q_0+1} - w_j) \} \tag{15}$$

where $w_j \varepsilon GF(q^s)$. The degree of $p(X)$ is

$$(m - Q_0 - 1)(q^s - 1) + q^s - R_0 - 1 \tag{16}$$

It follows from Eq. (13) that the vector $\nu(p)$ defined in accordance with Eq. (3) and Eq. (4) is orthogonal to every vector u in the polynomial code $C_m(\mu)$, i.e., $u\cdot\nu(p) = 0$. Let Tr stand for trace. It is clear that

$$\mathrm{Tr}[u\cdot\nu(p)] = 0 \ .$$

Since u is a vector over GF(q), thus

$$\begin{aligned}\mathrm{Tr}[u\cdot\nu(p)] &= u\cdot\mathrm{Tr}[\nu(p)]\\ &= u\cdot\nu[\mathrm{Tr}\ p(\bar{x})]\\ &= 0 \ .\end{aligned}$$

Since the vector $\nu[\mathrm{Tr}\ p(\bar{x})]$ is over GF(q), therefore it is in the dual code $D_m(\mu)$ of the polynomial code $C_m(\mu)$. The weight of $\nu[\mathrm{Tr}\ p(\bar{x})]$ is

$$\lambda = (R_0 + 2)q^{Q_0 s-1} \ .$$

It is clear that λ is an upper bound on the minimum distance of $D_m(\mu)$.

Theorem 1: The minimum distance d_{min} of the dual code $D_m(\mu)$ of a primitive polynomial code $C_m(\mu)$ is upper bounded by

$$\lambda = (R_0 + 2)q^{Q_0 s-1} \ . \tag{17}$$

where Q_0 and R_0 are quotient and remainder resulting from dividing $\mu + 1$ by $(q^s - 1)$.

For several binary cases, this upper bound is tight and is equal to the lower bound of Eq. (12), i.e.

$$\lambda = h_0 + 1 \ .$$

Case 1: For q=2 and $R_0=2^s-2$, we have

$$\mu = Q_0(2^s-1) + 2^s-3 \ .$$

By (17), the minimum distance d_{min} of binary code $D_m(\mu)$ is upper bounded by

$$\begin{aligned}\lambda &= (2^s)2^{Q_0 s - 1} \\ &= 2^{(Q_0+1)s - 1} \qquad (18)\end{aligned}$$

It follows from (7), (8), (9) and (10) we obtain

$$\begin{aligned}A_0 &= 2^s - 1 \\ B_0 &= 2^{s-1} - 1 \qquad (19)\end{aligned}$$

Thus, by (11), the minimum distance of $D_m(\mu)$ is lower bounded by

$$h_0 + 1 = 2^{(Q_0+1)s - 1} \qquad (20)$$

From (18) and (20), we notice that the upper bound and lower bound are equal. Therefore, we conclude that for $\mu = Q_0(2^s-1) + 2^s-3$ the minimum distance d_{min} of $D_m(\mu)$ is exactly equal to

$$d_{min} = 2^{(Q_0+1)s - 1} . \qquad (21)$$

Case 2: For $q=2$ and $R_0=2^s-3$, we have

$$\mu = Q_0(2^s-1) + 2^s-4 .$$

By (17), the minimum distance d_{min} of $D_m(\mu)$ is upper bounded by

$$\lambda = (2^s-1)2^{Q_0 s - 1} . \qquad (22)$$

By (7), (8), (9) and (10), we obtain

$$A_0 = 2^{s-1} - 1$$

$$B_0 = 2^{s-1} - 1 .$$

Then, it follows from (11) that

$$h_0+1 = (2^s-1)2^{Q_0 s - 1} . \qquad (23)$$

From (22) and (23), we notice that the upper bound and the lower bound are equal. Thus, the code $D_m(\mu)$ with $\mu = Q_0(2^s-1) + 2^s-4$ has minimum distance exactly

$$d_{min} = (2^s-1)2^{Q_0 s - 1} .$$

4. The Exact Minimum Distance of a Class of Primitive BCH Code.

Let α be a primitive element in $GF(2^{ms})$. It is known that the code $D_m(\mu)$ is a subcode of the (h_0+1) - BCH code C_0 whose generator polynomial has

$$\alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^{h_0-1}$$

as roots [1,4]. From the conclusion which we obtain in Case 2, we have the following theorem.

