Error-Correcting Codes — A Linear Programming Approach

By E. J. McCLUSKEY, JR.

(Manuscript received June 5, 1959)

Two theorems are proved that characterize the matrices used to construct systematic error-correcting codes. A lower bound on the number of required check bits is derived, and it is shown that, in certain cases, this bound for systematic codes is identical with Plotkin's bound on the size of any error-correcting code. A linear program whose solutions correspond directly to a minimum-redundancy error-correcting code is derived. This linear program can be solved by an algorithm that is essentially the simplex method modified to produce integer solutions. Explicit solutions in closed form that specify the codes directly are derived for the cases when the specified code parameters satisfy certain restrictions. Several theorems are proved about minimum redundancy codes with related parameters.

I. INTRODUCTION

This paper is concerned with the problem of transmitting binary signals over a noisy channel. Some situations in which this problem occurs are: when telephone lines are being used to transmit data in binary form; when an imperfect medium such as magnetic tape or a photographic emulsion is used to store binary data; or when operations on binary signals are being carried out by means of circuits constructed of devices such as relays, diodes or transistors, which have a probability of error. It has been shown by Shannon[1] that it is possible to add redundant bits to the transmitted messages so as to reduce the probability of error in the received messages to an arbitrarily small quantity. Since Shannon did not exhibit efficient codes for achieving this reduction in error probability, considerable attention has been devoted to the search for useful coding schemes. The usefulness of a coding scheme is determined by the number of redundant bits that must be added, by the complexity of the equipment required for inserting the redundant bits before transmission and for removing the redundant bits and correcting errors after transmission, and by the error-correcting capabilities.

In 1950, Hamming[2] published schemes for constructing codes for (a) detecting the presence of an error in one out of n bits, (b) correcting an error in one out of n bits or (c) correcting an error in one out of n bits *and* detecting errors in two out of n bits. In all these codes, it is possible to separate the transmitted message into information or message bits and redundant or check bits. Hamming defined codes that have this property as *systematic* codes, and proved that all systematic codes can be constructed by means of parity constraints on the transmitted bits. He also proved that the codes that he constructed contained the minimum number of check or redundant bits. While Hamming did not obtain any codes for correcting more than one error, he did show that a code for correcting e errors can always be changed into a code for correcting e errors *and* detecting $e + 1$ errors by adding one extra check bit that makes the over-all parity of the transmitted message always even.

A procedure for constructing codes for multiple errors was obtained by Reed[3] and Muller.[4] The resulting codes are commonly called Reed-Muller codes, since they were obtained independently by both Reed and Muller. A Reed-Muller code can be constructed for detecting e errors whenever e is a power of two ($e = 2^x$). The number of bits in the resulting code will also be a power of two. This paper presents a method for constructing minimum-redundancy codes for correcting or detecting any specified number of errors.

II. THE HAMMING MATRIX

A *binary word* is defined as a sequence of n binary digits, $x = x_1x_2 \cdots x_n$; and the *distance* between two binary words is defined as $d(x, y) = (x_1 \oplus y_1) + (x_2 \oplus y_2) + \cdots + (x_n \oplus y_n)$,* which is equal to the number of bit locations in which the two words differ. An *e-error-correcting code*[2] is a collection of binary words for which the distance between any two words is greater than or equal to $2e + 1$. If an error-correcting code consists of all binary words whose digits satisfy certain parity-check requirements, the code is called a *systematic error-correcting code.* For example, the collection of six-bit binary words that satisfy $x_3 \oplus x_4 \oplus x_5 = 0$, $x_2 \oplus x_4 \oplus x_6 = 0$ and $x_1 \oplus x_5 \oplus x_6 = 0$ forms a one-error-correcting code. The problem of obtaining a systematic error-correcting code is equivalent to that of finding a set of parity-check requirements that will generate a set of words with the required distance property.

The parity-check requirements can be specified by a matrix of zeros and ones in which the jth column corresponds to the jth bit of the

* The symbol $\oplus$ represents addition modulo two.

binary code words and the ith row corresponds to the ith parity check. The entry in the ith row and jth column is one if the jth bit is involved in the ith parity check and is zero otherwise. This matrix will be called a *Hamming matrix*, and its elements will be represented by the symbol h_{ij}. This is the Hamming matrix for parity rules $x_3 \oplus x_4 \oplus x_5 = 0$, $x_2 \oplus x_4 \oplus x_6 = 0$, $x_1 \oplus x_5 \oplus x_6 = 0$:

$$\begin{array}{c} \begin{array}{cccccc} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \end{array} \\ \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \end{array} = [h_{ij}].$$

The first problem considered in this paper is that of characterizing Hamming matrices by determining the necessary and sufficient conditions that a matrix of zeros and ones be a Hamming matrix for a code with minimum distance d (between any two code words).

In the following, the binary code words will be represented by column matrices,

$$x] = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix},$$

and the *Boolean product* of two matrices with elements a_{ij} and b_{ij} will be defined as a matrix $[c_{ij}] = [a_{ij}] \circ [b_{ij}]$ with elements $c_{ij} = \sum_k a_{ik}b_{kj}$ (modulo 2).

Example 1:

$$\begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{bmatrix} \circ \begin{bmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

Definition: A matrix of zeros and ones with k rows and n columns is the *Hamming matrix for a code of minimum distance* d if and only if $d(x, y) \geqq d$ for all x and y $(x \neq y)$ for which $[H]\circ x] = 0]$ and $[H]\circ y] = 0]$, where $0]$ represents a column matrix of k zeros.

Definition: The *weight of a matrix*, $w[a_{ij}]$, is equal to the number of entries of the matrix which are equal to one (for matrices of only zeros and ones).

Lemma 1: $d(0, x) = w[x]$, where 0 represents a sequence of n zeros.

Definition: The *sum (modulo 2) of two or more columns of a matrix* is the column matrix with each element equal to the sum modulo 2 of the elements in the same row of the columns being summed.

Lemma 2: If $d(x, y) = d_1$, then $y] = x \oplus z]$, where $w[z] = d_1$.

Theorem 1: H is the Hamming matrix for a code of minimum distance, d, if and only if $[H]\circ z] \neq 0]$ for all $z]$ $(z] \neq 0])$ for which $w[z] < d$.

Proof: First suppose the H is a Hamming matrix for a code of minimum distance d and that $w[z] < d$; then $[H]\circ 0] = 0]$ and $d(0, z) < d$, so that $[H]\circ z]$ cannot equal $0]$, by the definition of a Hamming matrix. Next suppose that $[H]\circ z] \neq 0]$ for all $z]$ $(z] \neq 0])$ for which $w[z] < d$, and $d(x, y) < d$. Then $y]$ can be expressed as $x \oplus z]$, where $w[z] < d$; and $[H]\circ y] = [H]\circ x \oplus z] = [H]\circ x] + [H]\circ z]$. Thus, if x is a code word, $[H]\circ x] = 0]$, y cannot be a code word, since $[H]\circ y] = [H]\circ x] + [H]\circ z] = 0] + [H]\circ z] \neq 0]$. This shows that, if $[H]\circ z] \neq 0$ for all $z]$ with $w[z] < d$, then $d(x, y)$ must be equal to or greater than d for all x and y with $[H]\circ x] = 0$ and $[H]\circ y] = 0$.

