WITTY, MARILYN PAIT. Minimum Distance Bounds for Error-Correcting Codes. (1977) Directed by: Dr. Richard Michael Willett. Pp. 58.

An error-correcting code consists of an algebraic procedure for altering the flow of information across a noisy transmission channel in such a way that the original information can be recovered from the received signal. An important parameter associated with the coding problem is the largest minimum distance over all block codes with a given transmission rate. An equivalent formulation of this minimum distance problem will be presented and the determination of upper and lower bounds will be discussed.

MINIMUM DISTANCE BOUNDS FOR ERROR-CORRECTING CODES

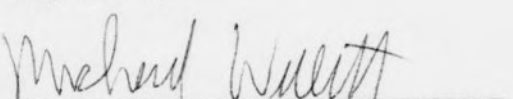
by

Marilyn Pait Witty

A Thesis Submitted to
the Faculty of the Graduate School at
The University of North Carolina at Greensboro
in Partial Fulfillment
of the Requirements for the Degree
Master of Arts

Greensboro
1977

Approved by



Thesis Adviser

APPROVAL PAGE

This thesis has been approved by the following committee of the Faculty of the Graduate School at the University of North Carolina at Greensboro.

Thesis Adviser Michael Willett

Committee Members

August 3, 1977
Date of Acceptance by Committee

ACKNOWLEDGEMENTS

The author would like to express her appreciation to Dr. Michael Willett for his invaluable guidance and encouragement in the preparation of this thesis. Appreciation is also extended to Dr. E. E. Posey and Dr. Charles A. Church for their critical reading of the thesis manuscript.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

INTRODUCTION

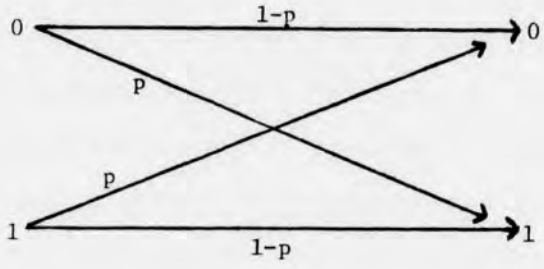
Communication is the transmission of information from a source to a receiver (destination). Human speech, telephone conversations, high frequency radios, and space communication links each involve communication. In each case information is passed from a source through a channel (telephone line, space, etc.) to a receiver. If the channel is "noiseless" the information being transmitted is not altered and is received correctly. However, most channels are noisy, where noise is defined as any alteration of the message in a non-deterministic or probabilistic way. Messages transmitted through noisy channels may be affected by the noise, resulting in a different message being received. For example, cross-talk in telephone conversations, lightning, or static may cause errors to be introduced in the transmitted message. The communication problem is to determine a way to decrease the effects of the noise in the channel on the message so that the message may be transmitted as reliably as possible.

In this thesis it will be assumed that information is represented as binary numbers. For example, a letter of the alphabet may be coded as the binary number which denotes the letter's position in the alphabet. The letter m is the thirteenth letter of the alphabet and is coded as 01101. Any English message is converted into this code before being transmitted and the coded message is converted back to English when received, as in the following model.

Source → Source to binary converter → Channel → Binary to destination converter → Destination

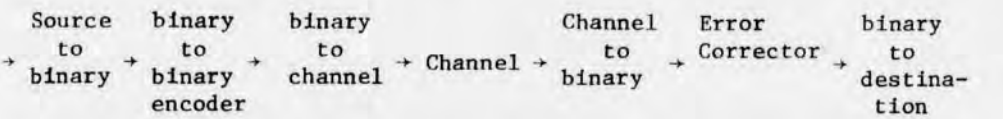
It will also be assumed that the channel is accurately modeled by the binary symmetric channel. (Figure 1.1) Each binary symbol (0 or 1) is transmitted incorrectly with probability p, $p < \frac{1}{2}$ and correctly with probability $1-p > \frac{1}{2}$. In other words, the probability that a symbol is altered by the noise of the channel is less than $\frac{1}{2}$.

Figure 1.1 Binary Symmetric Channel



Assume that the messages "yes" or "no" can be transmitted across a noisy telegraph line. "Yes" is coded as 1 and "no" is coded as 0. If 1 is transmitted and, due to the noise of the line, 0 is received the receiver would incorrectly assume that 0 was the message transmitted since it is more probable that an error did not occur. However assume that 1 is first coded into 11111 before being transmitted and 0 into 00000. Then if 11111 is transmitted and 11011 is received, the receiver would correctly assume that 11111 was sent since it is more probable that the noise of the channel caused one error rather than four errors. Notice that in both transmissions only one error was made.

However in the first situation the receiver was unable to detect that an error had been made while in the second situation the receiver was able to detect and correct the error. Coding 1 as 11111 and 0 as 00000 added redundancy to the information thus reducing the effects of the noise of the channel on the receiver's ability to determine the transmitted message. The following is a model of this communication scheme.



For some channels it is sufficient that the receiver be able to detect that errors have been made. Upon discovering an error the receiver simply requests re-transmission of the message. However, for some channels (such as deepspace) re-transmission is impractical, in which case the receiver must make the best possible estimate of the errors. In the example of the telegraph line it was impossible to detect errors when "yes" was transmitted as 1 and "no" as 0. In order to increase the error detection and correction capabilities of the receiver it was necessary to increase the number of symbols required for each message, thus decreasing the speed at which the message could be transmitted. Coding theory is concerned with techniques of altering (coding) the information on input in such a way that the transmission rate is barely affected and the receiver is able to separate the information from the noise of the channel with small probability of error. Since these are conflicting and difficult goals much work has been done on deriving bounds on the capabilities of codes.