Theorem 2: For $d_0 = (2^s-1)2^{\ell s-1}$ for $1 \leq \ell < m-1$, the d_0 - BCH code of length $2^{ms} - 1$ whose generator polynomial has

$$\alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^{d_0-1}$$

as roots has minimum distance exactly equal to

$$(2^s-1)2^{\ell s-1} .$$

Due to the symmetry property of primitive BCH codes [5], a direct consequence of Theorem 2 is the following corollary.

Corollary 2: For $d = (2^s-1)2^{\ell s-1} - 1$ with $1 \leq \ell < m-1$, the d-BCH code of length $2^{ms} - 1$ whose generator polynomial has

$$\alpha^1, \alpha^2, \ldots, \alpha^{d-1}$$

as roots has minimum distance exactly equal to

$$(2^s-1)2^{\ell s-1} - 1 . \qquad (24)$$

Corollary 2 gives us some new information about the exact minimum distance of a subclass of primitive BCH codes.

REFERENCES

1. Kasami, T., S. Lin and W. W. Peterson, "Polynomial Codes," IEEE Trans., Vol. IT-14, pp. 807-814, November, 1968.

2. Chen, C. L., and S. Lin, "Further Results on Polynomial Codes," Information and Control, Vol. 15, No. 1, pp. 38-60, July, 1969.

3. Gore, W. C. and A. B. Cooper, "A Recent Result Concerning the Dual of Polynomial Codes", IEEE Trans., Vol. IT-16, pp. 638-639, Sept. 1970.

4. Lin, S., "On a Class of Cyclic Codes", Chapter 7, Error-Correcting Codes, H. Mann, Ed., John Wiley, New York, 1968.

5. Peterson, W. W., "On the Weight Structure and Symmetry of BCH Codes", J. Inst. Elect. Commun. Eng. Japan, 50, 1183-1190, 1967.

Part Seven

On Shortened Reed-Muller Codes

by

C L. Chen and S. Lin

1. Introduction

The Reed-Muller (RM) codes[1,2] not only provided the first example of a class of multiple-error-correcting codes, they also have the important feature of being majority decodable. However, the code length and the code dimension of these codes are rather sparsely distributed. Very often this hinders the adaption of these codes in practical application.

Weiss has found a way to overcome this situation by puncturing some digits from the RM codes.[3,4] The code length of the punctured codes is greater than while the minimum distance of the punctured codes is less than the original RM codes. Furthermore, the punctured RM codes also have the important property of being majority logic decodable.

Another way to increase the number of codes from the RM codes is to shorten the RM codes. In this part we shall introduce a way of shortening the RM codes. The shortened RM codes have the same minimum distance as the original codes. They also preserve the feature of being majority logic decodable.

2. The RM Codes and the Punctured RM Codes

Let $n = 2^m$ and v_0 be a vector of all 1's n-tuple. In addition, arrange the m n-tuples $v_1, v_2, \ldots, v_m$, in rows so that the n columns formed by them are the all possible 2^m m-tuples. Finally, define the vector product of two n-tuples as follows:

$$u = (a_1, a_2, \ldots, a_n)$$

$$v = (b_1, b_2, \ldots, b_n)$$

$$u \cdot v = (a_1 b_1, a_2 b_2, \ldots, a_n b_n)$$

Then the r-th order Reed-Muller code is formed by using as a basis $v_0, v_1, \ldots, v_m$, and all vector products of these vectors r or fewer at a time. That is, the generator matrix of the code is of the form

$$G_r = \begin{bmatrix} v_0 \\ v_1 \\ \cdot \\ \cdot \\ \cdot \\ v_m \\ v_1 v_2 \\ \cdot \\ \cdot \\ \cdot \\ v_{m-1} v_m \\ v_1 v_2 v_3 \\ \cdot \\ \cdot \\ \cdot \\ v_{m-r+1} v_{m-r+2} \cdots v_m \end{bmatrix} \qquad (1)$$