Corollary 1: H is the Hamming matrix for a code of minimum distance d if and only if no set of $d - 1$ or fewer columns sums to the all-zero column.

Proof: If $d - 1$ or fewer columns sum to zero there is a corresponding z with $w[z] < d$ such that $[H]\circ z] = 0]$.

This theorem makes it possible to attack the problem of finding a systematic code with the specified d by constructing a matrix satisfying the given conditions. However, no satisfactory procedure for constructing such a matrix directly is known, and the construction procedure to be developed here is based on Theorem 2, which characterizes the parity-check matrix, a submatrix of the Hamming matrix.

III. THE PARITY-CHECK MATRIX

Hamming showed that a Hamming matrix can always be put in the form of a $k \times k$ unit matrix (matrix with ones on the main diagonal and zeros elsewhere) and a $k \times n - k$ arbitrary matrix called the *parity-check matrix* (see Ref. 2, Section 7). This form of the Hamming matrix will be called the *standard form.* In the following it will be assumed that the Hamming matrices are always in standard form.

It is customary to use the term redundant bits or *check bits* for the bits of the code words which correspond to columns of the unit matrix part of the Hamming matrix. The remaining $n - k = m$ bits are called *information* or *message* bits. This usage derives from the fact that each of the check bits occurs in only one of the parity checks, and therefore the values of each check bit can be calculated directly from the values of the information bits, independent of the values of the other check bits. If the elements of the parity-check matrix are denoted by p_{ij}, the check bits (u_i) are obtained from the message bits (x_j) according to the following expression:

$$u_i = \sum_{j=1}^{m} p_{ij}\, x_j \quad \text{(modulo 2)}. \tag{1}$$

A systematic error-correcting code is thus completely specified by the parity-check matrix. The main object of this paper is to present methods for obtaining parity-check matrices corresponding to systematic codes that have a specified minimum distance d between any pair of code words and requiring the minimum number of check bits.

The following is an example of a systematic code of minimum distance 3 (one-error-correcting code) having two message bits and three check bits.

Example 2:

Matrix:

$$P = \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix};$$

equations:

$$\begin{aligned} u_1 &= x_1 \oplus x_2 , \\ u_2 &= x_1 , \\ u_3 &= x_2 ; \end{aligned}$$

code:

$$\begin{array}{ccccc} u_1 & u_2 & u_3 & x_1 & x_2 \\ \end{array}$$
$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

The method to be used for constructing parity-check matrices depends on the following theorem.

Theorem 2: P is a parity-check matrix for a code of minimum distance d if and only if:

i. the weight of each column of P is greater than or equal to $d - 1$;

ii. the weight of the sum (modulo 2) of J columns is greater than or equal to $d - J$.

Proof: First, suppose that the conditions of the theorem are not satisfied, and consider the Hamming matrix made up of a unit matrix and the given P matrix. If there is a column of P with weight $w_1 < d - 1$, then the sum of this column and w_1 of the unit columns (one unit column for each one entry of the column of P) will be equal to zero. Since the total number of columns involved in this sum is $w_1 + 1 < d$, the conditions of the Corollary 1 are violated and P cannot correspond to a code of minimum distance d. Similarly, if the sum of J columns has weight $w_J < d - J$, these J columns of P plus w_J unit columns will sum to the all-zero column. The total number of columns summed is $J + w_J < J + d - J = d$, again violating the conditions of the Corollary 1. Thus, unless conditions i and ii are satisfied by P it cannot be the parity-check matrix for a code of minimum distance d.

Next, suppose that conditions i and ii of this theorem are satisfied, and consider which combinations of columns will sum to the all-zero column. No combination involving only unit columns can sum to zero, since these are linearly independent. As discussed in the preceding paragraph, any combination involving only one of the columns of the P matrix will contain $w_1 + 1 \geqq d$ columns, and any combination involving more than one of the columns of the P matrix will contain $J + w_J \geqq J + d - J = d$ columns. Thus, any combination of columns that sums to the all-zero column must involve at least d columns. The conditions of Corollary 1 are satisfied and P corresponds to a code of minimum distance d.

In this paper the construction of error-correcting codes will be based on finding matrices which satisfy the conditions of Theorem 2. The matrices will be obtained directly from the solutions to a set of linear inequalities.

IV. FORMATION OF LINEAR PROGRAM

In order to check that a given matrix P satisfies the conditions of Theorem 2, it is necessary to form the sums modulo 2 of all pairs of columns of P, compute the weights, and compare the weights with $d - 2$; then this must be repeated for all triples of columns, comparing with $d - 3$; all quadruples of columns, comparing with $d - 4$, etc. A systematic procedure for doing this can be given in terms of the following definition.

Definition: P_J $(J = 1, 2, \cdots m)$ is the matrix formed from P by taking, as the columns of P_J, the sums of all possible combinations of J columns of P (P_1 is identical with P).

Example 3: P is the parity check matrix for a code of minimum distance 3 since the weight of each column of P is at least $3 - 1 = 2$, and the weight of each column of P_2 is at least $3 - 2 = 1$:

$$\underset{\text{(a)}P}{\begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}} \quad \underset{\text{(b)}P_2}{\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}} \quad \underset{\text{(c)}P_3}{\begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}} \quad \underset{\text{(d)}P_4}{\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}}.$$

A method for checking a matrix P is to form $P_2, P_3, \cdots$ and then to verify that the weight of each column of P_J is at least $d - J$. While this method is quite satisfactory for verifying that a given matrix satisfies the conditions for a parity-check matrix of a code of minimum distance d, it is of little use for the more important problem of constructing a matrix satisfying these conditions. For this reason, a modified method for testing a matrix will be presented as a preliminary to the discussion of methods for constructing parity-check matrices.

In any $k \times m$ parity-check matrix there are only $2^m - 1$ different rows that can occur, since the all-zero row never appears in such a matrix. This does not mean that the total number of rows cannot be larger than $2^m - 1$, since the same row may appear more than once. For any given m, it is possible to compute the rows of $P_2, P_3, \cdots, P_m$ that correspond to each possible row of P. Any specific P matrix with m columns can then be tested by selecting the appropriate P_J rows, taking into account any multiple occurrences of rows in the P matrix being tested. This procedure can be stated more precisely in terms of the following definitions.

Definition: P^m is the matrix having m columns (and $2^m - 1$ rows) in which each possible m-bit binary word, except the all-zero word, appears exactly once. The rows are ordered in the following fashion:

First, all the rows containing a single one are written down. These rows are ordered so that, when the rows are interpreted as binary numbers, they occur in decreasing arithmetic order (this means that the first m rows form a unit matrix). Next, the rows containing exactly two ones are written down, with these rows arranged so that they occur in decreasing arithmetic order. This procedure is repeated by writing down the rows with three ones, four ones, etc. until finally the row with m ones is written down. Within each set of rows that all contain the same number of ones, the rows are arranged in decreasing arithmetic order.

