REPORT R-477 JUNE, 1970 UILU-ENG 70-222

COORDINATED SCIENCE LABORATORY

L-STEP MAJORITY LOGIC DECODING

ROBERT T. CHIEN
SPENCER W. NG

UNIVERSITY OF ILLINOIS - URBANA, ILLINOIS

UILU-ENG 70-222

L-STEP MAJORITY LOGIC DECODING

Robert T. Chien
Spencer W. Ng

This work was supported in part by the Joint Services Electronics Program (U.S. Army, U.S. Navy, & U.S. Air Force) under Contract DAAB 07-67-C-0199; and in part by the Rome Air Development Center under Contract No. F30602-70-C-0014 (EMKC).

Other CSL Reports in Information Science include:

☐ 1. Lum, Vincent, "A Theorem on the Minimum Distance of BCH Codes over GF(q)," March, 1966, R-281.

☐ 2. Preparata, Franco P., "Convolutional Transformations of Binary Sequences: Boolean Functions and Their Resynchronizing Properties," March, 1966, R-283.

☐ 3. Kasami, Tadao, "A Note on Computing Time for Recognition of Languages Generated by Linear Grammars," April, 1966, R-287.

☐ 4. Lum, Vincent, "On Bose-Chaudhuri-Hocquenghem Codes over GF(q)," July, 1966, R-306.

☐ 5. Bahl, Lalit Rai, "Matrix Switches and Error Correcting Codes from Block Designs," August, 1966, Thesis, R-314.

☐ 6. Kasami, Tadao, "Weight Distributions of Bose-Chaudhuri-Hocquenghem Codes," August, 1966, Thesis, R-317.

☐ 7. Preparata, F. P., Metze, G. and Chien, R. T., "On the Connection Assignment Problem of Diagnosable Systems," October, 1966, R-322.

☐ 8. Chien, R. T. and Preparata, F. P., "Topological Structures of Information Retrieval Systems," October, 1966, R-325.

☐ 9. Heller, James Ernest, "Decoding Procedures for Convolutional Codes," November, 1966, R-327.

☐ 10. Lum, Vincent and Chien, R. T., "On the Minimum Distance of Bose-Chaudhuri-Hocquenghem Codes," November, 1966, R-328.

☐ 11. Hsu, Hsung Tsao, "Error Correcting Codes for Compound Channels," December, 1966, R-331.

☐ 12. Hong, SeJune, "On Minimum Distance of Multiple Error Correcting Arithmetic Codes," January, 1967, R-336.

☐ 13. Gaddess, Terry G., "A Study of an Error Detecting Parallel Adder," January, 1967, M.S. Thesis, R-337.

☐ 14. Preparata, Franco P., "Binary Sequence Convolutional Mapping: The Channel Capacity of a Non-Feedback Decoding Scheme, March, 1967, R-345.

☐ 15. Preparata, F. P. and Chien, R. T., "On Clustering Techniques of Citation Graphs," May, 1967, R-349.

16. Lipovski, Gerald J., "Compatibility and Row-Column Minimization of Sequential Machines," May, 1967, R-355.

17. Lipovski, Gerald J., "An Improved Method of Finding all Largest Combinable Classes," August, 1967, R-362.

18. Tracey, Robert J., "Lattice Coding for Continuous Channels," December, 1967, R-371.

19. Preparata, Franco P., "A Study of Nordstrom-Robinson Optimum Code," April, 1968, R-375.

20. Preparata, Franco P., "A Class of Optimum Non-linear Double-Error-Correcting Codes," July, 1968, R-389.

21. Beach, Edward J., "A Study of a Feedback Time-Sharing System," September, 1968, R-391.

22. Weston, P. and Taylor, S. M., "Cylinders: A Data Structure Concept Based on Rings," September, 1968, R-393.

23. Bahl, Lalit Rai, "Correction of Single and Multiple Bursts of Error," October, 1968, R-397.

24. Carroll, D. E., Chien, R. T., Kelley, K. C., Preparata, F. P., Reynolds, P., Ray, S. R., and Stahl, F. A., "An Interactive Document Retrieval System," December, 1968, R-398.

25. Biss, Kenneth, "Syntactic Analysis for the R2 System," December, 1968, R-399.

26. Tzeng, Kenneth Kai Ming, "On Iterative Decoding of BCH Codes and Decoding Beyond the BCH Bound," January, 1969, R-404.

27. Kelley, K. C., Ray, S. R. and Stahl, F. A., "ISL - A String Manipulating Language," February, 1969, R-407.

28. Lombardi, Daniel Joseph, "Context Modeling in a Cognitive Memory," February, 1969, R-408.

29. Hong, SeJune, "On Bounds and Implementation of Arithmetic Codes," October, 1969, R-437.

30. Chien, R. T. and Hong, S. J., "Error Correction in High Speed Arithmetic," October, 1969, R-438.

31. Chien, R. T. and Hong, S. J., "On a Root-Distance Relation for Arithmetic Codes," October, 1969, R-440.

- [ ] 32. Chien, R. T., "Recent Developments in Algebraic Decoding," November, 1969, R-441.

- [ ] 33. Chien, R. T. and Hong, S. J., "An Iterative Approach for the Correction of Iterative Errors," November, 1969, R-443.

- [ ] 34. Jansen, Jr., James Merritt, "Phrase Dictionary Construction Methods for the R2 Information Retrieval Systems," December, 1969, R-447.

- [ ] 35. Chien, R. T., Ray, S. R., and Stahl, F., "ISL - A New Programming Language for Information Retrieval," December, 1969, R-449.

- [ ] 36. Cordaro, Jr., J. T. and Chien, R. T., "Design Considerations of On-Line Document Retrieval Systems," February, 1970, R-456.

- [ ] 37. Hartmann, Carlos R. P., "On the Minimum Distance Structure of Cyclic Codes and Decoding Beyond the BCH Bound," February, 1970, R-458.

- [ ] 38. Bell, Frank Ellwood III, "On the Equivalence of Free Distance and Column Distance of a Convolutional Code," April, 1970, R-462.

- [ ] 39. Chow, James Cheh-Min, "Pattern Classification with a Partitioned Training Set," April, 1970, R-463.

- [ ] 40. Esser, Nicholas Matthew, Jr., "A Relational Structure for Document Retrieval in Coding Theory," May, 1970, R-469.

For copies of these reports please complete this form and send to

Professor R. T. Chien
Coordinated Science Laboratory
University of Illinois
Urbana, Illinois 61801

My name and address is ______________________________

____

____

____

L-STEP MAJORITY LOGIC DECODING*

Robert T. Chien
Spencer W. Ng

Coordinated Science Laboratory
University of Illinois
Urbana, Illinois

*This work was supported by the Rome Air Development Center under Contract No. F30602-70-C-0014 (EMKC).

TABLE OF CONTENTS

I. INTRODUCTION

In the search for multiple-error-correcting codes which can be easily and rapidly decoded, some coding theorists have turned their attentions to threshold (majority logic) decoding. Much work has been done in this area recently, and quite a few classes of new codes suitable for threshold decoding have been developed.

The main desirable feature of majority logic decoding is that it can be very simply implemented. While the BCH codes are the best known class of codes for correcting large numbers of random errors, the cost and complexity of its implementation and the time required for decoding leaves something to be desired. On the other hand, although most of the known majority logic decodable codes are somewhat inferior to the BCH codes, the simplicity of a majority logic decoder and the ease of decoding give this method of decoding an attractive prospect. Furthermore majority decoding can also automatically correct many more patterns of errors other than those guaranteed by the decoding schemes without any additional equipment.

This paper is a survey of the L-step majority decoding. One-step majority decoding is studied extensively in a separate report.[3] Majority logic decoding of block codes was first introduced in 1954 by Reed [16] who invented a decoding scheme for the Reed-Muller codes. In 1958 Yale [26] and Zierler [27] applied majority logic decoding to the maximal length sequence codes. In 1961 Mitchell [14] majority decoded the cyclic Hamming codes, the augmented maximal length sequence codes, and the (17,7), (21,11), and (73,45) BCH codes. In his book of 1963, "Threshold Decoding" [13] Massey presented majority decoding algorithms for block codes that are one-step and L-step orthogonalizable. Rudolph's majority decoding algorithm [17,18] differs from previous ones in that the parity checks need not be orthogonal. He also introduced finite geometry in the construction of majority logic decodable codes. His geometric codes were further studied by Chow,[4] Weldon,[15,24,25] Goethals and Delsarte.[5]

Weldon in 1966 devised a class of cyclic codes based on perfect difference sets.[21] Kasami, Lin, and Peterson [9,10,11] showed that all binary Reed-Muller codes with one digit dropped can be made cyclic by rearranging the digits. Generalization to the nonbinary case was then easily made. The non-primitive Reed-Muller codes were studied by Weldon.[22,23] All these codes are subclasses of Rudolph's projective geometry codes and hence are majority decodable.

In 1967 Townsend and Weldon [20] devised a new class of linear block codes, called self-orthogonal quasi-cyclic codes, which is obtained from disjoint difference sets. The code is one-step decodable. In 1969 Gore [6] generalized Massey's concept of threshold decoding and showed that the Reed-Solomon codes are completely threshold decodable. The formal equivalence between Massey's L-step orthogonalization decoding procedure and Reed's majority decoding scheme is also demonstrated by Gore [7] through the formal equivalence of their respective decoding circuit.

II. L-STEP DECODING ALGORITHM

We shall begin our discussion with a series of definitions and examples to make the understanding of the basic idea behind L-step majority decoding as simple as possible.

Consider an (n,k) block code over GF(q) with parity check matrix [H]. We expand this parity check matrix by taking all possible linear combinations of its rows and call this expanded matrix $[H_E]$. If $C = (C_0, C_1, \ldots, C_{n-1})$ is a code vector, obviously

$$[H_E] \cdot C^T = 0 \tag{2.1}$$

Each row of equation (2.1) is a parity check equation.