It can be shown that the code has the following specifications:

$$\text{code length} = n = 2^m$$

$$\text{Dimension} = K = 1 + \binom{m}{1} + \binom{m}{2} + \ldots + \binom{m}{r}$$

$$= \sum_{i=0}^{r} \binom{m}{i}$$

$$\text{minimum distance} = d = 2^{m-r}$$

The punctured RM codes, or the Weiss codes, are obtained from the RM codes by puncturing some digits of the code words. Let us consider the matrix G_r of Eq. (1) and its submatrix G

$$G = \begin{bmatrix} v_1 \\ v_2 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ v_m \end{bmatrix} \tag{2}$$

The punctured code is obtained by the deletion of those columns of G_r which have p+1 or more 1's in the submatrix G, where p is an integer greater than r and less than or equal to m.

It can be shown that the punctured code thus obtained has the following specifications:[3]

$$\text{code length} = n_p = 1 + \binom{m}{1} + \binom{m}{2} + \ldots + \binom{m}{p}$$

$$= \sum_{i=0}^{p} \binom{m}{i} \qquad\qquad p \leqq m$$

$$\text{dimension} = K_p = 1 + \binom{m}{1} + \ldots + \binom{m}{r}$$

$$= \sum_{i=0}^{r} \binom{m}{i} \qquad\qquad 0 < r < p$$

$$\text{minimum distance} = d_p = \sum_{i=0}^{p-r} \binom{m-r}{i}$$

In the following, we shall briefly describe the decoding procedures for both the RM codes and the punctured codes.

Let $a_{i_1 i_2 \dots i_j}$ be the information digit corresponding to the vector $v_{i_1} v_{i_2} \dots v_{i_j}$ in the matrix G_r. Then a code word of the r-th order RM code is of the form

$$
\begin{aligned}
b &= (b_1, b_2, \dots, b_n) \\
&= a_0 v_0 + \Sigma a_{i_1 i_2} v_{i_1} v_{i_2} + \Sigma a_{i_1 i_2 i_3} v_{i_1} v_{i_2} v_{i_3} + \dots \\
&\qquad + \Sigma a_{i_1 i_2 \dots i_r} v_{i_1} v_{i_2} \dots v_{i_r} \qquad (3)
\end{aligned}
$$

where i_j's are taken from 1 to m and $i_j \neq i_k$ in each of the summation terms.

The decoding of the RM codes was described in Ref. [2,5]. It can be shown in general that, for the generator matrix of the r-th order code, the columns can be grouped into 2^{m-r} disjoint sets of 2^r each, such that the sum of the columns in each set has a "1" only in the position corresponding to the row vector $v_{i_1} v_{i_2} \dots v_{i_r}$. Thus, there are 2^{m-r} independent determinations that can be formed to solve $a_{i_1 i_2 \dots i_r}$. Since each error digit can affect only one determination, $a_{i_1 i_2 \dots i_r}$ can be determined correctly by a majority decision if $2^{m-r-1} - 1$ or fewer errors occurred. All of the $\binom{m}{r}$ information digits of the form $a_{i_1 i_2 \dots i_r}$ can be determined by this way.

After the $\binom{m}{r}$ information digits of the form $a_{i_1 \dots i_r}$ have been determined, the summation $\Sigma\, a_{i_1 i_2 \ldots i_r} v_{i_1} v_{i_2} \ldots v_{i_r}$ can be subtracted from the received vector. Then the modified received vector can be treated as if it were coded from an (r-1)-th order code and each of the $\binom{m}{r-1}$ information digits of the form $a_{i_1 \ldots i_{r-1}}$ can be determined from a majority decision on a set of 2^{m-r+1} independent determinations. Then the procedure continues until the modified received vector is treated as if it were coded from a 0-th order code and a_0 is determined.