Example 4:

$$P^3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}, \qquad P^4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}.$$

By making use of this definition of P^m, a concise specification of any P matrix having m columns can be given by listing which rows of P^m occur in P.

Definition: If P is a parity-check matrix having m columns, then $z_i(P)$, $i = 1, 2, \cdots 2^m - 1$, is equal to the number of times that the ith row of P^m occurs in P. Usually $z_i(P)$ will be written simply as z_i when the appropriate P is clear from the context.

Example 5:

$$P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \qquad \begin{aligned} z_1(P) &= 1 \\ z_2(P) &= 2 \\ z_3(P) &= 0\,. \\ z_4(P) &= 0 \\ z_5(P) &= 1 \\ z_6(P) &= 0 \\ z_7(P) &= 1 \end{aligned}$$

It is now possible to state the requirements for parity-check matrices in terms of $z_i(P)$, P^m and $P_J{}^m$, where $P_J{}^m$ is the matrix formed of all sums of J columns of P^m.

Theorem 3: A matrix P with each entry equal to zero or one is a parity-check matrix for a code of minimum distance d if and only if

$$[z_1(P)\ z_2(P)\ \cdots\ z_{2^m-1}(P)]\ [P_J{}^m] \geqq [d - J, d - J, \cdots, d - J]^* \tag{2}$$

for $1 \leqq J \leqq m$.

Proof: For $J = 1$,

$$[z_1(P)\ z_2(P)\ \cdots\ z_{2^m-1}(P)]\ [P_1{}^m]$$

is just equal to the weights of the columns of P, since each row of P^m is multiplied by the number of times it occurs in P $[z_i(P)]$ and then a sum for each column is formed. Similarly, for $J \neq 1$,

$$[z_i(P)\ z_2(P)\ \cdots\ z_{2^m-1}(P)]\ [P_J{}^m]$$

is equal to the weights of the columns of P_J. By Theorem 1, these weights must be greater than or equal to $d - J$.

* The multiplication here is ordinary matrix multiplication. The inequality is satisfied if, and only if, each element of the row matrix obtained by the multiplication is at least as large as the corresponding element of the row matrix given on the right side of the inequality.

Example 6:

$$P = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}, \qquad \begin{array}{l} z_1 = 0 \\ z_2 = 0 \\ z_3 = 0, \\ z_4 = 1 \\ z_5 = 1 \\ z_6 = 1 \\ z_7 = 1 \end{array}$$

$$[z_1 z_2 \cdots z_7] \cdot [P_1^3] = [0001111] \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} = [333] \geqq [d-1, d-1, d-1],$$

$$[z_1 z_2 \cdots z_7] \cdot [P_2^3] = [0001111] \cdot \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} = [222] \geqq [d-2, d-2, d-2],$$

$$[z_1 z_2 \cdots z_7] \cdot [P_3^3] = [0001111] \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = [1] \geqq [d - 3].$$

Thus, P is the parity-check matrix for a code of minimum distance 4.

Theorem 3 is merely a restatement of Theorem 2 using different notation. The reason for introducing this new notation is that, by means of Theorem 3, the problem of constructing minimum redundancy codes can be formulated as an integer linear programming problem.

Lemma 3:

$$k = \sum_{i=1}^{2^m-1} z_i .$$

Proof: By definition, k equals the number of rows in the matrix P and z_i equals the number of times that row i of P^m occurs in P. Since each row of P is identical with some row of P^m, the total number of rows of P just equals

$$\sum_{i=1}^{2^m-1} z_i \, .$$

Theorem 4: The problem of finding a minimum-redundancy, systematic, error-collecting code for specified values of m (the number of message bits) and d (the minimum distance between any pair of code words) is equivalent to the problem of solving the following linear program:

minimize:

$$k = \sum_{i=1}^{2^m-1} z_i$$

subject to: (LP)

(1) z_i integers,

(2) $z_i \geqq 0$,

(3) $[z_1 \, z_2 \cdots z_{2^m-1}] \cdot [P_J{}^m] \geqq [d - J, d - J, \cdots, d - J]$ for $J = 1, 2, \cdots m$.

Proof: The solution to (LP) will be a set of values for $z_1 , z_2 , \cdots, z_{2^m-1}$. These values can be used to construct a matrix P by interpreting them as $z_i(P)$. By Theorem 3, these values for $z_i(P)$ must satisfy (LP-3) and by the definition of $z_i(P)$ they must satisfy (LP-1, 2). Since a minimum-redundancy code is desired, it is necessary to minimize k. Lemma 3 establishes the expression for k in terms of $z_i(P)$.

The remainder of this paper will consist mainly of obtaining solutions to this linear program.

V. BOUNDS ON REDUNDANCY

In a certain sense, the formulation of (LP) solves the problem of constructing the desired codes, since a numerical procedure exists for solving this type of integer linear program.[5] Practically, this procedure is of limited usefulness, since the size of the program to be solved soon exceeds the capability of the largest electronic computer. Also, numerical solutions do not provide information about the interrelations among various codes with different parameters. A much more desirable solution would be a closed solution of (LP) in which the values of $z_1, z_2, \cdots, z_{2^m-1}$ and k are expressed as functions of m and d. The derivation of such closed solutions and of various properties relating solutions for different parameters will constitute the remainder of this paper.

The first step in obtaining solutions of (LP) will be to remove the matrix notation and express (LP-3) as a set of simultaneous inequalities. This is done to simplify the proofs of the theorems to follow.

The inequalities represented by (LP-3) can be expressed in terms of a single matrix by defining a matrix A^m in which all of the columns of $P_1^m, P_2^m, \cdots, P_m^m$ appear.[6]

Definition: The matrix A^m is formed as follows:

(1) The first m columns of A^m are identical with P^m.

(2) The jth column of A^m ($j > m$) is formed by taking the sum modulo 2 of the columns of P^m that have one entries in the jth *row* of P^m. When the value of m is clear from the context, A^m will be written as A.

Example 7: For $m = 3$,

$$P^3 = \left[\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{array}\right]\begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \end{array}, \qquad A^3 = \begin{array}{c} \begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array} \\ \left[\begin{array}{ccccccc} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right] \end{array}.$$

The fifth column of A^3 is formed from the sum modulo 2 of the first and third columns of P^3 since the fifth row of P^3 has ones in the first and third columns, etc.

Definition: Let $\epsilon_j(m)$ be defined as follows:

$$\epsilon_j(m) = 1 \qquad \text{for} \quad 1 \leqq j \leqq m,$$

$$\epsilon_j(m) = 2 \qquad \text{for} \quad 1 + m \leqq j \leqq m + \binom{m}{2},$$

$$\epsilon_j(m) = s \qquad \text{for} \quad \sum_{\nu=0}^{s-1} \binom{m}{\nu} \leqq j \leqq \sum_{\mu=1}^{s} \binom{m}{\mu},$$

$$\epsilon_j(m) = m \qquad \text{for} \quad \sum_{\nu=0}^{m-1} \binom{m}{\nu} \leqq j \leqq 2^m - 1.$$

Theorem 3 can be stated in terms of A^m as follows:

Theorem 3': A matrix P is a parity-check matrix for a code of minimum distance d if and only if:

$$[z_1(P)\ z_2(P)\ \cdots\ z_{2^m-1}(P)] \cdot [A^m] \geqq [w_1\ w_2\ \cdots\ w_{2^m-1}], \qquad (2')$$

where $w_j = d - \epsilon_j(m)$.