Definition 2.1: A set of J of the parity check equations of equation (2.1) is said to be orthogonal on the i^{th} bit position if the i^{th} bit is checked by every one of those J equations while no other bit position is checked by more than one of the J equations. Let $[H_E^i] = (h_{jk}^i)$ be the submatrix of $[H_E]$ corresponding to this set of J equations. Then $[H_E^i]$ will have only nonzero elements in the i^{th} column while each of the remaining columns will have no more than one nonzero entry. For example, the following set of 4 equations is orthogonal on the 0^{th} digit

$$\begin{aligned} C_0 + C_1 + C_5 &= 0 \\ C_0 + C_2 + C_6 &= 0 \\ C_0 + C_3 + C_7 &= 0 \\ C_0 + C_4 + C_8 &= 0 \end{aligned} \tag{2.2}$$

corresponding to the submatrix

$$[H_E^o] = \begin{bmatrix} 1&1&0&0&0&1&0&0&0 \\ 1&0&1&0&0&0&1&0&0 \\ 1&0&0&1&0&0&0&1&0 \\ 1&0&0&0&1&0&0&0&1 \end{bmatrix} . \tag{2.3}$$

Suppose $[H_E^i]$ is a submatrix orthogonal on the i^{th} bit position, and let $R = (r_0, r_1, \ldots, r_{n-1})$ be a received vector.

Let

$$[H_E^i] \cdot R^T = [S] \tag{2.4}$$

where $[S]$ is a J elements column vector.

Let $R = C + E = (c_0, \ldots, c_{n-1}) + (e_0, \ldots, e_{n-1})$, where C is the transmitted code vector and E is the error vector. Then from (2.4)

$$[H_E^i] \cdot R^T = [H_E^i] \cdot C^T + [H_E^i] \cdot E^T = 0 + [H_E^i] \cdot E^T = [S].$$

Hence

$$[H_E^i] \cdot E^T = [S] \tag{2.5}$$

is a set of J equations orthogonal on e_i. Equation (2.5) can be written in the alternate expanded form:

$$\sum_{k=0}^{n-1} h_{jk}^{\ i} \cdot e_k = s_j, \qquad j = 1, \ldots, J \tag{2.6}$$

Multiply both sides of each equation by $(h_{ji}^{\ i})^{-1}$ for each $j = 1, \ldots, J$ we obtain

$$e_i + (h^i_{ji})^{-1} \sum_{k \neq i} h^i_{jk} \cdot e_k = (h^i_{ji})^{-1} \cdot s_j = s_j',$$

$$j = k, \ldots, J \qquad (2.7)$$

To obtain an estimate on e_i, we proceed according to theorem 2.2:

Theorem 2.2: e_i is estimated to be equal to that value of GF(q) which is assumed by the majority of $s_1', s_2', \ldots, s_J'$. In case of a tie between zero and a nonzero element, set $e_i = 0$. e_i will be correctly estimated by this decoding procedure if the number of errors $t \leq \frac{J}{2}$.

Proof: (a) If $e_i = 0$, then t of the e_j's, $j \neq i$, are nonzero. Since each e_j, $j \neq i$, is in no more than one of the equations in (1.7), at most t of the J s_j's are nonzero. Hence if $t \leq \frac{J}{2}$, at least half of the $s_1', s_2', \ldots, s_J'$ are equal to 0.

(b) If $e_i = \alpha$, $\alpha \in GF(q)$, $\alpha \neq 0$, then t-1 of the e_j's, $j \neq i$, are nonzero, each appearing in no more than one of the J equations in (2.7). Thus if $t \leq \frac{J}{2}$, at least $J - (t-1) = J+1-t \geq J+1 - \frac{J}{2} = 1 + \frac{J}{2} > \frac{J}{2}$, i.e., more than half, of the J s_j's are equal to α. Hence in both cases, the decoding algorithm works.

Q.E.D.

Theorem 2.2 extends naturally to the decoding of an entire received vector. If for each bit position a set of J or more parity check equations orthogonal on that bit position can be found, then each digit of a received vector can be correctly decoded by the algorithm of theorem 2.2 if a total of no more than $[\frac{J}{2}]$ (where [ ] stands for "the integer part of") errors have occurred. In particular, for a cyclic code, if a set of J parity check equations orthogonal on any bit position can be found, then by the cyclical nature of the code, such a set can be found for every bit position, and hence the entire code vector can be majority decoded using theorem 2.2. For a systematic code, decoding is complete when the first k (information) digits are determined. Hence for complete decoding of a systematic code, J orthogonal parity checks are necessary only for each of the first k digits.

<u>Theorem 2.3</u>: If a set of J parity check equations can be formed orthogonal on every bit position, then the code has minimum distance at least J + 1.

Proof: Assume that there is a nonzero code vector of weight J or less. A set of J orthogonal parity checks can be formed on one of the nonzero digits. The remaining J - 1 or less nonzero digits of the code vector can appear in at most that many parity checks, leaving at least one parity check nonzero, which is not possible. Hence each code vector must have weight J + 1 or greater.

Q.E.D.

<u>Corollary 2.4</u>: For a code in systematic form, if a set of J parity check equations orthogonal on each of the information digits can be formed, then the code has minimum distance at least J+1.

Proof: Observing that every nonzero code vector has at least one nonzero information digit, the proof follows similarly to that of theorem 2.3.

Q.E.D.

As an example of a parity check matrix of a systematic code orthogonal on each of the first k digits, consider the parity check matrix of the following (26,13) code:

$$H = \left[\begin{array}{cccccccccccccccccccccccccc}
1&1& &1& & & &1& & & & & &1& & & & & & & & & & & & \\
1& &1& &1& & & &1& & & & & &1& & & & & & & & & & & \\
1& & & & &1&1& & &1& & & & & &1& & & & & & & & & & \\
1& & & & & & & & & &1&1&1& & & &1& & & & & & & & & \\
 &1&1& & &1& & & & & & &1& & & & &1& & & & & & & & \\
 &1& & &1& &1& & & &1& & & & & & & &1& & & & & & & \\
 &1& & & & & & &1&1& &1& & & & & & & &1& & & & & & \\
 & &1&1& & &1& & & & &1& & & & & & & & &1& & & & & \\
 & &1& & & & &1& &1&1& & & & & & & & & & &1& & & & \\
 & & &1&1& & & & &1& & &1& & & & & & & & & &1& & & \\
 & & &1& &1& & &1& &1& & & & & & & & & & & & &1& & \\
 & & & &1&1& &1& & & &1& & & & & & & & & & & & &1& \\
 & & & & & &1&1&1& & & &1& & & & & & & & & & & & &1
\end{array}\right] \qquad (2.8)$$

Here J = 4 and d = 5. The code can therefore correct 2 errors by the algorithm of theorem 2.2. The code can be over any finite Galois field.

Thus far, the decoding of a digit depends on the existence of a set of parity check equations orthogonal on that digit which are obtainable directly from the original parity check matrix. Such majority decoding is called one-step decoding. However, not all codes can be decoded by such a procedure. For some codes it is necessary to arrive at a set of parity check sums orthogonal on a digit from the original parity check matrix in L steps.

<u>Def 2.5</u>: A set of J parity check equations is said to be orthogonal on the sum of i bit positions ($\alpha_1, \alpha_2, \ldots, \alpha_i$) if the coefficients in positions $\alpha_1, \alpha_2, \ldots, \alpha_i$ are 1 in each equation and no other position has more than one nonzero coefficient in the J parity check equations.

From the original parity check matrix, suppose that we can find sets of parity checks orthogonal on selected sums of noise bits. By applying the algorithm of theorem 2.2 on these sums, they can be determined. These sums of noise bits can then be regarded as new check sums and used to form new sets of parity check sums orthogonal on some smaller sums. Eventually after repeating such steps L times a set of parity check sums orthogonal on a bit position is formed. Such a decoding procedure is called L-step decoding. For a cyclic code, a procedure for decoding one digit decodes all the other digits.

III. HAMMING CODES

Massey has shown that for $M = 2,3,4,\ldots$, the Mth-order binary Hamming $(2^M-1, 2^M-M-1)$, $d = 3$, codes can be L-step orthogonalized for L no greater than M-1. However, it has been shown in a separate report on one-step decoding [3] that all Hamming codes can be one-step decoded by a somewhat different one-step decoding algorithm. Since one-step decoding is simpler than L-step decoding, we shall just look at one example of L-step decoding of a Hamming code for illustration purpose and then move along.

Example: Consider the (7,4) binary Hamming code with $d = 3$. Here $M = 3$ and it will be shown that the code can be 2-step decoded.

The parity check matrix is given by:

$$[H] = \begin{bmatrix} 1&1&0&1&1&0&0 \\ 1&1&1&0&0&1&0 \\ 1&0&1&1&0&0&1 \end{bmatrix} \qquad (3.1)$$

The corresponding parity checks are

$$e_0 + e_1 + e_3 + e_4 = S_1 \qquad (3.2)$$

$$e_0 + e_1 + e_2 + e_5 = S_2 \qquad (3.3)$$

$$e_0 + e_2 + e_3 + e_6 = S_3 \qquad (3.4)$$

Equations (3.2) and (3.3) are 2 equations orthogonal on $e_0 + e_1$ while (3.3) and (3.4) are orthogonal on $e_0 + e_2$. Thus if no more than one error has occurred, the majority decoding algorithm of theorem 2.2 can 2.2 can be used to determine $e_0 + e_1$ and $e_0 + e_2$ from these two sets of orthogonal equations.

Let

$$e_0 + e_1 = t_1 \qquad (3.5)$$

and

$$e_0 + e_2 = t_2 \qquad (3.6)$$

Now equations (3.5) and (3.6) are a set of 2 equations orthogonal on e_0, and hence theorem 2.2 can again be applied to determine e_0 provided that no more than one error has occurred. Thus e_0 can be estimated by the above procedure of 2-step orthogonalization and decoding. A similar procedure can be followed for e_1, e_2, and e_3.

IV. SOME CLASSES OF CODES BASED ON FINITE GEOMETRIES

A class of codes can be defined by taking the incidence matrix of a (b, v, r, k, λ) balanced incomplete block design (BIBD)[12] as its parity check matrix.[17,18] I have called this class of codes the class I BIBD codes.[3] The codes can be one-step decoded by a majority algorithm that does not depend on orthogonal parity checks,[18] and can correct $\left[\frac{r+\lambda-1}{2\lambda}\right]$ errors by such a procedure. The investigation of the possibility of L-step decoding this class of codes is worthwhile if better error correcting capabilities can be achieved by such a procedure than by one-step decoding. So far such an investigation has only been performed on two subclasses of the class I BIBD codes, namely those BIBD's that are related to the projective geometry [1] and the Euclidean geometry. It is well known that block designs can be derived from both of these geometries. We shall now first review some of the properties of finite geometries.