The procedure for decoding the punctured RM codes is similar to that for decoding the RM codes. To determine $a_{i_1 i_2 \ldots i_r}$, there are d_p independent determinations that can be formed. After all of the $\binom{m}{r}$ information digits of the form $a_{i_1 i_2 \ldots i_r}$ have been determined by a majority decision, the summation term $\Sigma\, a_{i_1 i_2 \ldots i_r} v_{i_1} v_{i_2} \ldots v_{i_r}$ is subtracted from the received vector. The modified received vector can be treated as if it were coded from a punctured (r-1)-th order RM code. Then the decoding procedure continues in a similar way as in the RM codes until a_0 is determined.

3. The Shortened RM Codes

Consider the submatrix G_s of G_r formed from $v_0, v_1, v_2, \ldots, v_p$ and their vector products taken r or fewer at a time, where $p < m$. That is,

$$G_s = \begin{bmatrix} v_0 \\ v_1 \\ \vdots \\ v_p \\ v_1v_2 \\ \vdots \\ v_{p-1}v_p \\ v_1v_2v_3 \\ \vdots \\ v_{p-r+1}\cdots v_p \end{bmatrix} \qquad p < m \tag{4}$$

Ne^t, consider the columns in G of (2) that all have 0's in the last m-p rows. It is clear that these columns form an additive group. Furthermore, consider the corresponding columns in the matrix G_r. All of the rows except those rows in G_s have 0's in these columns Therefore, if we delete from G_r the submatrix G_s and the columns that all have 0's in the last m-p columns of G, the minimum distance of the shortened code will remain the same. Thus, the shortened r-th order RM code as constructed above has the following parameters:

dimension $k_s = k - (1 + \binom{p}{1} + \binom{p}{2} + \ldots + \binom{p}{r})$

$$= \sum_{i=0}^{r} [\binom{m}{i} - \binom{p}{i}]$$

code length $n_s = n - 2^p$

$$= 2^m - 2^p$$

minimum distance $d_s = d = 2^{m-r}$

where $p < m$, and the convention that $\binom{x}{y} = 0$ for $y > x$ is used.

Notice that the number of parity check digits of the RM code is equal to n-k, and that of the shortened code is equal to $n-k-(2^p - \sum_{i-0}^{r} \binom{p}{i})$. Therefore, the number of parity check digits of the shortened codes is reduced by $\sum_{i=r+1}^{p} \binom{p}{i}$ while the minimum distance remains the same.

Recall that there are 2^{m-r} independent determinations that can be formed to solve $a_{i_1 i_2 \ldots i_r}$ in a code word of the r-th order RM code. If we delete the submatrix G_s from the matrix G, the columns of G can still be grouped into 2^{m-r} disjoint sets of 2^r each, such that the sum of the columns in each set has a "1" only in the row corresponding to nonzero $v_{i_1} v_{i_2} \ldots v_{i_r}$. From the way we shortened the RM codes, it can be seen that the nonzero vector $v_{i_1} v_{i_2} \ldots v_{i_r}$ has zero's at those positions corresponding to the columns we deleted from G_r. Therefore, the columns of the generator matrix of the shortened code can also be grouped into 2^{m-r} disjoint sets such that the sum of the columns in each set has a "1" only in the row corresponding to $v_{i_1} v_{i_2} \ldots v_{i_r}$. Thus, $a_{i_1 i_2 \ldots i_r}$ can be determined by a majority decision on a set of 2^{m-r} independent determinations. After all the $C_r^m - C_r^p$ information digits of the form $a_{i_1 \ldots i_r}$ have been determined, the sum $\Sigma\, v_{i_1} v_{i_2} \ldots v_{i_r} a_{i_1 i_2 \ldots i_r}$ is subtracted from the received vector. Then the modified received vector is treated as if it were coded from a shortened (r-1)-th order code. By a similar argument, all the $C^m_{r-1} - C^p_{r-1}$ information digits of the form $a_{i_1 i_2 \dots i_{r-1}}$ can be determined by majority decisions. Then the decoding procedures continue until a_{p+1} is determined. Thus, the shortened RM codes are majority logic decodable.

REFERENCES

1. Muller, D. E., "Application of Boolean Algebra to Switching Circuit Design and to Error Detection," IRE Trans., Vol. EC-3, pp. 6-12, 1954.