Some properties of A^m are stated in the following lemmas, in which $a_{ij}{}^m$ represents the element of the ith row and jth column of A^m. When there is no ambiguity possible, $a_{ij}{}^m$ is written simply as a_{ij}. Proofs will be given in the Appendix.

Lemma 4: The matrix A^m can be partitioned into submatrices as follows:

$$A^m = [P_1{}^m \vdots P_2{}^m \vdots P_3{}^m \vdots \cdots \vdots P_m{}^m].$$

Lemma 5:

$$a_{ij} = a_{i1}a_{j1} \oplus a_{i2}a_{j2} \oplus \cdots \oplus a_{im}a_{jm} \qquad \text{for} \quad j > m.$$

Lemma 6: The transpose of A is identical with A: $A^T = A$, or $a_{ji} = a_{ij}$.

Lemma 7:

$$\sum_{i=1}^{2^m-1} a_{ij}{}^m = \sum_{j=1}^{2^m-1} a_{ij}{}^m = 2^{m-1}.$$

Lemma 8:

$$\sum_{i=1}^{m} a_{ij}{}^m = \epsilon_j(m).$$

Lemma 9: The inverse of A, A^{-1}, is obtained from A by replacing each one entry of A by 2^{1-m} and replacing each zero entry by -2^{1-m}:

$$\begin{aligned} a_{ij}{}^{-1} &= 2^{1-m} \quad \text{if} \quad a_{ij} = 1, \qquad \text{and} \\ a_{ij}{}^{-1} &= -2^{1-m} \quad \text{if} \quad a_{ij} = 0. \end{aligned}$$

Theorem 3 can be stated directly in terms of the $a_{ij}{}^m$ as follows:

Theorem 3″: A matrix P is a parity-check matrix for a code of minimum distance d if and only if:

$$\sum_{i=1}^{2^m-1} a_{ij}z_i \geqq w_j, \qquad (2'')$$

where $w_j = d - \epsilon_j(m)$.

The corresponding formulation for the program (LP) is

minimize:

$$k = \sum_{i=1}^{2^m-1} z_i$$

subject to:

$$(1)\ z_i \text{ integers},\qquad \text{(LP}')$$

$$(2)\ z_i \geqq 0,$$

$$(3)\ \sum_{i=1}^{2^m-1} a_{ij}z_i \geqq w_j\,,$$

where $w_j = d - \epsilon_j(m)$.

The following theorem presents a lower bound on k, the number of check bits that are required for specified values of m, the number of information bits and d, the minimum distance between code words.

Theorem 5: For an error-correcting code having minimum distance d and m message bits, the number of check bits, k, must satisfy

$$k \geqq \left(\frac{2^m - 1}{2^{m-1}}\right) d - m. \tag{3}$$

Proof: By (2″),

$$\sum_{i=1}^{2^m-1} a_{ij}z_i \geqq w_j\,,$$

$$\sum_{j=1}^{2^m-1} \sum_{i=1}^{2^m-1} a_{ij}z_i \geqq \sum_{j=1}^{2^m-1} w_j\,,$$

$$\sum_{i=1}^{2^m-1} \sum_{j=1}^{2^m-1} a_{ij}z_i \geqq \sum_{j=1}^{2^m-1} w_j\,,$$

$$\sum_{i=1}^{2^m-1} z_i \sum_{j=1}^{2^m-1} a_{ij} \geqq \sum_{j=1}^{2^m-1} w_j\,.$$

But, by Lemma 7,

$$\sum_{j=1}^{2^m-1} a_{ij} = 2^{m-1},$$

so

$$2^{m-1} \sum_{i=1}^{2^m-1} z_i \geqq \sum_{j=1}^{2^m-1} w_j\,,$$

and

$$k = \sum_{i=1}^{2^m-1} z_i \geqq 2^{1-m} \sum_{j=1}^{2^m-1} w_j\,, \quad \text{by Lemma 3.} \tag{i}$$

By the definition of w_j,

$$\sum_{j=1}^{2^m-1} w_j = \sum_{s=1}^{m} \binom{m}{s} d - \binom{m}{s} s = (2^m - 1)\, d - \sum_{s=1}^{m} \binom{m}{s} s \tag{ii}$$

but

$$\sum_{s=1}^{m} \binom{m}{s} s = m2^{m-1},$$

so

$$\sum_{j=1}^{2^m-1} w_j = (2^m - 1) d - m2^{m-1}.$$

Substituting this in (i) yields

$$k \geqq 2^{1-m}[(2^m - 1)\, d - m2^{m-1}]$$

or

$$k \geqq \left(\frac{2^m - 1}{2^{m-1}}\right) d - m.$$

Since the total number of bits in each code word, n, is just equal to $m + k$, this bound on k yields a bound on n.

Corollary 2: For an error-correcting code having minimum distance d and m message bits, the total number of bits in each code word must satisfy:

$$n \geqq \left(\frac{2^m - 1}{2^{m-1}}\right) d. \tag{4}$$

If $d < m$, the bounds given in (3) and (4) can be improved, since some of the w_j in (2″) will be negative and should be replaced by zeros.

Corollary 3: When $d < m$, k and n must satisfy the following inequalities:

$$k \geqq \left(\frac{2^m - 1}{2^{m-1}}\right) d - m + 2^{1-m} \sum_{s=d+1}^{m} \binom{m}{s} (s - d), \tag{3′}$$

$$n \geqq \left(\frac{2^m - 1}{2^{m-1}}\right) d + 2^{1-m} \sum_{s=d+1}^{m} \binom{m}{s} (s - d) \tag{4′}$$

Proof: From (ii) of Theorem 5,

$$\sum_{j=1}^{2^m-1} w_j = \sum_{s=1}^{m} \binom{m}{s} (d - s),$$

but when $w_j < 0$ it can be replaced by 0. This is equivalent to defining $w_j' = d - \epsilon_j(m)$ for $d \geqq \epsilon_j(m)$ and $w_j' = 0$ for $d < \epsilon_j(m)$. Then,

$$\sum_{j=1}^{2^m-1} w_j' = \sum_{s=1}^{d} \binom{m}{s} (d - s) \qquad \text{for } d < m,$$

or

$$\sum_{j=1}^{2^m-1} w_j' = \sum_{s=1}^{m} \binom{m}{s} (d - s) + \sum_{s=d+1}^{m} \binom{m}{s} (s - d) \qquad \text{for } d < m$$

$$= (2^m - 1)\, d - m2^{m-1} + \sum_{s=d+1}^{m} \binom{m}{s} (s - d).$$

By (i) of Theorem 5,

$$\begin{aligned} k &\geqq 2^{1-m} \sum_{j=1}^{2^m-1} w_j \\ &\geqq 2^{1-m} \sum_{j=1}^{2^m-1} w_j' \\ &\geqq 2^{1-m} \left[(2^m - 1)\, d - m2^{m-1} + \sum_{s=d+1}^{m} \binom{m}{s} (s - d) \right] \\ &\geqq \left(\frac{2^m - 1}{2^{m-1}} \right) d - m + 2^{1-m} \sum_{s=d+1}^{m} \binom{m}{s} (s - d). \end{aligned}$$

Whenever $d \neq h2^{m-1}$, the bounds (3) and (4) are not integers and therefore cannot be met exactly.