A. Projective geometry

An m-dimensional finite projective geometry over $GF(p^t)$ is denoted by $PG(m, p^t)$. A $PG(m, p^t)$ may be considered as a set of points and subspaces. Each point can be represented by a nonzero element of a $GF(p^{(m+1)t})$. Two elements α and β of $GF(p^{(m+1)t})$ represent the same point if $\alpha = \theta \cdot \beta$, where $\theta \in GF(p^t)$. There are thus $v = (p^{(m+1)t}-1)/(p^t-1)$ points in a $PG(m, p^t)$. A set of all the points linearly dependent on s+1, $s<m$, linearly independent points over $GF(p^t)$ constitutes an s-dimensional subspace $PG(s, p^t)$. There are

$$b(s,m,p^t) = \frac{(p^{(m+1)t}-1)(p^{mt}-1)\dots(p^{(m-s+1)t}-1)}{(p^{(s+1)t}-1)(p^{st}-1)\dots(p^t-1)}$$ distinct $PG(s,p^t)$ contained

in a given PG(m, p^t). Furthermore, each PG(n, p^t), $n<s$, is contained in exactly

$$\lambda(n, s, m, p^t) = \frac{(p^{(m-n)t}-1)(p^{(m-n-1)t}-1)\ldots(p^{(m-s+1)t}-1)}{(p^{(s-n)t}-1)(p^{(s-n-1)t}-1)\ldots(p^t-1)} \qquad (4.1)$$

PG(s, p^t) which are contained in a given PG(m, p^t). By associating the points with varieties, the PG(s, p^t) with blocks, one can obtain from a given PG(m, p^t) a BIBD with parameters:

$$b = b(s, m, p^t)$$

$$v = (p^{(m+1)t}-1) / (p^t-1)$$

$$k = \frac{(p^{(s+1)t}-1)}{(p^t-1)}$$

$$r = \lambda(0, s, m, p^t) \qquad (4.2)$$

$$\lambda = \begin{cases} \lambda(1, s, m, p^t) & \text{for } s > 1 \\ 1 & \text{for } s = 1 \end{cases}$$

The incidence matrix [S] = (s_{ij}) of a PG(m, p^t) is defined by setting $s_{ij} = 1$ if the j^{th} point is in the i^{th} PG(s, p^t), and $s_{ij} = 0$ otherwise.

Theorem 4.1: The incidence matrix [S] of a PG(m, p^t) is cyclic, i.e., every cyclic permutation of a row of [S] is also a row of [S].

Proof: Let α be a primitive root of $GF(p^{(m+1)t})$. Then α^v is a primitive root of $GF(p^t)$. $\alpha^0, \alpha^1, \ldots\ldots, \alpha^{v-1}$ are linearly independent over $GF(p^t)$ and are used to represent all the v points in a $PG(m, p^t)$. Let $\beta_0, \beta_1, \ldots, \beta_s$ be a set of s+1 linearly independent points defining a $PG(s, p^t)$, which is all the distinct linear combinations of the β's over $GF(p^t)$. Each point can be expressed in the form

$$C_i = \sum_{j=0}^{s} \theta_{ij} \beta_j \quad , \qquad \theta_{ij} \in GF(p^t).$$

Cyclic permutation of the row representing this $PG(s, p^t)$ is equivalent to multiplying each point C_i by α, where α^v is identical to α^0. Since

$$\alpha \cdot C_i = \sum_{j=0}^{s} \theta_{ij}(\alpha\beta_j),$$

this results in a set of points which are all the distinct linear combinations of the $\alpha\beta$'s. It only remains to show that $\alpha\beta o, \alpha\beta 1, \ldots, \alpha\beta s$ are a set of s+1 linearly independent points and hence also defines a $PG(s, p^t)$. Assuming that they are linearly dependent over $GF(p^t)$, then

$$\sum_{j=0}^{s} \omega_j(\alpha\beta_j) = 0, \qquad \omega_j \in GF(p^t)$$

for some ω_j, j = 0, 1,..., s. However since $\alpha \neq 0$, this implies that

$$\sum_{j=0}^{s} \omega_j \beta_j = 0,$$

which is a contradiction. Hence $\alpha\beta_0, \ldots., \alpha\beta_s$ are linearly independent.

Q.E.D.

Because of theorem 4.1, in the construction of an incidence matrix of a $PG(m, p^t)$ one does not have to determine all the b distinct $PG(s, p^t)$. One only has to determine the b/v $PG(s, p^t)$ which cannot be obtained from each other by permutation on the incidence matrix, and permutes these rows to obtain the remaining rows.

B. Euclidean geometry

From a given $PG(m, p^t)$, if any $PG(m-1, p^t)$ and all its points are deleted, a new system of points and subspaces results. This new m-dimensional geometry over $GF(p^t)$ is called the Euclidean geometry, denoted by $EG(m, p^t)$. Each point of an $EG(m, p^t)$ can be represented by an element of a $GF(p^{mt})$. There are thus

$$v = p^{mt}$$

points in an $EG(m, p^t)$. Each $PG(s, p^t)$ contained in the original $PG(m, p^t)$ but not in the deleted $PG(m-1, p^t)$ becomes an $EG(s, p^t)$, since by deleting a $PG(m-1, p^t)$ from $PG(m, p^t)$ we also delete a $PG(s-1, p^t)$ from each of these $PG(s, p^t)$. Therefore the number of $EG(s, p^t)$ contained in an $EG(m, p^t)$ is

$$b(s, m, p^t) - b\ (s, m-1, p^t).$$

The number of $EG(s, p^t)$ containing a given $EG(n, p^t)$, $n < s$, is the same as the number of $PG(s, p^t)$ containing a given $PG(n, p^t)$, namely $\lambda(n, s, m\ p^t)$. Let $\beta_1, \beta_2, \ldots, \beta_s$ be s elements of $GF(p^{mt})$ linearly independent over $GF(p^t)$. Then an $EG(s, p^t)$ can be considered as the set of points $a_1\beta_1 + a_2\beta_2 + \ldots + a_s\beta_s + \gamma$

where $a_1, a_2, \ldots, a_s$ run independently over $GF(p^t)$ and γ is some element in $GF(p^{mt})$. As with the projective geometry, the $EG(s, p^t)$ of an $EG(m, p^t)$ form a balanced incomplete block design with parameters

$$
\begin{aligned}
b &= b(s, m, p^t) - (b(s, m-1, p^t) \\
v &= p^{mt} \\
r &= \lambda(0, s, m, p^t) \\
k &= p^{st} \\
\lambda &= \begin{cases} \lambda(1, s, m, p^t) & \text{if } s < 1 \\ 1 & \text{if } s = 1 \end{cases}
\end{aligned}
\qquad (4.3)
$$

C. Class A PG Codes

As stated in the beginning of this section, the class I BIBD codes are defined by taking the incidence matrix of a balanced incomplete block design as its parity check matrix. We shall now define the class A PG codes by taking the incidence matrix of a projective geometry as its parity check matrix. Since a balanced incomplete block design can be derived from a projective geometry, the class A PG code is naturally a subcode of the class I BIBD code. Since there are m-1 levels of $PG(s, p^t)$ in a $PG(m, p^t)$, corresponding to $s=1,2,\ldots,m-1$, there are m-1 different incidence matrices for each $PG(m,p^t)$. Furthermore, the code which is defined by an incidence matrix of a projective geometry may be taken over any finite Galois field. Hence there can be infinitely many class A PG codes.

The class A PG codes can be one-step majority decoded by an algorithm which does not depend on orthogonal parity checks. The number of errors that can be corrected by this procedure is

$$t = \frac{r+\lambda-1}{2\lambda} \tag{4.4}$$

where r and λ are as in (4.2). However the class A PB codes can also be L-step majority decoded which may or may not yeild better error correcting capabilities. Consider the incidence matrix of the b distinct $PG(1, p^t)$, every pair of points is in one and only one $PG(1, p^t)$. Hence a set of r orthogonal parity ckecks can be formed on any bit position, and the code is one-step orthogonalizable. From now on we shall only consider the case $s > 1$ where the code cannot be one-step orthogonalized.

Now consider the parity check matrix of a class A PG code which is the incidence matrix of the b distinct $PG(s, p^t)$ in a $PG(m, p^t)$. Each $PG(s-1, p^t)$ of $PG(m, p^t)$ is contained in exactly

$$J^o = \lambda(s-1, s, m, p^t) = \frac{p^{(m-s+1)t}-1}{p^t-1} \tag{4.5}$$

$PG(s, p^t)$. Since the s linearly independent points defining a given $PG(s-1, p^t)$ plus another point not in this $PG(s-1, p^t)$ define one and only one $PG(s, p^t)$, each point in the $PG(m, p^t)$ which is not in a given $PG(s-1, p^t)$ appears in at most one of the J^o $PG(s, p^t)$ containing this $PG(s-1, p^t)$. Consequently a set of J^o parity checks orthogonal on the points of each $PG(s-1, p^t)$ can be formed. In general, a given $PG(s-i-1, p^t)$ is contained in exactly

$$J^i = \lambda(s-i-1, s-i, m, p^t) = \frac{p^{(m-s+i+1)t}-1}{p^t-1} \tag{4.6}$$

$PG(s-i, p^t)$. These again form J^i orthogonal parity check sums on the points of the given $PG(s-i-1, p^t)$. Thus beginning with i=0 and finishing with i=s-1, one arrives in s steps at a set of J^{s-1} parity check sums orthogonal on one point. Looking at equation (4.6) one can see that $J^o < J^1 <\ldots< J^{s-1}$. Applying the majority decoding algorithm of theorem 2.2 at each step, the error at a point can eventually be correctly estimated if the total number of errors $t \leq \frac{\min\{J^i\}}{2} = \frac{J^o}{2}$.