2. Reed, I. S., "A Class of Multiple-Error-Correcting Codes and the Decoding Schemes," IRE Trans., Vol. IT-4, pp. 38-49, 1954.

3. Weiss, E., "Generalized Reed-Muller Codes," Information and Control, Vol. 5, pp. 213-222, September, 1962.

4. Solomon, G., Algebraic Coding Theory, Chapter 6 in A.V. Balakrishnan, Communication Theory, McGraw-Hill Company, New York, N. Y., 1968.

5. Peterson, W. W., Error-Correcting-Codes, The MIT Press, Cambridge, Mass., and John Wiley and Sons, Inc., New York, N. Y., 1961.

APPENDIX A

SCIENTIFIC REPORT NO. 1 AFCRL-70-0325
ON MAJORITY-LOGIC DECODING FOR THE DUAL OF PRIMITIVE POLYNOMIAL CODES - TADAO KASAMI, SHU LIN - MAY 20, 1970

The class of polynomial codes introduced by Kasami et al. has considerable inherent algebraic and geometric structure. It has been shown that this class of codes and their dual codes contain many important classes of cyclic codes as subclasses, such as BCH codes, Reed-Solomon codes, generalized Reed-Muller codes, projective geometry codes and Euclidean geometry codes.

The purpose of this paper is to investigate further properties of polynomial codes and their duals. First, majority-logic decoding for the duals of certain primitive polynomial codes is considered. Two methods of forming non-orthogonal parity-check sums are presented. Second, the maximality of Euclidean geometry codes is proved. The roots of the generator polynomial of an Euclidean geometry code are specified.

SCIENTIFIC REPORT NO. 2 AFCRL-70-0430
ON THE CONSTRUCTION OF A CLASS OF MAJORITY-LOGIC DECODABLE CODES - TADAO KASAMI, SHU LIN - JUNE 15, 1970

The attractiveness of majority-logic decoding is its simple implementation. Several classes of majority-logic decodable block codes have been discovered for the past two decades. In this paper, a method of constructing a new class of majority-logic decodable block codes is presented. Each code in this class is formed by combining majority-logic decodable codes of shorter lengths. A procedure for orthogonalizing codes of this class is formulated. For each code, a lower bound on the number of correctable errors with majority-logic decoding is obtained. An upper bound on the number of orthogonalization steps for decoding each code is derived. Some majority-logic decodable codes which have more information digits than the Reed-Muller codes of the same length and the same minimum distance are found.

Some results presented in this paper are extensions of the results of Lin and Weldon and Gore on the majority-logic decoding of direct product codes.

APPENDIX B

Papers for Publication on Work Supported by Project F19628-70-C-0082

T. Kasami and S. Lin, "On Majority-Logic Decodin; for the Duals of Polynomial Codes", To appear, IEEE Trans. on Information Theory, IT-17, 1971.

T. Kasami and S. Lin, "On the Construction of a Class of Majority-Logic Decodable Codes," Submitted to IEEE Trans. on Information Theory.

Unclassified

DOCUMENT CONTROL DATA - R & D

Department of Electrical ENgineering
University of Hawaii
~~Honolulu, Hawaii~~ 96822

Unclassified

A STUDY FO PROBLEMS IN INFORMATIO:I PROCESSING

Scientific, Final, 1 November 1969 - 31 October 1970(appvd. Dec. 1970)

Tadao Kasami
Shu Lin

November 20, 1970	57	36

F19628-70-C-0082

5632-05-01

61102F

681305

AFCRL-70-0655

1-This document has been approved for public release and sale; its distribution is unlimited.

TECH, OTHER

Air Force Cambridge Research
Laboratories (LR)
~~L. G. Hanscom Field~~
Bedford, Massachusetts 01730

This final report summarizes research for a one-year project. Abstracts for the two scientific reports are given, and some new results are included on reduction of context-free grammars, decoding binary block codes on Q-ary output channels, a procedure for decoding binary product codes, on the minimum weight code words of a certain class of cyclic codes, distance property of the dual codes of polynomial codes and on shortened Reed-Muller codes.

Unclassified