Definition: Let $\{N\}$ equal N if N is an integer and equal the smallest integer larger than N if N is not an integer.

Definition: Let

$$k^*(m,d) = \left\{ \left(\frac{2^m - 1}{2^{m-1}} \right) d - m \right\}$$

and

$$n^*(m,d) = \left\{ \left(\frac{2^m - 1}{2^{m-1}} \right) d \right\}.$$

Since the total number of bits per code word and the number of check bits must both be integers, the following inequalities follow directly from Theorem 5 and Corollary 2.

Corollary 4: For an error-correcting code of minimum distance d and having m message bits:

$$k \geqq k^*$$

and

$$n \geqq n^*$$

VI. MINIMUM-REDUNDANCY CODES

Since n and k must be integers, the bounds given by (2) and (3) can be met exactly only when d is divisible by 2^{m-1}, that is, when d can be written as $d = h2^{m-1}$, where h is a positive integer. The following theorem shows that the bounds can always be achieved in these cases. The appropriate P matrix is formed by including each possible distinct row h times, except for rows of weight one, which are included only $h - 1$ times.

Theorem 6: Whenever $d = h2^{m-1}$, where h is any positive integer, a minimum-redundancy code exists with

$$k = h(2^m - 1) - m,$$
$$n = h(2^m - 1)$$

and

$$\begin{aligned} z_i &= h - 1 && \text{for } 1 \leqq i \leqq m \\ &= h && \text{for } m + 1 \leqq i \leqq 2^m - 1. \end{aligned}$$

Proof: Let $z_i = h - 1$ for $1 \leqq i \leqq m$ and $z_i = h$ for $m + 1 \leqq i \leqq 2^m - 1$. Then,

$$\sum_{i=1}^{2m-1} a_{ij}z_i = \sum_{i=1}^{2m-1} ha_{ij} - \sum_{i=1}^{m} a_{ij},$$

$$\sum_{i=1}^{2m-1} ha_{ij} = h \sum_{i=1}^{2m-1} a_{ij} = h2^{m-1} \quad \text{by Lemma 7},$$

$$\sum_{i=1}^{m} a_{ij} = \epsilon_j(m) \quad \text{by Lemma 8}.$$

Thus,

$$\sum_{i=1}^{2m-1} a_{ij}z_i = h2^{m-1} - \epsilon_j(m).$$

But, by Theorem 3″, this is exactly the condition for a code of minimum distance $h2^{m-1}$.

The number of check bits, k, is given by

$$k = \sum_{i=1}^{2m-1} z_i = \sum_{i=1}^{2m-1} h - \sum_{i=1}^{m} (1)$$
$$= h(2^m - 1) - m.$$

By Theorem 5,

$$k \geqq \left(\frac{2^m - 1}{2^{m-1}}\right)(h2^{m-1}) - m$$

$$\geqq (2^m - 1)\, h - m.$$

Therefore, the code is a minimum-redundancy code.

Example 8: For $m = 3$, $d = 8 = h \cdot 2^{m-1} = 2 \cdot 2^{3-1}$:

$$k = h(2^m - 1) - m = 2(2^3 - 1) - 3 = 11,$$

$$P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

and

$$z_1 = z_2 = z_3 = 1,$$

$$z_4 = z_5 = z_6 = z_7 = 2.$$

Theorem 5 can be extended to the case when $d = h2^{m-1} - 1$ by means of the following theorem, which has originally proved by Hamming.[2]

Theorem 7 (Hamming): From any minimum-redundancy code* containing n bits per code word and having minimum distance d, with d an even number, it is possible to obtain a minimum-redundancy code containing $n - 1$ bits per code word and having minimum distance $d - 1$ by removing one of the bits from each of the code words (the same bit must be removed from each word). If the original code was a systematic code, the bit removed should be one of the check bits.

Conversely, from any minimum-redundancy code† containing n bits per code word and having minimum distance d, with d an odd number, it is possible to obtain a minimum-redundancy code with $n + 1$ bits per code word and having minimum distance $d + 1$. This is done by

* Not necessarily a systematic code.

adding a check bit that is a parity check over all of the bits of each code word.

Corollary 5: If $z_1, z_2, \cdots, z_{2^m-1}$ specify a minimum-redundancy systematic code for d, where d is an even number, it is possible to obtain a minimum-redundancy code for $d - 1$ by decreasing any nonzero z_i by one.

Corollary 6: Whenever $d = h2^{m-1} - 1$, where h is any positive integer, a minimum-redundancy code exists with

$$k = h(2^m - 1) - (m - 1),$$

$$n = h(2^m - 1) - 1.$$

This follows directly from Theorem 7 and Corollary 5.

There is a large class of codes for which

$$\left(\frac{2^m - 1}{2^{m-1}}\right) d$$

is not an integer, but for which minimum-redundancy codes with $k = k^*$ can be derived.

Theorem 8: Whenever $d = h_1 2^{m-1} - 2^{h_2}$, where h_1 is a positive integer and h_2 is a positive integer with $h_2 < m - 1$, there exists a minimum-redundancy code with

$$\begin{aligned} k &= h_1(2^m - 1) - 2^{h_2+1} - m + 1, \\ n &= h_1(2^m - 1) - 2^{h_2+1} + 1 \end{aligned}$$

and

$$z_i = z_i' - z_i'',$$

where

$$\begin{aligned} z_i' &= h_1 - 1 && \text{for } 1 \leqq i \leqq m \\ &= h_1 && \text{for } m + 1 \leqq i \leqq 2^m - 1, \end{aligned}$$

and

$$\begin{aligned} z_i'' &= 1 \text{ if the corresponding row of } A^m \text{ has all zeros in its first } m - h_2 - 1 \text{ columns} \\ &= 0 \text{ if the corresponding row of } A^m \text{ does not have all zeros in its first } m - h_2 - 1 \text{ columns.} \end{aligned}$$

Proof: Let z_i, z_i' and z_i'' be defined as in the statement of the theorem.