As already pointed out, a class A PG code defined by an incidence matrix [S] of a projective geometry may be taken over any GF(q). The choice of GF(q) does not affect the error correcting ability of the code, as is obvious in the above discussion. The number of check digits per block length is equal to the rank of [S], the parity check matrix, over GF(q). Thus the efficiency of the code depends on the choice of the field. All the work done in this area so far has been limited to the choice of q = p, where the code is commonly known as projective geometry code. However, since all practical codes are binary codes, GF(2) seems to be a more practical choice although this may yield a less efficient code.

To summarize, the class A PG code can correct $[\frac{r+\lambda-1}{2\lambda}]$ errors using one-step decoding and $[\frac{J^o}{2}]$ errors using L-step decoding. The choice of which decoding procedure to use is not obvious. One-step decoding is easier to implement and is definitely the better choice when it can correct the same number of errors as L-step decoding, i.e., $[\frac{r+\lambda-1}{2\lambda}] = [\frac{J^o}{2}]$. However in the case where $[\frac{J^o}{2}] > [\frac{r+\lambda-1}{2\lambda}]$, a trade off must be made between ease of implementation on one hand and error correcting capabilities on the other.

D. Class A EG Codes

A class A EG code can be defined in a similar manner as the class A PG code by taking the incidence matrix [S] of all the EG(s, p^t) contained in an EG(m, p^t) as the parity check matrix. This class A EG code is also a subcode of the class I BIBD code. The field of the code can again be chosen arbitrarily without affecting the error correcting capabilities of the code. The choice of the field GF(q), however, does affect the number of check digits which is the rank of [S] over GF(q). When q = p, the code is commonly known as Euclidean geometry code. However GF(2) is a more suitable choice for practical applications.

When one-step majority decoding is applied, the class A code can correct $[\frac{r+\lambda-1}{2\lambda}]$ errors, where r and λ are as in (4.3). Just as the class A PG code, the class A EG code can also be L-step decoded. The procedure is exactly analogous to that of the PG code. Each EG(s-i-1, p^t) is contained in exactly J^i EG(s-i, p^t). Since the (s-i-1) linearly independent points defining an EG(s-i-1, p^t) plus another point not in this EG(s-i-1, p^t) define one and only one EG(s-i-1, p^t), each point in the EG(m, p^t) which is not in a given EG(s-i-1, p^t) is in at most one of the J^i EG(s-i, p^t) containing this EG(s-i-1, p^t). Thus in s steps a set of J^{s-1} EG(1, p^t) orthogonal on a point can be formed. Applying the majority decoding algorithm of theorem 2.2 at each step, the error at a point can eventually be correctly estimated if the total number of errors $t \le \frac{J^o}{2}$.

E. Class B PG Codes

The incidence matrix of a balanced incomplete block design can also be used to generate another class of codes, which I have called the class III

BIBD codes.[3] Consider the parity check matrix [H] of a code which is in the systematic form. Then [H] is of the form

$$[H] = [P \vdots I] \tag{4.7}$$

where I is an identity matrix. A class III BIBD code is defined by substituting the incidence matrix [S] of a balanced incomplete block design into P of (4.7). If [S] is also the incidence matrix of a projective geometry, then we define the resulting code to be a class B PG code. Naturally this code is a subclass of the class III BIBD codes. Once again the choice of the field of the code can be arbitrary. However, here the choice of the field does not have any effect on the efficiency of the code, since from (4.7) it is obvious that the code has block length b+v, b parity check digits, and v information digits, where b and v are as in (4.2). Furthermore since $b \geq v$, the class B PG code can only have a maximum efficiency of no more than 0.5.

Since the (b+v,v) class B PG code is in systematic form, the first v digits of each code word are the information digits. For each received vector, it is then only necessary to decode these first v digits. It is now obvious that each of these first v digits can be decoded in exactly the same manner as the decoding of each digit of a class A PG code, because each parity check digit appears in one and only one parity check equation. Consequently a class A PG code and a class B PG code can correct $[\frac{r+\lambda-1}{2\lambda}]$ errors using one-step decoding and $[\frac{J^{o}}{2}]$ errors using L-step decoding. The choice of which decoding procedure to use faces the same considerations as those of the class A codes.

F. Class B EG Codes

The class B EG code can be similarly defined as the class B PG code. By substituting the incidence matrix [S] of an Euclidean geometry into P of equation (4.7), the result is a parity check matrix of a class B PG code, which can be decoded in exactly the same manner as the class B PG code. $\left[\frac{r+\lambda-1}{2\lambda}\right]$ and $\left[\frac{J^{o}}{2}\right]$ are its error correcting capabilities by one-step and L-step decoding respectively. The code has block length b+v and v information digits, where b and v are as in (4.3). The choice of the field can be taken arbitrarily without affecting either the error correcting capabilities or the efficiency of the code.

V. GENERALIZED THRESHOLD DECODING

In all of the previous sections, L-step majority logic decoding had depended on the existence of a set of J parity check equations orthogonal on the sum of s positions, and the coefficients of each of these s positions are 1 in all of the parity check equations. If any of those coefficients is other than 1, the decoding scheme will obviously still work provided that the coefficients of each of the s positions are the same throughout the set of J parity check equations. In other words, if $a_1e_1+b_1e_2$ and $a_2e_1+b_2e_2$ are in two different parity check equations orthogonal on e_1 and e_2, majority logic decoding is seen to work easily just as well in determining the sum ae_1+be_2 provided $a_1 = a_2 = a$ and $b_1 = b_2 = b$. However if $a_1 \neq a_2$ or $b_1 \neq b_2$, it is not obvious at all that majority decoding would work. After all it does not make any sense to take a majority vote on $a_1e_1 + b_1e_2$ and $a_2e_1 + b_2e_2$ when they are two different entities. Thus if a set of J parity check equations is orthogonal on s positions with the coefficients in these positions arbitrary, it seems apparent that the previously given majority decoding algorithm cannot be applied. However, by interpreting the meaning of a parity check in a somewhat different manner, Gore was able to show that our previously given majority decoding algorithm can still be applied in precisely the same form to the case of arbitrary coefficients. He called it "generalized threshold decoding"[6] although the algorithm is the same.

A. Generalized threshold decoding

Consider a parity check equation on position i and s other positions $(m_1, m_2, \ldots, m_s)$. With the coefficient in position i normalized, the equation can be written as

$$e_i + \sum_{j=1}^{s} \beta_{m_j} e_{m_j} = A. \tag{5.1}$$

We can interpret (5.1) as an equation which gives the error digit in position i if no errors have occurred in positions $m_1, m_2, \ldots, m_s$. Such an equation is called a generalized parity check equation and is written as

$$C(i;m_1,m_2,\ldots,m_s) = A. \tag{5.2}$$

Thus every parity check equation can be written as some generalized parity check equation.

We define here again a set of J parity check equations to be orthogonal on position i and s other positions $(m_1, m_2, \ldots, m_s)$ if the coefficient in position i is 1 in each equation, and the coefficients in positions $m_1, m_2, \ldots, m_s$ are arbitrary, while no other position has more than one nonzero coefficient in the J parity check equations. Also we define a set of J generalized parity check equations to be orthogonal on position i and s other positions $(m_1, m_2, \ldots, m_s)$ if i and $m_1, m_2, \ldots, m_s$ are in every one of these J generalized parity checks while no other position appears in more than one of these equations. Since every parity check equation is in fact a generalized parity check, a set of J parity check equations orthogonal on position i and s other positions $(m_1, m_2, \ldots, m_s)$ can be written as a set J generalized parity check equations orthogonal on the same set of positions. For example, (5.3) is a set of 4 parity check equations orthogonal on position 1 and positions 2 and 3.

$$
\begin{aligned}
&e_1 + \beta_1 e_2 + \beta_2 e_3 + \gamma_1 e_4 \qquad\qquad + \gamma_5 e_8 &&= A_1\\
&e_1 + \beta_3 e_2 + \beta_4 e_3 \qquad + \gamma_2 e_5 \qquad\qquad + \gamma_6 e_9 &&= A_2\\
&e_1 + \beta_5 e_2 + \beta_6 e_3 \qquad\qquad + \gamma_3 e_6 \qquad\qquad + \gamma_7 e_{10} &&= A_3\\
&e_1 + \beta_7 e_2 + \beta_8 e_3 \qquad\qquad\qquad + \gamma_4 e_7 \qquad\qquad + \gamma_8 e_{11} &&= A_4 \,.
\end{aligned}
\tag{5.3}
$$

(5.3) may be written as a set of 4 generalized parity check equations also orthogonal on position 1 and positions 2 and 3 as in (5.4).

$$
\begin{aligned}
C_1(1;2,3,4,8\ ) &= A_1\\
C_2(1;2,3,5,9\ ) &= A_2\\
C_3(1;2,3,6,10) &= A_3\\
C_4(1;2,3,7,11) &= A_4
\end{aligned}
\tag{5.4}
$$

The majority logic decoding algorithm given previously in section II can now be applied directly to the case of arbitrary coefficients. This is stated in theorem 5.1.

<u>Theorem 5.1</u>: A generalized parity check equation on position i and s other positions $(m_1,m_2,...,m_s)$ can be constructed from a set of J generalized parity check equations orthogonal on the same set of positions

$$
\begin{aligned}
C_1(i;m_1,m_2,...,m_s,S_1) &= A_1\\
C_2(i;m_1,m_2,...,m_s,S_2) &= A_2\\
&\vdots\\
C_J(i;m_1,m_2,...,m_s,S_J) &= A_J
\end{aligned}
$$

where S_1, S_2, ..., S_J represent disjoint sets of positions, provided that

[J/2] or fewer errors have occurred. The new generalized parity check equation $C(i;m_1,m_2,\ldots,m_s) = B$ is obtained by setting B to be that value assumed by the majority of the A_j. If zero (0) is assumed by exactly half of the A_j, B is given the value 0.

Proof: The proof is exactly the same as that of Theorem 2.2. Because of the definition of a generalized parity check equation, it is only necessary to show that if no errors occur in $m_1,m_2,\ldots,m_s$, the above assignment of the value of B indeed gives the correct error digit in position i. Thus assuming no errors in positions $m_1,m_2,\ldots,m_s$ for all cases, if $e_i = 0$, due to the orthogonality of the set of equations, at most $[\frac{J}{2}]$ of the A_j are incorrect leaving at least $J-[\frac{J}{2}]\geq[\frac{J}{2}]$ of the A_j correctly giving the value of 0. If $e_i \neq 0$, then at most $[\frac{J}{2}]-1$ of the A_j will be incorrect, leaving at least $J-[\frac{J}{2}]+1>[\frac{J}{2}]$ of the A_j correctly giving the value of e_i.