In this thesis we will discuss the bounds on the capabilities of a class of codes referred to as linear block codes. In Chapter II linear block codes will be defined and certain properties of such codes will be discussed. Minimum distance, generator matrices, and parity check matrices for linear block codes will also be introduced. Syndrome decoding, a scheme used by the receiver to detect and/or correct errors which may have been introduced in the message by the channel, will be explained and illustrated in Chapter III. Chapter IV is a presentation of several existing upper and lower bounds on the minimum distance of a linear block code. Chapter V and Chapter VI present refinements of known lower and upper bounds respectively, on the minimum distance of a linear block code.

CHAPTER II

LINEAR BLOCK CODES

In this chapter block coding, a technique for coding the input stream to a noisy channel, will be presented. The dual process of decoding (i.e. separating the original input from the noise) will also be discussed. It will be assumed that the members of the input sequence are chosen from the finite field F with two elements.

To use a block code, the input sequence is first divided into consecutive k-tuples over the field F. Each consecutive k-tuple is associated with an n-tuple over F as determined by some one-to-one function $f: F_k \xrightarrow{1-1} F_n$, $n > k$, where F_k denotes the vector space of k-tuples over F. The function f is called the encoding function. This sequence of consecutive n-tuples is then transmitted across the channel in place of the original sequence. If the n-tuples in the range of f form a subspace of the vector space F_n, then the code is called an (n,k) linear block code and the individual n-tuples in the range of f are called codewords. Any k-dimensional subspace of n-tuple space will also be referred to as an (n,k) linear block code without reference to any particular encoding function f. The following one-to-one function f defines an association of binary 3-tuples with binary 9-tuples:

$$\begin{aligned} f(100) &= 110101110 & f(110) &= 111010110 \\ f(010) &= 001111000 & f(101) &= 110011000 \\ f(001) &= 000110110 & f(011) &= 001001110 \\ f(000) &= 000000000 & f(111) &= 111100000 \end{aligned} \qquad (2.1)$$

The range of f in (2.1) can be seen to form a subspace of F_9 and therefore

$$C_1 = \{110101110, 001111000, 000110110,$$
$$000000000, 111010110, 110011000,$$
$$001001110, 111100000\} \qquad (2.2)$$

is a (9,3) linear block code. Reference will be made to this particular linear block code throughout the chapter.

The Hamming distance, $d(u,v)$, between tuples u and v is defined to be the number of positions in which the tuples differ. For example,

$$d(110101110, 001111000) = 6.$$

The minimum distance of a linear block code C, denoted $d(C)$, is the minimum Hamming distance that exists between any two codewords of C. In the case of code C_1 in (2.2), $d(C_1) = 4$. The Hamming weight of a tuple u, $w(u)$, is the number of nonzero components of u. For example,

$$w(11011000) = 4.$$

The minimum weight of a linear block code C is the weight of the nonzero codeword of C which has the smallest Hamming weight. The following lemma states an interesting relationship between the minimum distance and the minimum weight of a linear block code.

Lemma 2.1 The minimum distance and the minimum weight of a linear block code are equal.

Proof: If u and v are codewords of a linear block code, then $u-v$ must be a code word by definition of a subspace. Therefore the distance between any two codewords is equal to the weight of some other codeword. Conversely the weight of a codeword u is the distance between u and the all-zero codeword. Q.E.D.

The significance of the concept of minimum distance is realized in the decoding process. Assume the codeword v is transmitted and e errors occur during the process of transmission, resulting in the vector v' being received. Then $d(v,v') = e$. If e is less than the minimum distance of the code, $e < d(C)$, then v' could not have become another codeword. So any errors (i.e. $e \neq 0$) will be detected by the fact that v' is not a codeword. In this case the receiver could request retransmission. Now assume $d(v,v') = e$ and $e \leq \frac{d(C)-1}{2}$. Then v' will still be closer to v than to any other codeword. In this case one could determine the identity of v by finding the closest codeword to v'. This process constitutes error-correction and is referred to as closest codeword decoding. The following theorem states that closest codeword decoding minimizes the probability of decoding failure.

Theorem 2.1 Let C be an (n,k) linear block code for use over the binary symmetric channel with error probability $p(p < \frac{1}{2})$. Then the probability of correct decoding is maximized if closest codeword decoding is implemented as the decoding scheme.

Proof: Assume that an arbitrary decoding scheme associates an arbitrary n-tuple y with the codeword $C(y)$. Further assume that the codeword x is transmitted and received as y. Let X denote the random variable whose possible values are the codewords and let E denote the random

variable whose possible values are the errors produced by the channel. Define the random variable Y as $Y = X + E$. Note that y is a possible value of Y. Since Y is a random variable, the decoding scheme is a function of Y and is denoted $C(Y)$. Then the average probability of correct decoding is

$$\text{Prob}\,[C(Y) = X] = \text{Prob}\,[Y-X = Y-C(Y)] = \text{Prob}\,[E = Y-C(Y)]$$

$$= \sum_{y} \text{Prob}\,[E = y-C(y) \mid Y = y]\ \ \text{Prob}\,[Y = y].$$

Since $\text{Prob}\,[Y = y]$ does not depend on the decoding scheme we can maximize the above sum by maximizing the term $\text{Prob}\,[E = y-C(y) \mid Y = y]$ in each summand. For a particular y, let $d = d(y,C(y))$. Then $\text{Prob}\,[E = y-C(y) \mid Y = y] = p^d(1-p)^{n-d}$. Let $f(d) = p^d(1-p)^{n-d}$. We will now show that $f(d)$ is a monotone decreasing function of d. Note that $[f(d)]' = f(d)[\log_2 p - \log_2(1-p)]$. Since $p < \frac{1}{2}$, $[\log_2 p - \log_2(1-p)]$ is negative and therefore $f(d)$ is monotone decreasing. Then $\text{Prob}\,[E = y-C(y) \mid Y = y] = p^d(1-p)^{n-d}$ is monotone decreasing function of d. Thus $\text{Prob}\,[E = Y-C(Y)]$ (average probability of correct decoding) is maximized if $C(y)$ is the closest codeword to y for each y. Q.E.D.