By the methods used in proving Theorem 6, it follows that

$$\sum_{i=1}^{2^m-1} a_{ij}z_i' = h_1 2^{m-1} - \epsilon_j(m).$$

Consider

$$\sum_{i=1}^{2^m-1} a_{ij}z_i''.$$

This is equal to

$$\sum_{i=1}^{2^{h_2+1}-1} b_{ij},$$

where the b_{ij} are the entries of a matrix B, which is made up of those rows of A^m for which the corresponding z_i'' are equal to one. The first $m - h_2 - 1$ columns of B contain all zeros. Therefore,

$$\sum_{i=1}^{2^{h_2+1}-1} b_{ij} = 0 \qquad \text{for } 1 \leqq j \leqq m - h_2 - 1.$$

The next $h_2 + 1$ columns of B are identical with P^{h_2+1}, since each combination of zeros and ones (except the all-zero combination) occurs exactly once. Thus, since the weight of each column of P^{h_2+1} is 2^{h_2},

$$\sum_{i=1}^{2^{h_2+1}-1} b_{ij} = 2^{h_2} \qquad \text{for } m - h_2 \leqq j \leqq m.$$

Every other column of B is formed from the sum modulo 2 of some of the first m columns. Since the all-zero columns do not have any effect on the sum modulo 2 operation, every other column of B is equal either to one of the columns for $m - h_2 \leqq j \leqq m$ or to the sum modulo 2 of several of these columns. Thus, every remaining column of B is identical with some column of A^{h_2+1}. Therefore, for $m + 1 \leqq j \leqq 2^m - 1$,

$$\sum_{i=1}^{2^{h_2+1}-1} b_{ij} = \sum_{i=1}^{2^{h_2+1}-1} a_{ij}^{h_2+1} = 2^{h_2}.$$

Thus,

$$\begin{aligned}\sum_{i=1}^{2^m-1} a_{ij}z_i'' = \sum_{i=1}^{2^{h_2+1}-1} b_{ij} &= 0 \quad \text{for } 1 \leqq j \leqq m - h_2 - 1 \\ &= 2^{h_2} \text{ for } m - h_2 \leqq j \leqq 2^m - 1,\end{aligned}$$

and

$$\begin{aligned}\sum_{i=1}^{2^m-1} a_{ij}z_i &= h_1 2^{m-1} - \epsilon_j(m) - 0 \quad \text{for } 1 \leqq j \leqq m - h_2 - 1 \\ &= h_1 2^{m-1} - \epsilon_j(m) - 2^{h_2} \text{ for } m - h_2 \leqq j \leqq 2^m - 1.\end{aligned}$$

Thus,

$$\sum_{i=1}^{2m-1} a_{ij}z_i \geqq h_1 2^{m-1} - 2^{h_2} - \epsilon_j(m),$$

or the given z_i satisfy the requirements for a code with $d = h_1\, 2^{m-1} - 2^{h_2}$. This proves that a code constructed from the given z_i will have $d = h_1 2^{m-1} - 2^{h_2}$. A proof must now be given for the fact that the resulting code is minimum-redundancy

$$k = \sum_{i=1}^{2m-1} z_i = \sum_{i=1}^{2m-1} z_i' - \sum_{i=1}^{2m-1} z_i''.$$

The z_i' are the same as the z_i of Theorem 6; therefore,

$$\sum_{i=1}^{2m-1} z_i' = h_1(2^m - 1) - m.$$

Since there are $2^{h_2+1} - 1$ rows of A^m that have all zeros in the first $m - h_2 - 1$ columns,

$$\sum_{i=1}^{2m-1} z_i'' = 2^{h_2+1} - 1$$

and

$$k = h_1(2^m - 1) - m - 2^{h_2+1} + 1.$$

Now,

$$k^*\,(m,h_1 2^{m-1} - 2^{h_2}) = \left\{\left(\frac{2^m - 1}{2^{m-1}}\right)(h_1 2^{m-1} - 2^{h_2}) - m\right\},$$

which can be rewritten as

$$k^* = \{(2^m - 1)h_1 - 2^{h_2+1} + 2^{1+h_2-m} - m\},$$

but, since $m > 1 + h_2$,

$$2^{1+h_2-m} < 1,$$

so that

$$k^* = (2^m - 1)h_1 - 2^{h_2+1} - m + 1,$$

and therefore $k = k^*$ and the code is minimum-redundancy.

Corollary 7: Whenever $d = h_1 2^{m-1} - 2^{h_2} - 1$, where h_1 is a positive integer and h_2 is a positive integer with $h_2 < m - 1$, a minimum-redundancy code can be obtained from the code of Theorem 8 by the method given in Corollary 5.

Minimum-redundancy codes for $d = 2$, 3 and 4 were given in a paper by Hamming.[2] A code for $d = 2$ can be obtained by using all n-bit words that contain an even number of ones, since Theorem 2 just requires each column of P to contain at least one one. Thus, the minimum-redundancy codes for $d = 2$ all have $k = 1$.

For codes of distance 3, Theorem 2 requires that each column of P contain at least two ones and that no two columns be identical. In this case, m is equal to the number of different columns having k rows, and at least two entries equal to 1; or $m = 2^k - k - 1$.

VII. RELATIONSHIPS AMONG CODES

For values of d which are greater than 4 and do not satisfy the conditions of either Theorem 6 or Theorem 8, it has not been possible to obtain closed solutions of the linear program (LP). Computation using Gomory's algorithm[5] is necessary to obtain minimum-redundancy codes for these values of d. The following theorems present various general properties of minimum-redundancy codes that are useful in obtaining codes for new values of d from the codes obtained by use of the algorithm.

Definition: Let $K(m,d)$ be the minimum value of k that is possible for a code having m message bits and minimum distance d.

Definition: Let $N(m,d)$ be the minimum value of n that is possible for a code having m message bits and minimum distance d.

Lemma 10:

$$K(m-1,d) \leqq K(m,d).$$

Proof: A parity-check matrix for $m - 1$ can be obtained from the matrix for m by simply removing one column. Since the conditions of Theorem 2 must be satisfied by the reduced matrix if they were satisfied by the original matrix, the reduced matrix corresponds to a code of distance d if the original matrix corresponded to a code of distance d.

Theorem 9: For $m \leqq d < 2^{m-2}$,

$$N(m,d) > n^*(m,d),$$

$$K(m,d) > k^*(m,d).$$

Proof:

$$\begin{aligned} k^*(m,d) &= \left\{\left(\frac{2^m - 1}{2^{m-1}}\right) d - m\right\} \quad \text{for } m \leqq d \\ &= \{(2 - 2^{1-m})\, d - m\} \\ &= \left\{2d - \frac{d}{2^{m-1}} - m\right\} \end{aligned}$$

$$k^*(m,d) = 2d - m \qquad \text{for } m \leqq d < 2^{m-1},$$

$$k^*(m-1,d) = 2d - m + 1 \qquad \text{for } m - 1 \leqq d < 2^{m-2},$$

but

$$\begin{aligned} K(m,d) &\geqq K(m-1,d), \\ K(m-1,d) &\geqq k^*(m-1,d), \\ k^*(m-1,d) &> k^*(m,d) \qquad \text{for } m \leqq d < 2^{m-2}, \\ K(m,d) &\geqq K(m-1,d) \geqq k^*(m-1,d) > k^*(m,d), \end{aligned}$$

so that

$$K(m,d) > k^*(m,d) \qquad \text{for } m \leqq d < 2^{m-2}.$$

Since $n = k + m$, it follows that

$$N(m,d) > n^*(m,d) \qquad \text{for } m \leqq d < 2^{m-2}.$$

Theorem 10:

$$\begin{aligned} N(m,d_1 + d_2) &\leqq N(m,d_1) + N(m,d_2), \\ K(m,d_1 + d_2) &\leqq K(m,d_1) + K(m,d_2) + m. \end{aligned}$$