Q.E.D.

If one can apply the algorithm of theorem 5.1 repeatedly on successively smaller and smaller sets of positions $m_1,m_2,\ldots,m_s$ and arrive at the end of L steps a generalized parity check equation on i alone, i.e., $C(i) = e_i$, then L-step majority decoding is achieved. It is now obvious that the only difference between the algorithm of Section II and that of theorem 5.1 lies only in their interpretations of the result of a majority voting. The new interpretation extends the domain of the application of the majority logic decoding to include those cases of arbitrary coefficients, and hence are rightfully called generalized threshold decoding.

As a simple example of the application of this generalized threshold decoding, let us consider again the binary (7,4) Hamming code which has already been shown to be 2-step decodable previously. Referring to equations (3.2), (3.3), and (3.4), the corresponding generalized parity checks are

$$C_1(0;1,3,4) = S_1 \quad (5.5)$$

$$C_2(0;1,2,5) = S_2 \quad (5.6)$$

$$C_3(0;2,3,6) = S_3. \quad (5.7)$$

Equations (5.5) and (5.6) are a set of 2 generalized parity checks orthogonal on position 0 and position 1, while (5.6) and (5.7) are orthogonal on position 0 and position 2. Thus if no more than one error has occurred, the generalized threshold decoding algorithm of theorem 5.1 can be used to determine C(0;1) and C(0;2) from these two sets of orthogonal generalized parity checks. Let

$$C(0;1) = t_1 \quad (5.8)$$

and

$$C(0;2) = t_2. \quad (5.9)$$

Now (5.8) and (5.9) are a set of 2 generalized parity checks orthogonal on position 0 alone, and hence theorem 5.1 can again be applied to determine C(0), which is equal to the error digit in position 0. Hence e_o can be estimated by the above procedure of 2-step majority decoding. A similar procedure can be followed for the remaining digits.

B. Reed-Solomon Codes

The r-th order extended Reed-Solomon (ERS) code is defined to be the code of length $q = p^m$ and over GF(q), whose generator matrix G is given by

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots\cdots & 1 \\ 0 & 1 & \alpha^1 & \alpha^2 & \cdots\cdots & \alpha^{q-2} \\ 0 & 1 & \alpha^2 & \alpha^4 & \cdots\cdots & \alpha^{2(q-2)} \\ \cdot & \cdot & \cdot & & & \cdot \\ \cdot & \cdot & \cdot & & & \cdot \\ \cdot & \cdot & \cdot & & & \cdot \\ 0 & 1 & \alpha^r & \alpha^{2r} & \cdots\cdots & \alpha^{r(q-2)} \end{bmatrix} \qquad (5.10)$$

where α is a primitive element of GF(q). The code has minimum distance $d = q-r$ and is therefore capable of correcting $\left[\frac{q-r-1}{2}\right]$ or fewer errors. It will be shown that the code can be r-step majority decoded up to its guaranteed minimum distance.

Let $(b_1, b_2, \ldots, b_n)$ be the set of coefficients of a parity check equation. This vector is in the null space of the generator matrix and hence

$$[b_1 \; b_2 \; \cdots \; b_n]G^T = 0. \qquad (5.11)$$

Since the rows of G are all linearly independent, the rank of matrix G is (r+1). We can therefore select arbitrarily (q-r-1) of the b_j and determine the remaining (r+1) b_j from (5.11). Suppose we wish to determine the error digit in position i. We can assign the value 1 to b_i and 0 to any (q-r-2) of the remaining (q-1) b_j. Then from (5.11) we can determine the value of b_j for the remaining (r+1) positions $(m_1, m_2, \ldots, m_{r+1})$. Therefore

$$e_i + \sum_{k=1}^{r+1} b_{m_k} e_{m_k} = S \qquad (5.12)$$

is a parity check equation from which we can obtain a generalized parity check equation on position i and positions $(m_1, m_2, \ldots, m_{r+1})$

$$C(i; m_1, m_2, \ldots, m_{r+1}) = S. \qquad (5.13)$$

However $(m_1, m_2, \ldots, m_{r+1})$ in (5.13) can be chosen arbitrarily from (q-1) positions except i. Hence we can fix r of the positions and choose the (r+1)st position from the remaining (q-r-1) positions successively, yielding a set of $J = (q-r-1)$ generalized parity check equations orthogonal on i and r other positions. If $[\frac{J}{2}]$ or fewer errors have occurred, we can apply the generalized threshold decoding algorithm of theorem 5.1 and obtain a new generalized parity check on i and the other r positions. Again since the r positions can be chosen arbitrarily, we can repeat the procedure, obtaining at the k-th step a new generalized parith check on i and (r+1-k) other positions from a set of J_k orthogonal generalized parity checks, where

$$J_k = q - r - 2 + k. \qquad (5.14)$$

Hence at the end of (r+1) steps, the generalized parity check on position i is determined, which is e_i. Further, since (5.14) is a monotonically increasing function of k, e_i will be correctly determined by the above (r+1)-step majority decoding procedure if $[\frac{J_1}{2}] = [\frac{q-r-1}{2}]$ or fewer errors have occurred, which is the original guaranteed error correcting ability of the code. Hence the r-th order ERS code can be completely (r+1)-step majority decoded.

VI. RUDOLPH'S THRESHOLD DECODING OF CYCLIC CODES

Closely related to the subject of majority decoding is the threshold decoding. In threshold decoding, a threshold function assigns an error digit or output digit to each received vector. Majority logic decoding can obviously be considered as one form of threshold decoding. Rudolph [19] has devised a threshold decoding algorithm which can decode any cyclic code over GF(p) up to its minimum distance by a single threshold element. The algorithm depends on a general decomposition theorem for complex-valued functions defined on the space of all r-tuples with elements from the ring of integers modulo p.

We first define the following notations.

1) The symbol † defines the mapping $x^{\dagger} = \epsilon^{x}$, where $\epsilon = \exp(2\pi i/p)$. If (a_{ij}) is a matrix, then $(a_{ij})^{\dagger} = (a_{ij}^{\dagger})$.
2) A_r stands for the $p^r \times r$ matrix whose rows are the p-ary representations of the numbers $0,1,\ldots,p^r-1$ in that order.
3) If $x = \rho\epsilon^{\theta}$ is any complex number where ρ and θ are real numbers and $\rho \geq 0$, $-\frac{1}{2} \leq \theta < \rho - \frac{1}{2}$, then we define a threshold function T such that $T(x) = [\theta + \frac{1}{2}]$, where $[z]$ denotes the integer part of z. If y is an integer, then

$$\begin{aligned} y + T(x) &= y + [\theta + \tfrac{1}{2}] \\ &= [y + \theta + \tfrac{1}{2}] \\ &= T(p\, \epsilon^{y+\theta}) \\ &= T(\epsilon^{y} \cdot p\, \epsilon^{\theta}) \\ &= T(y^{\dagger} \cdot x). \end{aligned} \tag{6.1}$$

Let H be the r×n parity check matrix of a linear cyclic code over GF(p). Let y be a received vector when the code vector c is sent. Then y-c=e where e is the error vector. Let s be the syndrome when y is received. Then $s = yH^T$. The set of all syndromes is the set of p-ary numbers $0,1,\ldots,p^r-1$, i.e., the rows of A_r. Let e_s be the error pattern associated with a syndrome s. Then the decoded code word $\hat{c} = y-e_s$, where $s = yH^T$. Considering only the first digit, then

$$\hat{c}_o = y_o - e_{so} \pmod{p}. \tag{6.2}$$

Let f be a function that maps the syndrome s to the first digit of its corresponding error pattern, i.e., $f(s) = -e_{so}$. Then

$$\hat{c}_o = y_o + f(s). \tag{6.3}$$

By the decomposition theorem for complex-valued functions, there exists a weight vector w such that f(s) can be expressed in the form

$$f(s) = T[(sA_r^T)^\dagger w]. \tag{6.4}$$

Since $s = yH^T$,

$$\begin{aligned} f(s) &= T[(yH^T A_r^T)^\dagger w] \\ &= T[(yH'^T)^\dagger w], \end{aligned} \tag{6.5}$$

where

$$H' = A_r H. \tag{6.6}$$

Equation (6.3) can now be rewritten as

$$\hat{c}_o = y_o + T[(yH'^T)^{\dagger} w] \quad (\text{mod } p). \tag{6.7}$$

By the property (6.1),

$$\hat{c}_o = T[y_o^{\dagger} (yH'^T)^{\dagger} w] \quad (\text{mod } p). \tag{6.8}$$

Now

$$\begin{aligned} a^{\dagger} \cdot b^{\dagger} &= \epsilon^a \cdot \epsilon^b \\ &= \epsilon^{a+b} \\ &= (a+b)^{\dagger}. \end{aligned} \tag{6.9}$$

Therefore

$$\begin{aligned} y_o^{\dagger} (yH'^T)^{\dagger} &= y_o^{\dagger} [(y_o\ y_1\ \ldots\ y_{n-1})H'^T]^{\dagger} \\ &= [(y_o\ y_o\ \ldots\ y_o) + (y_o\ y_1\ \ldots\ y_{n-1})H'^T]^{\dagger} \\ &= \left[(y_o\ y_1\ \ldots\ y_{n-1}) \begin{bmatrix} 1\ 1\ \ldots\ 1 \\ 0 \end{bmatrix} + (y_o\ y_1\ \ldots\ y_{n-1})H'^T \right]^{\dagger} \\ &= [(y_o\ y_1\ \ldots\ y_{n-1})B]^{\dagger}, \end{aligned} \tag{6.10}$$

where B is the matrix obtained by adding 1 to each element in the first row of H'^T. Now (6.8) can be rewritten as

$$\hat{c}_o = T[(yB)^{\dagger} w] \quad (\text{mod } p). \tag{6.11}$$

Equation (6.11) is the threshold decoding function for y_o. To decode the remaining digits, it is only necessary to shift the vector y successively in

(6.11), since the code is a cyclic code. It only remains to find the weight vector w such that it satisfies equation (6.4) and gives the simplest decoding circuit.