A code C is considered <u>e-error detecting</u> if $e < d(C)$ and <u>e-error correcting</u> if $e \leq \frac{d(C)-1}{2}$. For the code C_1 in (2.2), $d(C_1) = 4$ and therefore any occurrence of three or fewer errors in transmission can be detected and any occurrence of one error in transmission can be corrected.

A $k \times n$ matrix whose rows consist of a basis for a linear block code C is referred to as a <u>generator matrix for C</u>, denoted G. The rowspace of G is the linear block code C and a vector is a codeword of C if and only if it is a linear combination of the rows of G. Since there are k coefficients and 2 possible values for each coefficient,

there are 2^k distinct linear combinations and hence 2^k vectors in C. The following matrix G_1 is a generator matrix for the code C_1 in (2.2).

$$G_1 = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \end{bmatrix} \tag{2.3}$$

The generator matrix G_1 was determined by choosing three linearly independent codewords of C_1.

The nullspace of a subspace V of F_n is defined as follows.

$$N(V) = \{v = (v_1 \ \dots \ v_n) \mid \sum_{i=1}^{n} u_i v_i = 0 \quad \text{for all}$$

$$u = (u_1 \ \dots \ u_n) \quad \text{in} \quad v\} .$$

The sum in the definition of $N(V)$ is reduced modulo 2. A basic result of linear algebra states that if the dimension of a subspace of n-tuples is k, then the dimension of the nullspace is $n-k$. Therefore an (n,k) code C has as its nullspace a vector space C' of dimension $n-k$. An $(n-k) \times n$ matrix H of rank $n-k$ can be constructed such that the rowspace of H is $N(C)$ and therefore the rows of H form a basis for $N(C)$. Any such matrix H is called a <u>parity check matrix</u> for the code C. Dually C is the nullspace of $N(C)$, that is $N(N(C)) = C$, and so a vector v is a codeword of C if and only if it is orthogonal to every row of H. In other words, v is in C if and only if

$$vH^T = 0 . \tag{2.4}$$

If $v = (v_1 \ \dots \ v_n)$ and h_{ij} is the element in the i^{th} row, j^{th} column of H, then (2.4) becomes

$$\sum_j v_j h_{ij} = 0 \quad \text{for} \quad 1 \le i \le n-k.$$

Thus the components of v must satisfy a set of $n-k$ independent homogeneous equations. These equations are called generalized parity check equations. For each row of H, the number of 1's in v which correspond to the 1's in a row of H is even. Therefore these equations are checks for even parity on certain components of the codeword. A parity check matrix H_1 for the code C_1 in (2.2) is:

$$H_1 = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{2.5}$$

Note that the rowspace of H_1 is the nullspace of C_1. This can be checked by observing that $G_1 H_1^T = 0$; that is, the rows of H_1 are orthogonal to a basis for C_1. A vector space C and its nullspace $N(C)$ are both linear block codes. If C is an (n,k) code, then $N(C)$ is an $(n, n-k)$ code. If a code is the rowspace of a matrix then the nullspace of the matrix is called the dual of the code and vice versa. Therefore the rowspace of H_1 in (2.5.), denoted $N(C_1)$, is a $(9,6)$ linear block code and $N(C_1)$ is the dual of C_1. The following theorem describes an important algebraic relationship between a linear block code and any of its parity check matrices.

Theorem 2.2 An (n,k) linear block code C that is the nullspace of an $(n-k) \times n$ matrix H has minimum weight (and hence minimum distance) d if and only if every set of $d-1$ or fewer columns of H is linearly independent.

Proof: (Sufficiency) Let $H = [h_1 h_2 \ldots h_n]$ and choose an arbitrary set $\{h_{i_1}, h_{i_2}, \ldots, h_{i_t}\}$, $t \leq d-1$, of columns from H. Assume that

$$a_1 h_{i_1} + a_2 h_{i_2} + \ldots + a_t h_{i_t} = 0$$

for some a_i. Then $vH^T = 0$ where v has a_s in position i_s and zeros elsewhere so that v is a codeword of C. Since $w(v) \leq d-1 = d(C)-1$, it follows that $v = 0$. Therefore $a_i = 0$, $i = 1,2,\ldots,t$, and $\{h_{i_1}, h_{i_2}, \ldots h_{i_t}\}$ is linearly independent.

(Necessity) Assume there exists a codeword of C, say v, with $w = w(v) \leq d-1$. Then $vH^T = 0$ or

$$h_{i_1} + h_{i_2} + \ldots + h_{i_w} = 0$$

where $i_1, i_2, \ldots i_w$ are the positions in v where 1's occur. This is a linear dependence relationship among $d-1$ or fewer columns of H which contradicts the fact that every set of $d-1$ or fewer columns of H is linearly independent. Therefore the code has minimum weight at least d.

Q.E.D.