Proof: Let $z' = [z_1' \; z_2' \; \cdots \; z_{2^m-1}']$ be the values of z_i corresponding to $N(m,d_1)$ and $z'' = [z_1'' \; z_2'' \; \cdots \; z_{2^m-1}'']$ be the values of z_i corresponding to $N(m,d_2)$. Thus,

$$\sum_{i=1}^{2m-1} a_{ij}^m \, z_i' \geqq d_1 - \epsilon_j(m)$$

and

$$\sum_{i=1}^{2m-1} a_{ij}^m \, z_i'' \geqq d_2 - \epsilon_j(m).$$

Let

$$\hat{z}_i = z_i' + z_i'' + 1 \qquad \text{for } 1 \leqq i \leqq m$$

and

$$\hat{z}_i = z_i' + z_i'' \qquad \text{for } m + 1 \leqq i \leqq 2^m - 1.$$

Then,

$$\begin{aligned} \sum_{i=1}^{2m-1} a_{ij}^m \hat{z}_i &= \sum_{i=1}^{2m-1} a_{ij}^m z_i' + \sum_{i=1}^{2m-1} a_{ij}^m z_i'' + \sum_{i=1}^{m} a_{ij}^m \\ &\geqq d_1 - \epsilon_j(m) + d_2 - \epsilon_j(m) + \epsilon_j(m) \\ &\geqq d_1 + d_2 - \epsilon_j(m). \end{aligned}$$

Thus, $\hat{z}_i$ satisfy the conditions for a code of distance $d_1 + d_2$. Furthermore,

$$\sum_{i=1}^{2^m-1} \hat{z}_i = \sum_{i=1}^{2^m-1} z_i' + \sum_{i=1}^{2^m-1} z_i'' + \sum_{i=1}^{m} (1),$$

$$k(m,d,+d_2) = \sum_{i=1}^{2^m-1} \hat{z}_i = K(m,d_1) + K(m,d_2) + m,$$

so that

$$K(m,d_1 + d_2) \leqq K(m,d_1) + K(m,d_2) + m.$$

Corollary 8:

$$N(m,d_1 + h2^{m-1}) \leqq N(m,d_1) + h(2^m - 1),$$

$$K(m,d_1 + h2^{m-1}) \leqq K(m,d_1) + h(2^m - 1).$$

Definition: Let $\max(z_1, z_2, \cdots, z_m)$ equal the largest of the values of the z_i.

Theorem 11: Let $z_1, z_2, \cdots, z_{2^m-1}$ correspond to a code for which $k = K(m,d)$. Then, if $\max(z_1, \cdots, z_m) = M$,

$$K(m - 1,d) \leqq K(m,d) - M.$$

Proof. Let z_I, $(1 \leqq I \leqq m)$ be one of the z_i such that $z_I = M$. Then, if the Ith column is removed from the matrix P specified by $(z_1, z_2, \cdots, z_{2^m-1})$, the resulting matrix must still correspond to a code of minimum distance d (Lemma 10). However, M of the rows of the reduced matrix consist of all zeros, since there are M rows which contain a one only in column I. Thus, these M rows can be removed without affecting the minimum distance d. Removal of M rows decreases k by M, giving

$$K(m - 1,d) \leqq K(m,d) - M.$$

VIII. COMPARISON WITH PLOTKIN'S BOUND

The approach of this paper has been to search for codes which require the minimum number of check bits, k, for specified values of m and d. Another common approach to the study of error-correcting codes is to specify the total number of bits per code word, n, and the minimum distance, d, and then to try to construct codes which contain the largest number of messages. A bound on this maximum number of messages has been proved by Plotkin.[7]

Theorem 12 (Plotkin): Let $A(n,d)$ equal the maximum number of binary n-bit words in an error-correcting code (not necessarily a systematic code), for which the distance between any two code words is at least equal to d. Then

$$A(n,d) \leqq \frac{2d}{2d - n} \qquad \text{for} \quad 2d > n.$$

For a systematic code, the number of messages must be a power of two, and therefore this bound can be met exactly only when $2d/(2d - n)$ is a power of two. The following theorem shows that, whenever this is true, a systematic code exists which does meet the bound.

Theorem 13: For values of n and d such that $2d/(2d - n) = 2^m$, for some m, a systematic code exists with m message bits and therefore 2^m code words. For such values of n and d, no code of any type is possible with more code words.

Proof: The equation $2d/(2d - n) = 2^m$ can be written as

$$d = \left(\frac{n}{2^m - 1}\right) 2^{m-1}.$$

Since d and 2^{m-1} are integers, and $2^m - 1$ does not divide 2^{m-1}, $n/(2^m - 1)$ must be an integer. Let $h = n/(2^m - 1)$, then $d = h2^{m-1}$. By Theorem 6, a code exists with $d = h2^{m-1}$ and

$$n = h(2^m - 1) = \left(\frac{n}{2^m - 1}\right)(2^m - 1) = n$$

and m message bits.

By Plotkin's theorem, no code with more code words is possible.

IX. ACKNOWLEDGMENT

The author wishes to acknowledge the many helpful comments contributed by D. H. Evans, S. H. Unger and M. C. Paull. Thanks are due also to W. Ulrich and C. Y. Lee for many stimulating discussions on the general subject of error-correcting codes.

APPENDIX

Various proofs have been omitted in order not to disturb the continuity of the paper. These proofs will be presented here.

Lemma 4: The matrix A^m can be partititioned into submatrices as follows:

$$A^m = [P_1{}^m \vdots P_2{}^m \vdots P_3{}^m \vdots \cdots \vdots P_m{}^m].$$

Proof: By definition, the first m columns of A^m are identical with $P_1{}^m$.

The rows of P^m are ordered so that all rows with one one come first, then all rows with two ones, etc. The columns of P^m which must be summed to form the jth column of A^m are determined by the jth row of P^m. Because of the ordering of the rows of P^m, all sums of pairs of columns of P^m will occur as columns of A^m, then all sums of three columns of P^m, etc. Since $P_J{}^m$ contains all sums of J columns of P^m, A^m can be partitioned as shown.

Lemma 5: $a_{ij} = a_{i1}a_{j1} \oplus a_{i2}a_{j2} \oplus \cdots \oplus a_{im}a_{jm}$, for $j > m$.

Proof: The jth column of $A^m (j > m)$ is formed by taking the sum modulo 2 of the first m columns of A^m which have a one entry in the jth *row* of A^m. Thus, if the jth column of A^m is denoted by $A_j{}^m$,

$$A_j{}^m = a_{j1}A_1{}^m \oplus a_{j2}A_2{}^m \oplus \cdots \oplus a_{jm}A_m{}^m \qquad \text{for } j > m,$$

since the column $A_1{}^m$ is to enter into the sum only if $a_{j1} = 1$, etc. It follows from this that the ith element of the jth column $(j > m)$ is given by

$$a_{ij} = a_{i1}a_{j1} \oplus a_{i2}a_{j2} \oplus \cdots \oplus a_{im}a_{jm} .$$

Lemma 6:

$$a_{ij} = a_{ji} .$$

Proof: It follows directly from Lemma 5 that $a_{ij} = a_{ji}$ for $j > m$ or $i > m$. For $j < m$ and $i < m$, the definition of A requires that $a_{ij} = 0$ unless $i = j$, so that $a_{ij} = a_{ji} = 0$ for $i \neq j$ and, for $i = j$, a_{ij} is identical with a_{ji}.