As an example, we again consider the binary (7,4) Hamming code, whose parity check matrix is

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 \end{bmatrix} . \tag{6.12}$$

The eight different syndromes and their corresponding error patterns are tabulated below together with the function $f(s) = -e_{so}$:

s	e_s	f(s)
0 0 0	0 0 0 0 0 0 0	0
0 0 1	0 0 0 0 0 1 0	0
0 1 0	0 0 0 1 0 0 0	0
0 1 1	0 0 0 0 0 0 1	0
1 0 0	0 0 0 0 1 0 0	0
1 0 1	0 0 1 0 0 0 0	0
1 1 0	0 1 0 0 0 0 0	0
1 1 1	1 0 0 0 0 0 0	1

(6.13)

Note that for the binary case $\epsilon = \exp(\frac{2\pi i}{2}) = -1$. We now have to find a weight vector w such that (6.4) is satisfied for all s. One of the possible solutions is

$$w = \begin{pmatrix} 2 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} . \tag{6.14}$$

The matrix H' as defined by (6.6) is obtained by substituting in A_3 and (6.12),

$$H' = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix} . \tag{6.15}$$

Finally the B matrix in (6.11) is obtained by adding 1 to each element in the first row of the transpose of H'.

$$B = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \end{bmatrix} . \tag{6.16}$$

Therefore the threshold function for the first decoded digit is

$$\hat{c}_o = T\left\{ \left(y \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \end{bmatrix} \right)^{\dagger} \begin{bmatrix} 2 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \right\}$$

$$= T\left\{ \left(y \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix} \right)^{\dagger} \begin{bmatrix} 2 \\ 1 \\ 1 \\ 1 \end{bmatrix} \right\} . \tag{6.17}$$

The threshold functions for the remaining digits are obtained from (6.17) by simply cyclic shifting the received vector y. Note that since $\epsilon = -1$ for the binary case, the function $\dagger$ simply maps even integers to 1 and odd integers to -1, while the function T maps positive integers to 0 and negative integers to 1.

VII. SUMMARY

In the preceding sections a survey on L-step majority decoding has been given. In Chapter II the procedure of L-step decoding was explained. The application of L-step majority decoding to Hamming codes was shown in Chapter III. In Chapter IV four classes of codes, including two new classes, constructed from finite geometry were introduced. These codes can all be L-step majority decoded. Chapter V explained Gore's generalized threshold decoding which increases the number of classes of majority decodable codes. Finally a new threshold decoding procedure for cyclic codes over GF(p) by Rudolph was presented in Chapter VI.

As a final word, further research should be done in the area of majority logic decoding to find better majority logic decodable codes and decoding algorithm; better codes in the sense of higher efficiency and greater number of correctable errors, and better algorithm in the sense of easier implementation and correcting larger number of errors.

REFERENCES

1. Berman, G., 1952, "Finite Projective Geometries," Canadian Journal of Mathematics, Vol. IV, No. 3.

2. Bose, R. C., 1939, "On the Construction of Balanced Incomplete Block Designs," Annals of Eugenics, 9, pp. 353-399.

3. Chien, R. T. and Ng, S. W., 1970, "One-step Majority Logic Decoding," Coordinated Science Lab., University of Illinois, Urbana, Ill., CSL Report I-138.

4. Chow, D., 1967, "A Geometric Approach to Coding Theory with Application to Information Retrieval," Coordinated Science Lab., University of Illinois, Urbana, Ill., CSL Report R-368.

5. Goethals, J. M. and Delsarte, P., 1968, "On a Class of Majority Logic Decodable Cyclic Codes," IEEE Trans. Information Theory, IT-14, pp. 182-188.

6. Gore, W. C., 1969, "Generalized Threshold Decoding and the Reed-Solomon Codes," IEEE Trans. Information Theory, Vol. IT-15, pp. 78-81.

7. Gore, W. C., 1969, "The Equivalence of L-step Orthogonalization and a Reed Decoding Procedure," IEEE Trans, Information Theory, Vol. IT-15, p. 184.

8. Graham, R. L. and MacWilliams, F. J., 1966, "On the Number of Information Symbols in Difference Set Cyclic Codes," B.S.T.J., Vol. 45, pp. 1057-1070.

9. Kasami, T. and Lin, S., 1966, "Some Codes Which are Invariant Under Doubly Transitive Permutation Group and their Connection with Balanced Incomplete Block Designs," AFCRL-66-142.

10. Kasami, T., Lin, S. and Peterson, W. W., 1966, "Some Results on Cyclic Codes which are Invariant Under the Affine Group," AF Cambridge Res. Ctr. Rept. 9, Proj. AF 19 (628) - 4371.

11. Kasami, T., Lin, S. and Peterson, W. W., 1968, "New Generalization of the Reed-Muller Codes. Part I: Primitive Codes, IEEE Trans. Information Theory, IT-14, pp. 189-199.

12. Mann, H. B., 1949, Analysis and Designs of Experiments, Dovis Pulbications, New York.

13. Massey, J., 1963, Threshold Decoding, M.I.T. press.

14. Mitchell, M. E., et al., 1961, "Coding and Decoding Operations Research," for U.S.A.F. Cambridge Research Ctr., Bedford, Mass., General Electric Co. Final Rept., Contract AF 19_604)-6183.

15. Peterson, W. W. and Weldon, E. J., Error-Correcting Codes, 2nd Edition, to be published.

16. Reed, I. S., 1954, "A Class of Multiple-Error-Correcting Codes and the Decoding Scheme," IRE Trans. on Information Theory, IT-4, pp. 38-49.

17. Rudolph, L. D., 1964, "Geometric Configuration and Majority Logic Decodable Codes," MEE Thesis, University of Oklahoma, Norman, Okla.

18. Rudolph, L. D., 1967, "A Class of Majority Logic Decodable Codes," IEEE Trans. Inform. Theory, IT-13, pp. 305-6.

19. Rudolph, L. D., 1969, "Threshold Decoding of Cyclic Codes," IEEE Trans. Inform. Theory, IT-15, pp. 414-418.

20. Townsend, R. L. and Weldon, E. J., 1967, "Self-Orthogonal Quasi-Cyclic Codes," IEEE Trans. Inform. Theory, IT-13, pp. 183-195.

21. Weldon, E. J., 1966, "Difference Set Cyclic Codes," B.S.T.J., Vol. 45, pp. 1045-55.

22. Weldon, E. J. 1967, "Non-primitive Reed-Muller Codes," presented at First Princeton Symposium on Circuit Theory.

23. Weldon, E. J., 1968, "New Generalization of the Reed-Muller Codes Part II: Nonprimitive Codes," IEEE Trans. Inform. Theory, IT-14, pp. 199-205.

24. Weldon, E. J., 1968, "Euclidean Geometry Cyclic Codes," Chapt. 23 in R. C. Bose and T. A. Dowling (eds.) Proceedings of the Conference on Combinatorial Mathematics and Its Applications (Apr. 10-14, 1967), University of North Carolina Press.

25. Weldon, E. J., 1968, "Majority-Logic Decodable Codes," Chapt. 11 in Principles of Data Communication by R. W. Lucky, J. Salz, and E. J. Weldon, McGraw Hill.

26. Yale, R. B., 1958, "Error-Correcting Codes and Linear Recurring Sequences," M.I.T. Lincoln Lab., Lexington, Mass., Lincoln Laboratory Group Rept. 34-77.

27. Zierler, N., 1958, "On a Variation of the First Order Reed-Muller Codes," M.I.T. Lincoln Lab., Lexington, Mass., Lincoln Laboratory Group Rept. 34-80.

Distribution List as of April 1,1970

ESD (ESTI)
L. G. Hanscom Field
Bedford, Mass 01731 2 copies

Defense Documentation Center
Attn: DDC-TCA
Cameron Station
Alexandria, Virginia 22314 50 copies

Commanding General
Attn: STEWS-RE-L, Technical Library
White Sands Missile Range
New Mexico 88002 2 copies

Mr Robert O. Parker, AMSEL-RD-S
Executive Secretary, TAC/JSEP
U.S. Army Electronics Command
Fort Monmouth, New Jersey 07703

Director, Electronic Programs
Attn: Code 427
Department of the Navy
Washington, D.C. 20360 2 copies

Naval Air Systems Command
AIR 03
Washington, D.C. 20360 2 copies

Director
Naval Research Laboratory
Attn: Code 2027
Washington, D.C. 20390 6 copies

Naval Electronic Systems Command
ELEX 03, Room 2046 Munitions Building
Department of the Navy
Washington, D.C. 20360 2 copies

Commander
U.S. Naval Ordnance Laboratory
Attn: Librarian
White Oak , Md 20910 2 copies

LTC H. W. Jackson
Chief, Electronics Division
Directorate of Engineering Sciences
Air Force of Scientific Research
Arlington, Virginia 22209 5 copies

Commander
Naval Electronics Laboratory Center
Attn: Library
San Diego, Calif 92152 2 copies

Dr. L. M. Hollingsworth
AFCRL (CRN)
L. G. Hanscom Field
Bedford, Mass 01731

Division of Engineering & Applied Physics
210 Pierce Hall
Harvard University
Cambridge, Mass 02138

Director
Research Laboratory of Electronics
Massachusetts Institute of Technology
Cambridge, Mass 02139

Miss R. Joyce Harman
Project MAC, Room 810
545 Technology Square
Cambridge, Mass 02139

Professor R. H. Rediker
Elec Engineering Professor
Mass, Institute of Technology
Building 13-3050
Cambridge, Mass 02139

Raytheon Company
Research Division Library
28 Seyon Street
Waltham, Mass 02154

Sylvania Electronic Systems
Applied Research Laboratory
Attn: Documents Librarian
40 Sylvan Road
Waltham, Mass 02154

Commanding Officer
Army Materials & Mechanics
Research Center
Attn: Dr H. Priest
Watertown Arsenal
Watertown, Mass 02172

MIT Lincoln Laboratory
Attn: Library A-082
PO Box 73
Lexington, Mass 02173

Commanding Officer
Office of Naval Research
Branch Office
495 Summer Street
Boston, Mass 02210

Commanding Officer (Code 2064)
U.S. Naval Underwater Sound Laboratory
Fort Trumbull
New London, Conn 06320