If a set of vectors obtained by applying a single fixed permutation to the codewords in an (n,k) code C is also an (n,k) code, say C^*, then C^* is said to be equivalent to C. Equivalent codes have the same minimum distance and therefore are equivalent with respect to error correction capability. The re-arrangement of the columns of a generator matrix G results in a matrix G^* whose rowspace consists of vectors which only differ from the vectors of the rowspace of G by a fixed rearrangement of components. Therefore if a code C is the rowspace of a matrix G then C^* is a code equivalent to C if and only if C^* is the rowspace of G^*, a matrix obtained from G by rearranging the columns of G. An elementary row operation performed on G results in

a matrix G' with the same rowspace as G and therefore G and G' will both be generator matrices for the same code. A combination of row operations and column permutations of G yields a matrix G'' which is said to be <u>combinatorially equivalent</u> to G. Every generator matrix G is combinatorially equivalent to a reduced echelon matrix of the following form.

$$G'' = \begin{bmatrix} 1 & 0 & \cdots & 0 & p_{11} & p_{12} & \cdots & p_{1n-k} \\ 0 & 1 & \cdots & 0 & p_{21} & p_{22} & \cdots & p_{2n-k} \\ \vdots & & & & & & & \\ 0 & 0 & \cdots & 1 & p_{k1} & p_{k2} & \cdots & p_{kn-k} \end{bmatrix} = [I_k : P] \qquad (2.6)$$

For example, G_1 in (2.3) is combinatorially equivalent to the following reduced echelon matrix G_1''.

$$G_1'' = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix} \qquad (2.7)$$

Let $w = (v_1 v_2 \cdots v_k)$ be an arbitrary k-tuple over F. Consider the linear combination of the rows of a reduced echelon matrix G'' as in (2.6) where v_i is used as the i^{th} coefficient. The linear combination can be represented by the following equation.

$$wG'' = (v_1 v_2 \cdots v_k C_1 C_2 \cdots C_{n-k}) = u$$

$$\text{where } C_j = \sum_{i=1}^{k} v_i p_{ij},\ 1 \le j \le n-k \qquad (2.8)$$

Therefore the first k components of u can be arbitrarily chosen information symbols and each of the last $n-k$ components are linear combinations of the first k components. The rowspace of G'' which consists of vectors in the form of the vector u in (2.8) forms a systematic code. The first k components of a codeword of a systematic code are always the original k-tuple input symbols and are called information symbols. The last $n-k$ components of a codeword are called the redundant or check symbols. Since every generator matrix G is combinatorially equivalent to a reduced echelon matrix in the form of G'' in (2.6), the following theorem holds.

Theorem 2.3 Every linear code is combinatorially equivalent to a systematic code.

The code C_1 in (2.2) is combinatorially equivalent to the following systematic code C_1'' which is the rowspace of the matrix G_1'' given in (2.7).

$$C_1'' = \{100011010,\ 010111000,\ 001110100,\ 000000000,\ 110100010,\ 101101110,\ 011001100,\ 111010110\} \tag{2.9}$$

Given a reduced echelon generator matrix for a code, the following theorem demonstrates a simple way to determine a parity check matrix for the code.

Theorem 2.4 If V is the rowspace of the matix $G = [I_k : P]$ where P is a $k \times (n-k)$ matrix, then V is the nullspace of the matrix $H = [-P^T : I_{n-k}]$.

Proof: $GH^T = [I_k P] \begin{bmatrix} -P \\ I_{n-k} \end{bmatrix} = [0]$.

The rank of G is k and the rank of H is $n-k$. Since the sum of their ranks is n and $GH^T = 0$, the rowspace of G is the nullspace of H. Q.E.D.

The parity check matrix for the code C_1'' in (2.9) as determined by the above theorem and the matrix G_1'' in (2.7) is:

$$H_1'' = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Using this form the first three components of a codeword $(a_1 a_2 a_3 a_4 a_5 a_6 a_7 a_8 a_9)$ of C_1'' can be chosen arbitrarily and the last six components, or check symbols, are determined by the following equations.

$$a_4 = a_2 + a_3 \qquad a_7 = a_3$$

$$a_5 = a_1 + a_2 + a_3 \qquad a_8 = a_1$$

$$a_6 = a_1 + a_2 \qquad a_9 = 0$$

Let $u = (v_1 v_2 \ldots v_n)$ be a codeword of an (n,k) systematic code. The first k components of u are the information symbols and the last $n-k$ components are the check symbols. The check symbols represent redundancy added to the message to decrease the chance of the message being lost to the noise of the channel. Therefore n symbols are used to transmit k symbols of information. It follows that the efficiency or rate of the code is $R = \frac{k}{n}$. For any channel, Shannon [4] has

defined a quantity called channel capacity, denoted R_o where $0 \leq R_o \leq 1$. The capacity of a channel represents the maximum average amount of information per source symbol that can flow across the channel with various sources attached to it. We emphasize that channel capacity (without defining it here) is an abstract quantity and that information can be contained in the received signal without this information being available to the receiver. Shannon found that, given a transmission rate which is less than the channel's capacity, it is possible to choose a code such that the probability of incorrect decoding for the code is arbitrarily small. Shannon's proof did not construct such codes but only declared their existence. Feinstein [2] found that Shannon's theorem holds for linear block codes as follows.

Theorem 2.5 For any $R < R_o$ and any $\epsilon > 0$, there exists an (n,k) linear block code such that $R \leq \frac{k}{n} \leq R_o$ and the probability of incorrect decoding is less than ϵ.

CHAPTER III

SYNDROME DECODING

In this chapter we shall present an efficient procedure for implementing the closest codeword decoding scheme for linear block codes. This procedure, which is referred to as syndrome decoding, yields the maximum probability of correct decoding and is the basis for most current decoding algorithms.