Lemma 7:

$$\sum_{i=1}^{2^m-1} a_{ij}{}^m = \sum_{j=1}^{2^m-1} a_{ij}{}^m = 2^{m-1}.$$

Proof: The first m columns of A^m contain each m-bit binary number, except the all-zero number, exactly once. Consider these rows which have a one entry in the first column. There must be 2^{m-1} such rows, since there are 2^{m-1} different $(m - 1)$-bit binary numbers, and each of these must occur once in the remaining $m - 1$ columns. Thus,

$$\sum_{i=1}^{2^m-1} a_{i1}{}^m = 2^{m-1}.$$

A similar argument shows that

$$\sum_{i=1}^{2^m-1} a_{ij}{}^m = 2^{m-1} \qquad \text{for } 1 \leqq j \leqq m.$$

For $j > m$, each entry a_{ij}^m is the sum modulo 2 of the entries in s of the first m columns. Consider these columns. Each s-bit binary number must occur exactly 2^{m-s} times (except the all-zero number, which occurs $2^{m-s} - 1$ times), since there are exactly 2^{m-s} ways to choose the entries in the remaining $m - s$ columns. There are 2^s different s-bit numbers and 2^{s-1} of these contain an odd number of one entries. Thus, there are $(2^{m-s})\ (2^{s-1}) = 2^{m-1}$ rows containing an odd number of one entries, and hence 2^{m-1} of the a_{ij}^m are equal to one. Thus,

$$\sum_{i=1}^{2m-1} a_{ij} = 2^{m-1} \qquad \text{for } j > m.$$

Since $a_{ij} = a_{ji}$, it follows that

$$\sum_{j=1}^{2m-1} a_{ij} = 2^{m-1}.$$

Lemma 8:

$$\sum_{i=1}^{m} a_{ij}^m = \epsilon_j(m).$$

Proof: The definition of $\epsilon_j(m)$ is:

$$\begin{aligned} \epsilon_j(m) &= 1 \qquad \text{for} \quad 1 \leqq j \leqq m, \\ \epsilon_j(m) &= 2 \qquad \text{for} \quad 1 + m \leqq j \leqq m + \binom{m}{2}, \\ &\vdots \\ \epsilon_j(m) &= s \qquad \text{for} \quad \sum_{\nu=0}^{s-1} \binom{m}{\nu} \leqq j \leqq \sum_{\mu=1}^{s} \binom{m}{\mu}. \end{aligned}$$

Consider the first m columns of A^m. The first m rows contain a single one, since they are all the m-bit numbers containing one one. The next $\binom{m}{2}$ rows contain two ones, the next $\binom{m}{3}$ rows contain three ones, etc. Thus,

$$\sum_{j=1}^{m} a_{ij}^m = \epsilon_i(m).$$

Since $a_{ij} = a_{ji}$, it follows from this that

$$\sum_{i=1}^{m} a_{ij}^m = \epsilon_j(m).$$

Lemma 9: If the elements of A^{-1} are represented by a_{ij}^{-1}, then

$$a_{ij}^{-1} = 2^{1-m} \qquad \text{if } a_{ij} = 1$$

and

$$a_{ij}^{-1} = -2^{1-m} \qquad \text{if } a_{ij} = 0.$$

Proof: The a_{ij}^{-1} given above are the elements of the inverse of A if and only if

$$b_{ij} = \sum_{s=1}^{2^m-1} a_{is}a_{sj}^{-1} = 1 \qquad \text{if } i = j$$

and

$$b_{ij} = \sum_{s=1}^{2^m-1} a_{is}a_{sj}^{-1} = 0 \qquad \text{if } i \neq j.$$

If $i = j$, then

$$\sum_{s=1}^{2^m-1} a_{is}a_{sj}^{-1} = \sum_{s=1}^{2^m-1} a_{is}a_{si}^{-1} = \sum_{s=1}^{2^m-1} a_{si}a_{si}^{-1},$$

which equals

$$2^{1-m} \sum_{s=1}^{2^m-1} a_{si}\,.$$

But

$$\sum_{s=1}^{2^m-1} a_{si} = 2^{m-1} \quad \text{by Lemma 7,}$$

so that

$$\sum_{s=1}^{2^m-1} a_{is}a_{si}^{-1} = 1.$$

If $i \neq j$,

$$b_{ij} = \sum_{s=1}^{2^m-1} a_{is}a_{sj}^{-1} = \sum_{s=1}^{2^m-1} a_{si}a_{sj}^{-1}.$$

Three cases will be considered:

Case 1: $i < m$ and $j < m$.

In this case, $b_{ij} = 2^{1-m}$ (number of 11 entries in columns i and j) minus 2^{1-m} (number of 10 entries in columns i and j). By the argument used in proving Lemma 7, there are 2^{m-2} 11 entries and 2^{m-2} 10 entries, so that $b_{ij} = (2^{1-m})\,(2^{m-2}) - (2^{1-m})\,(2^{m-2}) = 0$.

Case 2: $i < m$ and $j > m$.

In this case, the elements a_{sj} are formed as the sum modulo 2 of the entries in ν of the first m columns of A, so that $b_{ij} = 2^{1-m}\,N_0 - 2^{1-m}\,N_e$, where

$N_0 =$ the number of rows of A which have a 1 in the ith column and an odd number of 1's in the ν columns from which a_{sj} is formed.

$N_e =$ The number of rows of A which have a 1 in the ith column and an even number of 1's in the ν columns from which a_{sj} is formed.

Again, by the argument of Lemma 7, in the $\nu + 1$ columns consisting of column i and the ν columns used to form a_{sj}, each different binary number (except the all-zero number) must occur exactly $2^{m-\nu-1}$ times so that $N_e = N_0$ and $b_{ij} = 0$.

Case 3:

A similar argument shows that $b_{ij} = 0$ for the case when $1 > m$ and $j > m$.

REFERENCES

1. Shannon, C. E., A Mathematical Theory of Communication, B.S.T.J., **27,** July 1948, p. 279; October 1948, p. 623.
2. Hamming, R. W., Error Detecting and Error Correcting Codes, B.S.T.J., **29,** January 1950, p. 147.
3. Reed, I. S., A Class of Multiple-Error-Correcting Codes and the Decoding Scheme, Trans. I.R.E., **PGIT-4,** 1954, p. 38.
4. Muller, D. E., Metric Properties of Boolean Algebra and Their Application to Switching Circuits, Report No. 46, Digital Computer Lab., Univ. of Illinois, April 1953.
5. Gomory, R. E., Outline of an Algorithm for Integer Solutions to Linear Programs, Office of Ordnance Research Symposium on Combinational Problems, New York, April 1958.
6. Slepian, D., A Class of Binary Signalling Alphabets, B.S.T.J., **35,** January 1956, p. 203.
7. Plotkin, M., Binary Codes with Specified Minimum Distance, Research Division Report 51-20, Moore School of Electrical Engineering, Univ. of Pennsylvania, January 1951.