Dept of Eng & Applied Science
Yale University
New Haven, Conn 06520

Commanding General
U.S. Army Electronics Command
Attn: AMSEL-CT-A
Fort Monmouth, New Jersey 07703

Commanding General
U.S. Army Electronics Command
Attn: AMSEL-CT-D
Fort Monmouth, New Jersey 07703

Commanding General
U.S. Army Electronics Command
Attn: AMSEL-CT-I
Fort Monmouth, New Jersey 07703

Commanding General
U.S. Army Electronics Command
Attn: AMSEL-CT-L (Dr W.S. McAfee)
Fort Monmouth, New Jersey 07703

Commanding General
U.S. Army Electronics Command
Attn: AMSEL-CT-O
Fort Monmouth, New Jersey 07703

Commanding General
U.S. Army Electronics Command
Attn: AMSEL-CT-R
Fort Monmouth, New Jersey 07703

Commanding General
U.S. Army Electronics Command
Fort Monmouth, New Jersey 07703
Attn: AMSEL-CT-S

Commanding General
U.S. Army Electronics Command
Attn: AMSEL-GG-DD
Fort Monmouth, New Jersey 07703

Commanding General
U.S. Army Electronics Command
Attn: AMSEL-DL
Fort Monmouth, New Jersey 07703

Commanding General
U.S. Army Electronics Command
Attn: AMSEL-KL-D
Fort Monmouth, New Jersey 07703

Commanding General
U.S. Army Electronics Command
Attn: AMSEL-KL-E
Fort Monmouth, New Jersey 07703

Commanding General
U.S. Army Electronics Command
Attn: AMSEL-KL-I
Fort Monmouth, New Jersey 07703

Commanding General
U.S. Army Electronics Command
Attn: AMSEL-KL-SM
Fort Monmouth, New Jersey 07703

Commanding General
U.S. Army Electronics Command
Attn: AMSEL-KL-S
Fort Monmouth, New Jersey 07703

Commanding General
U.S. Army Electronics Command
Attn: AMSEL-KL-T
Fort Monmouth, New Jersey 07703

Commanding General
U.S. Army Electronics Command
Attn: AMSEL-NL-A
Fort Monmouth, New Jersey 07703

Commanding General
U.S. Army Electronics Command
Attn: AMSEL-NL-C
Fort Monmouth, New Jersey 07703

Commanding General
U.S. Army Electronics Command
Attn: AMSEL-NL-D (Dr H. Bennett)
Fort Monmouth, New Jersey 07703

Commanding General
U.S. Army Electronics Command
Attn: AMSEL-NL-P
Fort Monmouth, New Jersey 07703

Commanding General
U.S. Army Electronics Command
Attn: AMSEL-SC
Fort Monmouth , New Jersey 07703

Commanding General
U.S. Army Electronics Command
Attn: AMSEL-VL-D
Fort Monmouth, New Jersey 07703

Commanding General
U.S. Army Electronics Command
Attn: AMSEL-VL-F
Fort Monmouth, New Jersey 07703

Commanding General
U.S. Army Electronics Command
Attn: AMSEL-WL-D
Fort Monmouth, New Jersey 07703

Commanding General
U.S. Army Electronics Command
Attn: AMSEL-XL-DT
Fort Monmouth, New Jersey 07703

Commanding General
U.S. Army Electronics Command
Attn: AMSEL-XL-D
Fort Monmouth, New Jersey 07703

Mr Norman J. Field, AMSEL-RD-S
Chief, Office of Science & Technology
Research and Development Directorate
U.S. Army Electronics Command
Fort Monmouth, New Jersey 07703

Project Manager
Common Positioning & Navigation Systems
Attn: Harold H. Bahr (AMCPM-NS-TM),
Building 439
U.S. Army Electronics Command
Fort Monmouth, New Jersey 07703

U.S. Army Munitions Command
Attn: Science & Technology
Info Br., Bldg 59
Picatinny Arsenal, SMUPA-RT-S
Dover, New Jersey 07801

European Office of Aerospace Research
APO New York 09667

Director
Columbia Radiation Laboratory
Columbia University
538 West 120th ST
New York, N. Y. 10027

Dr John R. Ragazzini, Dean
School of Engineering & Science
New York University
University Heights
Bronx, New York 10453

Mr Jerome Fox, Research Coordinator
Polytechnic Institute of Brooklyn
333 Jay St.
Brooklyn, New York 11201

Airborn Instruments Laboratory
Deerpark, New York 11729

Dr W. R. Lepage, Chairman
Syracuse University
Dept of Electrical Engineering
Syracuse, New York 13210

Rome Air Development Center
Attn: Documents Library (EMTLD)
Griffiss Air Force Base, New York 13440

Mr H. E. Webb (EMBIS)
Rome Air Development Center
Griffiss Air Force Base, New York 13440

Professor James A. Cadzow
Department of Electrical Engineering
State University of New York at Buffalo
Buffalo, New York 14214

Dr A. G. Jordan
Head of Dept of Elec Engineering
Carnegie-Mellon University
Pittsburgh, Penn 15213

Hunt Library
Carnegie-Mellon University
Schenley Park
Pittsburgh, Penn 15213

Lehigh University
Dept of Electrical Engineering
Bethelehem, Penn 18015

Commander (ADL)
Naval Air Development Center
Attn: NADC Library
Johnsville, Warminster, Pa 18974

Technical Director (SMUFA-A2000-107-1)
Frankford Arsenal
Philadelphia, Penn 19137

Mr M. Zane Thornton, Chief, Network
Engineering, Communications and
Operations Branch, Lister Hill
National Center/ Biomedical Communications
8600 Rockville Pike
Bethesda, Maryland 20014

U.S. Post Office Dept
Library - Room 6012
12th & Pennsylvania Ave. N.W.
Washington, D.C. 20260

Technical Library
DDR&E
Room 3C-122, The Pentagon
Washington, D.C. 20301

Director for Materials Sciences
Advanced Research Projects Agency
Department of Defense
Washington, D.C. 20301

Asst Director (Research)
Rm 3C128, The Pentagon
Office of the Sec of Defense
Washington, D.C. 20301

Chief, R & D Division (340)
Defense Communications Agency
Washington, D.C. 20305

Distribution List (cont'd.)

Commanding General
U.S. Army Materiel Command
Attn: AMCRD-TP
Washington, D.C. 20315

Director, U.S. Army Material
Concepts Agency
Washington, D.C. 20315

Hq USAF (AFRDD)
The Pentagon
Washington, D.C. 20330

Hq USAF (AFRDDG)
The Pentagon
Washington, D.C. 20330

Hq USAF (AFRDSD)
The Pentagon
Washington, D.C. 20330

AFSC (SCTSE)
Andrews Air Force Base, Maryland 20331

Dr I. R. Mirman
Hq AFSC (SGGP)
Andrews AFB, Maryland 20331

Naval Ship Systems Command
Ship 031
Washington, D.C. 20360

Naval Ship Systems Command
Ship 035
Washington, D.C. 20360

Commander
U.S. Naval Security Group Command
Attn: G43
3801 Nebraska Avenue
Washington, D.C. 20390

Director
Naval Research Laboratory
Washington, D.C. 20390
Attn: Dr A. Brodizinsky, Sup. Elec Div

Director
Naval Research Laboratory
Washington, D.C. 20390
Attn: Maury Center Library (Code 8050)

Director
Naval Research Laboratory
Washington, D.C. 20390
Attn: Dr W.C. Hall, Code 7000

Director
Naval Research Laboratory
Attn: Library, Code 2029 (ONRL)
Washington, D.C. 20390

Dr G. M. R. Winkler
Director, Time Service Division
U. S. Naval Observatory
Washington, D.C. 20390

Colonel E.P. Gaines, Jr
ACDA/FO
1901 Pennsylvania Ave. N.W.
Washington, D.C. 20451

Commanding Officer
Harry Diamond Laboratories
Attn: Mr Berthold Altman (AMXDO-TI)
Connecticutt Ave & Van Ness St., N.W.
Washington, D.C. 20438

Central Intelligence Agency
Attn: CRS/ADD Publications
Washington, D.C. 20505

Dr H. Harrison, Code RRE
Chief, Electrophysics Branch
National Aeronautics & Space Admin
Washington, D.C. 20546

The John Hopkins University
Applied Physics Laboratory
Attn: Document Librarian
8621 Georgia Avenue
Silver Spring, Maryland 20910

Technical Director
U.S. Army Limited War Laboratory
Aberdeen Proving Ground
Aberdeen, Maryland 21005

Commanding Officer (AMXRD-BAT)
US Army Ballistics Research Laboratory
Aberdeen Proving Ground
Aberdeen, Maryland 21005

Electromagnetic Compatibility
Analysis Center (ECAC)
Attn: ACOAT
North Severn
Annapolis, Maryland 21402

Commanding Officer
U.S. Army Engineer Topographic Laboratories
Attn: STINFLO Center
Fort Belvoir, Virginia 22060

U.S. Army Mobility Equipment Research
and Development Center, Bldg 315
Attn: Technical Document Center
Fort Belvoir, Virginia 22060

Director (NV-D)
Night Vision Laboratory, USAECOM
Fort Belvoir, Virginia 22060

Dr Alvin D. Schnitzler
Institute for Defense Analyses
Science and Technology Division
400 Army-Navy Drive
Arlington, Virginia 22202

Director
Physical & Engineering Sciences Division
3045 Columbia Pike
Arlington, Va 22204

Commanding General
U.S. Army Security Agency
Attn: IARD-T
Arlington Hall Station
Arlington, Virginia 22212

Commanding General
USACDC Institute of Land Combat
Attn: Technical Library, Rm 636
2461 Eisenhower Avenue
Alexandria, Virginia 22314

VELA Seismological Center
300 North Washington St
Alexandria, Virginia 22314

U.S. Naval Weapons Laboratory
Dahlgren, Virginia 22448

Research Laboratories for the Eng
Sciences, School of Engineering &
Applied Science
University of Virginia
Charlottesville, Va 22903

Dr Herman Robl
Deputy Chief Scientist
U.S. Army Research Office (Durham)
Box CM, Duke Station
Durham, North Carolina 27706

Rochard O. Ulsh (CRDARD-IP)
U.S. Army Research Office (Durham)
Box CM, Duke Station
Durham, North