Let C be an (n,k) linear block code and let $v_1 = \theta$ denote the zero vector. The other codewords of C will be denoted by $v_2, v_3, \ldots, v_{2^k}$. An array called the standard array for C is constructed as follows. First the codewords are entered in a row with the zero vector θ at the left. Next one of the remaining n-tuples not in the code, say E_1, is placed under θ. The remaining entries in this row are the sums of E_1 and the codewords above each position. In other words, the vector in the i^{th} position of this row is the vector $u_{1i} = E_1 + v_i$. The next row is formed in a similar manner. A vector, say E_2, which does not appear in the two preceding rows is placed in the first column under θ. The i^{th} entry in this row is the vector $u_{2i} = E_2 + v_i$. This process is continued until each n-tuple appears in the array. The standard array is of the following form.

$$\begin{array}{ccccc} \theta & v_2 & v_3 & \cdots & v_{2^k} \\ E_1 & E_1 + v_2 & E_1 + v_3 & \cdots & E_1 + v_{2^k} \\ \vdots & & & & \\ E_{2^{n-k-1}} & E_{2^{n-k-1}} + v_2 & E_{2^{n-k-1}} + v_3 & \cdots & E_{2^{n-k-1}} + v_{2^k} \end{array} \qquad (3.1)$$

Note that the rows of the array are cosets of the additive subgroup C. Therefore each n-tuple appears exactly once in the array and there are $\frac{2^n}{2^k} = 2^{n-k}$ cosets. The elements in the first column are referred to as the coset leaders. The standard array yields its own scheme for decoding in the following way. When a vector is received, it is located in the array and decoded as the codeword which appears above it. For example, assume that the vector $w_{23} = E_2 + v_3$ is received. The vector w_{23} is located in the column headed by the codeword v_3 and therefore w_{23} is decoded as v_3. By decoding w_{23} as the codeword v_3 one is assuming that the error pattern which occurred during transmission was $E_2 = v_3 - w_{23}$. Therefore when a vector is received and decoded as the codeword which appears above it in the standard array the assumption is that the error pattern which occurred during transmission is the coset leader of the coset containing the received vector. Some error patterns have a higher probability of occurring than do others. Therefore it would be better to choose as coset leaders the more probable error patterns. We have already seen that the lower weight error vectors are more probable. The choice of low weight coset leaders is justified by the following theorem.

Theorem 3.1 If each coset leader is chosen to have minimum weight in its coset, then the standard array decoding scheme described above is closest codeword decoding.

Proof: Assume the coset leader of each coset has minimum weight in its coset. Suppose a particular vector u appears in the standard array under the codeword v and $d(u,v) = w$. Suppose the closest codeword to u is v_1 and $d(u,v_1) = w_1$. Let g denote the coset leader of

the coset which contains u. Then $g = u-v$ has weight w. The vector $u-v_1 = (g + v) - v_1 = g + (v-v_1)$ has weight w_1 and is in the same coset as g since $v-v_1$ is a codeword. Since it was assumed that g has minimum weight in its coset, $w_1 \geq w$ and u is at least as close to v as v_1. Q.E.D.

Therefore, by Theorem 2.1, if each coset leader is chosen to have minimum weight in its coset the standard array decoding scheme yields the maximum probability of correct decoding. Let C_2 denote the following (6,3) linear block code.

$$C_2 = \{100110, 010101, 001011, 110011,$$
$$101101, 011110, 111000, 000000\} \qquad (3.2)$$

The following standard array for C_2 is constructed in the manner set forth in the premise of Theorem 3.1.

000000	100110	010101	001011	110011	101101	011110	111000
100000	000110	110101	101011	010011	001101	111110	011000
010000	110110	000101	011011	100011	111101	001110	101000
001000	101110	011101	000011	111011	100101	010110	110000
000100	100010	010001	001111	110111	101001	011010	111100
000010	100100	010111	001001	110001	101111	011100	111010
000001	100111	010100	001010	110010	101100	011111	111001
100001	000111	110100	101010	010010	001100	111111	011001

Note that all weight = one error patterns appear as coset leaders. Therefore if one error is made during the transmission of a codeword the received vector can be correctly decoded. A weight = two error pattern

also appears as a coset leader (the choice of this coset leader is not unique). This means that some 6-tuples are two units away from the code.

For large values of n the standard array is too large to store. For example a (50,20) linear block code would require 2^{50} entries in the standard array. A concept referred to as the syndrome of a vector leads to a more compact standard array. Let H be a parity check matrix for an (n,k) linear block code C. For any received n-tuple u, the syndrome, s, of u is defined as

$$s = uH^T.$$

Since C is the nullspace of H, the syndrome of any codeword is the all-zero (n-k)tuple and the syndrome of any n-tuple which is not a codeword is a nonzero (n-k) tuple. The following theorem demonstrates an important relationship between the members of a coset of a standard array and their syndromes.

Theorem 3.2 Two vectors are in the same coset if and only if they have the same syndrome.

Proof: Let C be an (n,k) linear block code. Assume the vectors u_1 and u_2 are in the same coset of C and E_1 is the coset leader. Then $u_1 = v_i - E_1$ and $u_2 = v_j - E_1$ where v_i and v_j are codewords of C. Then $u_1 - u_2 = (v_i - E_1) - (v_j - E_i) = v_i - v_j$ which is a codeword. Let C be the nullspace of a matrix H. Then $u_1 - u_2$ is a codeword if and only if

$$(u_1 - u_2)H^T = 0.$$

Since the distributive law holds for the multiplication of matrices it follows that

$$(u_1 - u_2)H^T = u_1H^T - u_2H^T = \theta \quad \text{or}$$

$$u_1H^T = u_2H^T .$$

Therefore $u_1 - u_2$ is a codeword if and only if the syndromes of u_1 and u_2 are equal. Q.E.D.

The preceding theorem leads to a more compact realization of standard array decoding. When a vector is received its syndrome is calculated and the coset leader with the same syndrome is located. The coset leader represents the assumed error pattern. The coset leader is subtracted from the received vector and the codeword so produced is assumed to be the transmitted codeword. This process is referred to as <u>syndrome decoding</u>. The decoding table now need only consist of the 2^{n-k} coset leader/syndrome pairs. Not only does the scheme represent a more compact version of standard array decoding but syndrome decoding is the underlying basis for current schemes for which the size of 2^{n-k} prohibits even the storage of the coset leader/syndrome pairs.

The matrix

$$H_2 = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

is a parity check matrix for the code C_2 in (3.2) and is used in the calculations of the syndromes of the cosets of C_2 .

$$s_1 = (000000)H^T = 000$$
$$s_2 = (100000)H^T = 110$$
$$s_3 = (010000)H^T = 101$$
$$s_4 = (001000)H^T = 011$$
$$s_5 = (000100)H^T = 100$$
$$s_6 = (000010)H^T = 010$$
$$s_7 = (000001)H^T = 001$$
$$s_8 = (100001)H^T = 111$$

Assume the vector 101111 is received. First the vector's syndrome is calculated.

$$(101111)\begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = 010$$

The coset leader associated with the syndrome 010 is 000010. Therefore the vector 101111 is decoded as the codeword 101111 - 000010 = 101101.

CHAPTER IV

MINIMUM DISTANCE BOUNDS FOR ERROR-CORRECTING CODES

Let d denote the minimum distance of a linear block code C. Then all occurrences of $\frac{d-1}{2}$ or fewer errors made during the transmission of a code word of C can be corrected by the receiver. Therefore, for given values of n and k, one would want to know the largest minimum distance possible for an (n,k) linear block code in order to assure maximum error-correction capability. In this chapter we shall present upper and lower bounds on the minimum distance attainable for a given value of code rate $R = \frac{k}{n}$. Each bound is on the value $\frac{d}{2n}$ as a function of a fixed code rate R.

Hamming Upper Bound

The Hamming upper bound is derived by using a sphere-packing approach. Let C denote an (n,k) linear block code with minimum distance d and code rate $R = \frac{k}{n}$. A sphere, $S_t(v)$, of radius t and center v (where v is an n-tuple) is defined to be the set of all n-tuples whose Hamming distance from v is t. Since C consists of 2^k codewords, there are 2^k spheres of radius t which have codewords as centers. Let $A_t^{(n)}$ denote the number of n-tuples whose distance from a given codeword is equal to t. The following lemma shows that the number $A_t^{(n)}$ does not depend on the particular codeword.

Lemma 4.1 $A_t^{(n)} = \binom{n}{t}$.

Proof: Let $u = (v_1 v_2 \ldots v_n)$ be a codeword of a linear block code. The binomial coefficient $\binom{n}{t}$ is the number of ways of choosing t

entries from the n entries of u. Let $v_{i_1} v_{i_2} \ldots v_{i_t}$ represent one choice of t entries from u. If each of the v_{ij}'s are replaced by the other field element (i.e. if v_{ij} is 1, then it is replaced by 0 and vice versa), then the result is an n-tuple u' which differs from u in t positions. Continue this process for each of the $\binom{n}{t}$ choices of t entries from the n entries of u. Each of the resulting $\binom{n}{t}$ n-tuples will differ from u in t positions. Q.E.D.

Let $V_t^{(n)}$ denote the number of n-tuples whose distance from a codeword u is $\leq t$, that is $|S_t(u)| = V_t^{(n)}$. Note that $V_t^{(n)} = \sum_{i=o}^{t} A_i^{(n)}$.

If $d \geq 2t + 1$, then t is less than half the minimum distance between codewords and no n-tuple can be within distance t of more than one codeword. Therefore the 2^k spheres which have codewords as centers must be disjoint. Since each of the 2^k spheres contain $V_t^{(n)}$ n-tuples, a total of $2^k V_t^{(n)}$ distinct n-tuples appear in the spheres. But the number of n-tuples which appear in the spheres cannot exceed the total number of n-tuples. Therefore

$$2^k V_t^{(n)} \leq 2^n \quad \text{or}$$

$$V_t^{(n)} \leq 2^{n-k} . \tag{4.1}$$

If the $\log_2(x)$ function (which is monotone increasing) is applied to (4.1), this inequality becomes:

$$R = \frac{k}{n} \leq \frac{1 - \log_2 V_t^{(n)}}{n} . \tag{4.2}$$

For any value of $P = \frac{t}{n}$, define the function F(P) as follows:

$$F(P) = 1 - \lim_{n\to\infty} \frac{V_{Pn}^{(n)}}{n} \quad . \tag{4.3}$$

Therefore for large values of n, inequality (4.2) becomes:

$$R \leq F(\frac{t}{n}) \quad . \tag{4.4}$$

The limit appearing in (4.3) does exist and is expressible in the closed form stated in the following lemma.