Richard O. Ulsh (CRDARD-IP)
U.S. Army Research Office (Durham)
Box CM, Duke Station
Durham, North Carolina 27706

ADTC (ADBPS-12)
Eglin AFB, Florida 32542

Commanding Officer
Naval Training Device Center
Orlando, Florida 32813

Technical Library, AFETR
(ETV,MU-135)
Patrick AFB, Florida 32925

Commanding General
U.S. Army Missile Command
Attn: AMSMI-RR
Redstone Arsenal, Alabama 35809

Redstone Scientific Information Center
Attn: Chief, Document Section
U.S. Army Missile Command
Redstone Arsenal, Alabama 35809

AUL3T-9663
Maxwell AFB, Alabama 36112

Hq AEDC (AETS)
Attn: Library/Documents
Arnold AFS, Tennessee 37389

Case Institute of Technology
Engineering Division
University Circle
Cleveland, Ohio 44106

NASA Lewis Research Center
Attn: Library
21000 Brookpark Road
Cleveland, Ohio 44135

Director
Air Force Avionics Laboratory
Wright-Patterson AFB, Ohio 45433

AFAL (AVTA) R.D. Larson
Wright-Patterson AFB, Ohio 45433

AFAL (AVT) Dr H.V. Noble, Chief
Electronics Technology Division
Air Force Avionics Laboratory
Wright-Patterson AFB, Ohio 45433

Dr Robert E. Fontana
Head, Dept of Elec Engineering
Air Force Institute of Technology
Wright Patterson AFB, Ohio 45433

Dept of Electrical Engineering
Clippinger Laboratory
Ohio University
Athens, Ohio 45701

Commanding Officer
Naval Avionics Facility
Indianapolis, Indiana 46241

Dr John D. Hancock, Head
School of Electrical Engineering
Purdue University
Lafayette, Ind 47907

Professor Joseph E. Rowe
Chairman,
Dept of Elec Engineering
The University of Michigan
Ann Arbor, Michigan 48104

Dr G. J. Murphy
The Technological Institute
Northwestern University
Evanston, Ill 60201

Commanding Officer
Office of Naval Research
Branch Office
219 South Dearborn St
Chicago, Illinois 60604

Illinois Institute of Technology
Dept of Electrical Engineering
Chicago, Illinois 60616

Deputy for Res. and Eng (AMSE-DRE)
U.S. Army Weapons Command
Rock Island Arsenal
Rock Island, Illinois 61201

Commandant
U.S. Army Command & General
Staff College
Attn: Acquisitions, Library Division
Fort Leavenworth, Kansas 66027

Dept of Electrical Engineering
Rice University
Houston, Texas 77001

HQ AMD (AMR)
Brooks AFB, Texas 78235

USAFSAM (SMKOR)
Brooks AFB, Texas 78235

Mr B. R. Locke
Technical Adviser, Requirements
USAF Security Service
Kelly Air Force Base, Texas 78241

Director
Electronics Research Center
The University of Texas as Austin
Eng-Science Bldg 110
Austin, Texas 78712

Department of Elec Engineering
Texas Technological University
Lubbock, Texas 79409

Commandant
U.S. Army Air Defense School
Attn: Missile Sciences Div., C&S Dept
P.O. Box 9390
Fort Bliss, Texas 79916

Director
Aerospace Mechanics Sciences
Frank J. Seiler Research Laboratory (OAR)
USAF Academy
Colorado Springs, Colorado 80840

Director of Faculty Research
Department of the Air Force
U.S. Air Force Academy
Colorado Springs, Colorado 80840

Major Richard J. Gowen
Tenure Associate Professor
Dept of Electrical Engineering
U.S. Air Force Academy
Colorado Springs, Colorado 80840

Academy Library (DFSLB)
U.S. Air Force Academy
Colorado Springs, Colorado 80840

M.A. Rothenberg (STEPD-SC(S))
Scientific Director
Desert Test Center
Bldg 100, Soldiers' Circle
Fort Douglas, Utah 84113

Utah State University
Dept of Electrical Engineering
Logan, Utah 84321

School of Engineering Sciences
Arizona State University
Tempe, Ariz 85281

Distribution List (cont'd.)

Commanding General
U.S. Army Strategic Communications Command
Attn: SCC-CG-SAE
Fort Huachuca, Arizona 85613

The University of Arizona
Dept of Electrical Engineering
Tucson, Arizona 85721

Capt C.E. Baum
AFWL (WLRE)
Kirkland AFB, New Mexico 87117

Los Alamos Scientific Laboratory
Attn: Report Library
P.O. Box 1663
Los Alamos, N.M. 87544

Commanding Officer
(AMSEL-BL-WS-R)
Atmospheric Sciences Laboratory
White Sands Missile Range
New Mexico 88002

Commanding Officer
Atmospheric Sciences Laboratory
White Sands Missile Range
New Mexico 88002

Chief, Missile Electronic Warfare
Technical Area, (AMSEL-WL-M)
U.S. Army Electronics Command
White Sands Missile Range
New Mexico 88002

Director
Electronic Sciences Lab
University of Southern California
Los Angeles, Calif 90007

Eng & Math Sciences Library
University of California at Los Angeles
405 Hilgred Avenue
Los Angeles, Calif 90024

Aerospace Corporation
P.O. Box 95085
Los Angeles, California 90045
Attn: Library Acquisitions Group

Hq SAMSO (SMTTS/Lt Belate)
AF Unit Post Office
Los Angeles, Calif 90045

Dr Sheldon J. Wells
Electronic Properties Information Center
Mail Station E-175
Hughes Aircraft Company
Culver City, California 90230

Director, USAF PROJECT RAND
Via: Aif Force Liaison Office
The RAND Corporation
Attn: Library D
1700 Main Street
Santa Monica, California 90406

Deputy Director & Chief Scientist
Office of Naval Research Branch Office
1030 East Green Street
Pasadena, California 91101

Aeronautics Library
Graduate Aeronautical Laboratories
California Institute of Technology
1201 E. California Blvd
Pasadena, California 91109

Professor Nicholas George
California Institute of Technology
Pasadena, Califonria 91109

Commanding Officer
Naval Weapons Center
Corona Laboratories
Attn: Library
Corona, California 91720

Dr F. R. Charvat
Union Carbide Corporation
Materials Systems Division
Crystal Products Dept
8888 Balboa Avenue
P.O. Box 23017
San Diego, California 92123

Hollander Associates
P.O. Box 2276
Fullerton, California 92633

Commander, U.S. Naval Missile Center (56322)
Point Mugu, California 93041

W.A. Eberspacher, Associate Head
Systems Integration Division
Code 5340A,Box 15
U.S. Naval Missile Center
Point Mugu, California 93041

Sciences-Engineering Library
University of California
Santa Barbara, California 93106

Commander (Code 753)
Naval Weapons Center
Attn: Technical Library
China Lake, California 93555

Library (Code 2124)
Technical Report Section
Naval Postgraduate School
Monterey, California 93940

Glen A. Myers (Code 52Mv)
Assoc Professor of Elec Eng
Naval Postgraduate School
Monterey, California 93940

Dr Leo Young
Stanford Research Institute
Menlo Park, California 94025

Lenkurt Electric Co., Inc.
1105 County Road
San Carlos, California 94070
Attn: Mr E.K. Peterson

Director
Microwave Laboratory
Stanford University
Stanford, California 94305

Director
Stanford Electronics Laboratories
Stanford University
Stanford, California 94305

Director
Electronics Research Laboratory
University of California
Berkeley, California 94720

ADDENDUM

Dr Joel Trimble, Code 437
Information Systems Branch
Office of Naval Research
Department of the Navy
Washington, D.C. 20360

U.S. Naval Oceanographic Office
Attn: M. Rogofsky, Librarian (Code640)
Washington, D.C. 20390

CORRECTION

Director, Electronic Programs
Attn: Code 427
Office of Naval Research
Department of the Navy
Washington, D.C. 20360 2 copies

DELETE

Technical Director
U.S. Army Limited War Laboratory
Aberdeen Proving Ground
Aberdeen, Maryland 21005

REPLACE WITH

Technical Director
U.S. Army Land Warfare Laboratory
Aberdeen Proving Ground
Aberdeen, Maryland 21005

DELETE

USAF European Office of Aerospace Research
APO New York 09667

REPLACE WITH

European Office of Aerospace Research
Technical Information Office
Box 14, FPO New York 09510

DELETE

Dr John R. Raggazzini, Dean
School of Engineering and Science
New York University
University Heights
Bronx, New York 10453

REPLACE WITH

New York University
Engineering Library
Bronx, New York 10453

Security Classification

DOCUMENT CONTROL DATA - R & D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1. ORIGINATING ACTIVITY (Corporate author) University of Illinois Coordinated Science Laboratory Urbana, Illinois 61801	2a. REPORT SECURITY CLASSIFICATION 2b. GROUP

3. REPORT TITLE

L-STEP MAJORITY LOGIC DECODING

4. DESCRIPTIVE NOTES (Type of report and inclusive dates)

5. AUTHOR(S) (First name, middle initial, last name)

CHIEN, Robert T. & NG, Spencer W.

6. REPORT DATE	7a. TOTAL NO. OF PAGES	7b. NO. OF REFS
June, 1970	36	27

8a. CONTRACT OR GRANT NO. DAAB 07-67-C-0199; also in part Rome Air b. Development Center Contract No. F30602- 70-C-0014 (EMKC). c. d.	9a. ORIGINATOR'S REPORT NUMBER(S) R-477 9b. OTHER REPORT NO(S) (Any other numbers that may be assigned this report) UILU-ENG 70-222

10. DISTRIBUTION STATEMENT

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

11. SUPPLEMENTARY NOTES	12. SPONSORING MILITARY ACTIVITY
	Joint Services Electronics Program thru U.S. Army Electronics Command Fort Monmouth, New Jersey 07703

13. ABSTRACT

NONE

Security Classification

14 KEY WORDS	LINK A		LINK B		LINK C	
	ROLE	WT	ROLE	WT	ROLE	WT
Error-Correcting Codes						
Decoding						
Majority Decoding						
Threshold Decoding						
L-Step Decoding						
Geometric Codes						
Hamming Codes						
Reed-Solomon Codes						
Cyclic Codes						

Security Classification