Lemma 4.2 $\lim_{n\to\infty} \frac{\log_2 V_{Pn}^{(n)}}{n} = -P \log_2 P - (1-P)\log_2(1-P)$

Proof (Sketch): The following inequality can be obtained using the Chernoff bound on a certain sum of binomial coefficients.

$$\frac{[(P^{-P}(1-P)^{-(1-P)})^n]}{n+1} \leq V_{Pn}^{(n)} \leq [(P^{-P}(1-P)^{-(1-P)})^n]$$

If we apply the $\log_2(x)$ function to the above inequality and divide each term by n we obtain:

$$\frac{\log_2[(P^{-P}(1-P)^{-(1-P)})^n]}{n} - \frac{\log_2(n+1)}{n} \leq \log_2 V_{Pn}^{(n)} \leq \frac{\log_2[(P^{-P}(1-P)^{-(1-P)})^n]}{n}$$

Since $\lim_{n\to\infty} \frac{\log_2(n+1)}{n} = 0$, it follows that:

$$\lim_{n\to\infty} \frac{\log_2 V_{Pn}^{(n)}}{n} = \lim_{n\to\infty} \frac{\log_2[(P^{-1}(1-P)^{-(1-P)})^n]}{n}$$

$$= \lim_{n\to\infty} \frac{n \log_2(P^{-1}(1-P)^{-(1-P)}}{n}$$

$$= \log_2(P^{-P}(1-P)^{-(1-P)})$$

$$= -P \log_2 P - (1-P) \log_2 (1-P) . \qquad \text{Q.E.D.}$$

Therefore $F(P) = 1 + P \log_2 P + (1-P) \log_2 (1-P)$. A rough sketch of the function F appears in Figure 4.1. Since $d \leq n$ and $2t + 1 \leq d$, it follows that $\frac{t}{n} \in [0, \frac{1}{2}]$. Since F is decreasing on $[0, \frac{1}{2}]$ applying F^{-1} to both sides of (4.4) reverses the inequality.

$$F^{-1}(R) \geq F^{-1}(F(\tfrac{t}{n})) = \frac{t}{n} \quad \text{or}$$

$$\frac{t}{n} \leq F^{-1}(R) \qquad (4.5)$$

If $d = 2t + 1$, then inequality (4.5) becomes

$$\frac{d-1}{2n} \leq F^{-1}(R) \quad \text{or}$$

$$\frac{d}{2n} \leq F^{-1}(R) + \frac{1}{2n} . \qquad (4.6)$$

Since $\lim_{n\to\infty} \frac{1}{2n} = 0$, the asymptotic form of (4.6) is

$$\frac{d}{2n} \leq F^{-1}(R) .$$

This asymptotic form is referred to as the Hamming Upper Bound on $\frac{d}{2n}$ as a function of the code rate $R = \frac{k}{n}$. This bound is plotted in Figure 4.2.

Plotkin Upper Bound

The Plotkin upper bound is the result of a minimum weight argument. Lemma 4.3 and Lemma 4.4 give a very crude bound on $\frac{d}{2n}$. This bound is refined through applications of Lemma 4.5.

Lemma 4.3 The sum of the weights of an (n,k) binary linear block code C is $n2^{k-1}$.

Proof: The code C contains 2^k codewords. Let C_i denote the set of codewords of C which have a zero in the i^{th} position. Then C_i is a subspace of C. C_i contains 2^x codewords where x is an integer. We are assuming that C_i is not all of C because in this case the i^{th} position could be deleted from all codewords and not decrease tne minimum weight. The number of cosets of C_i in C is $\frac{|C|}{|C_i|} = 2^{k-x}$. Two codewords u and v which have a one in the i^{th} position are in the same coset of C_i because u-v has a zero in the i^{th} position and therefore $u-v \in C_i$. Therefore there are two cosets of C_i in C and each coset contains 2^x codewords. Since each codeword must appear in a coset, it follows that $2^k = 2^x \cdot 2$ or $x = k-1$. Then if the codewords of C are arranged as rows of a matrix, a zero appears 2^{k-1} times in each column and a one appears 2^{k-1} times in each column and the weight of each column is 2^{k-1}. Since there are n columns, the sum of the weights is $n2^{k-1}$. Q.E.D.

The following lemma gives a crude bound on the minimum distance of a linear block code C.

Lemma 4.4 The minimum distance d of an (n,k) linear block code satisfies the inequality $d \leq n2^{k-1}/(2^k-1)$.

Proof: The sum of the weights of the codewords of an (n,k) linear block code is $n2^{k-1}$ and there are 2^k-1 nonzero codewords. Therefore the average weight of the codewords is $n2^{k-1}/(2^k-1)$. The minimum weight (and hence the minimum distance) of the code is no greater than the average weight. Therefore $d \leq n2^{k-1}/(2^k-1)$. Q.E.D.

By the preceding lemma we have

$$\frac{d}{2n} \leq \frac{1}{4-\frac{1}{2^{k-2}}} \quad . \tag{4.7}$$

For large values of n and k (4.7) asymptotically becomes

$$\frac{d}{2n} \leq \frac{1}{4} \quad . \tag{4.8}$$

Although Lemma 4.4 gives only the crude bound expressed in (4.8), the following lemma provides for a substantial refinement.

Lemma 4.5 $B(n,d) \leq 2B(n-1,d)$ where $B(n,d)$ is the maximum number of codewords possible in an (n,k) linear block code C with minimum distance d.

Proof: Let C be an (n,k) linear block code with minimum distance d that has $B(n,d)$ codewords. The set C_i of all codewords in C whose last entry is zero forms a subspace of C since the sum of any two elements of C_i is in C_i and the scalar multiple of an element in C_i is in C_i. By the proof of Lemma 4.3 we know that $|C_i| = \frac{1}{2} \cdot B(n,d)$. The last component of each codeword of C_i can be dropped to give a linear code of $n-1$ symbols without affecting the number of codewords in C_i or the minimum distance. Thus C_i is an $(n-1, k')$ code with minimum distance d for some $k' \leq k$. Thus $|C_i| \leq B(n-1,d)$ so that $\frac{1}{2} B(n,d) \leq B(n-1,d)$ or $B(n,d) \leq 2B(n-1,d)$. Q.E.D.

For a code of block length i, the inequality appearing in Lemma 4.4 can be stated as follows:

$$d(2^k-1) \leq 2^{k-1} \quad \text{or}$$

$$2^{k-1}(2d-i) \leq d \quad .$$

If $2d-i > 0$, then

$$2^k = B(i,d) \leq \frac{2d}{2d-i} \quad .$$

Choose i such that $2d-1 = i$. Then

$$B(i,d) \leq \frac{2d}{2d-i} = 2d \quad .$$

If $n \geq i$, then repeated applications of Lemma 4.5 gives:

$$B(n,d) \leq 2^{n-i}B(i,d) \leq 2^{n-i}2d \quad \text{or}$$

$$B(n,d) \leq 2^{n-[2d-1]}2d \quad .$$

Since $B(n,d) = 2^k$ for some maximum value of k, the following inequality is obtained.

$$2^k \leq 2^{n-[2d-1]}2d$$

Application of the $\log_2(x)$ function to both sides of (4.9) gives

$$k \leq n-[2d-1] + 1 + \log_2 d \quad \text{or}$$

$$k \leq n-2d + 2 + \log_2 d \quad . \qquad (4.10)$$

For large values of d the last term in (4.10) is negligible compared to d. Therefore

$$2d \leq n-k + 2 \quad \text{or}$$

$$\frac{2d}{4n} \leq \frac{n-k+2}{4n} \qquad \text{or}$$

$$\frac{d}{2n} \leq \frac{1}{4} - \frac{k}{4n} + \frac{1}{2n} \quad . \tag{4.11}$$

Since $\lim_{n\to\infty} \frac{1}{2n} = 0$, (4.11) asymptotically becomes

$$\frac{d}{2n} \leq \frac{1}{4}(1-R) \quad .$$

This inequality is referred to as the Plotkin upper bound on $\frac{d}{2n}$ as a function of the code rate $R = \frac{k}{n}$. This bound is plotted in Figure 4.2. Note that the Plotkin upper bound is tighter than the Hamming upper bound on [0, .36].

Elias Upper Bound

Techniques used in deriving both the Hamming and Plotkin bounds are found in the derivation of the Elias upper bound. However asymptotically the Elias bound is tighter than either the Hamming or Plotkin bound.

Let C be an (n,k) linear block code. Number the n-tuples in the vector space F_n from 1 to 2^n. A sphere of radius r, where $r > 0$ and $\sum_{i=0}^{r} \binom{n}{j} > 2^{n-k}$, centered at the i^{th} n-tuple in F_n will contain a certain number of codewords of C, say M_i, $i = 1, 2, \ldots, 2^n$. Let $P_r^{(n)}$ represent the total number of n-tuples in each sphere. Then

$$P_r^{(n)} = \sum_{j=0}^{n} \binom{n}{j} \quad .$$

A codeword is at distance $\leq r$ from $\sum_{j=0}^{r} \binom{n}{j}$ n-tuples and therefore will appear in that number of the above 2^n spheres. Since there are 2^k codewords and each codeword appears in $\sum_{j=0}^{r} \binom{n}{j}$ spheres it follows that

$$\sum_{i=1}^{2^n} M_i = 2^k \sum_{j=0}^{r} \binom{n}{j} .$$

Let M denote the largest of the M_i. Then M is at least as large as the average of the M_i. Therefore:

$$M \geq \sum_{i=1}^{2^n} M_i$$

$$= \frac{2^k \sum_{j=0}^{r} \binom{n}{j}}{2^n}$$

$$= \frac{\sum_{j=0}^{r} \binom{n}{j}}{2^{n-k}} .$$

Note that $\frac{\sum_{j=0}^{r} \binom{n}{j}}{2^{n-k}} > 1$ because of the previous restriction on r. Among the 2^n spheres there exists a sphere of radius r containing M codewords since M is one of the M_i's.

The next step in determining the Elias bound is to find the average distance between these M codewords. Consider the translation of the sphere containing M codewords to the origin; that is, the center n-tuple is subtracted from each n-tuple in the sphere. Let the n-tuples obtained from subtracting the center n-tuple from the M codewords be denoted as follows:

$$\begin{matrix} (a_{11} & a_{12} & \cdots & a_{1n}) \\ (a_{21} & a_{22} & \cdots & a_{2n}) \\ \vdots & \vdots & & \vdots \\ (a_{M1} & a_{M2} & \cdots & a_{Mn}) \end{matrix} \qquad (4.12)$$

Let w_i denote the weight of the i^{th} of these n-tuples. Since the sphere has radius r and the center is now the zero vector, none of the n-tuples have weight greater than r. Therefore

$$\sum_{i=1}^{M} w_i \leq Mr \quad .$$

Let v_j denote the weight of the j^{th} column in (4.12). Then column j has v_j ones and $M-v_j$ zeros. It follows that

$$\sum_{i=1}^{n} v_j \leq Mr \tag{4.13}$$

since the number of ones in the n columns represents the total weight of the M n-tuples. The total distance, denoted d_{TOTAL}, between the M n-tuples in (4.12) is the sum of the $\binom{M}{2}$ distances between the n-tuples. The j^{th} column of (4.12) contributes the following to d_{TOTAL}:

$$\binom{M}{2} - \binom{v_j}{2} - \binom{M-v_j}{2} = v_j(M-v_j) \quad . \tag{4.14}$$

The term $\binom{v_j}{2}$ in (4.14) counts how many of the $\binom{M}{2}$ pairs of numbers in the j^{th} column are simultaneously one and therefore contribute nothing to the total distance. The $\binom{M-v_j}{2}$ term counts how many of the $\binom{M}{2}$ pairs contain zeros and therefore do not contribute to the distance. Summing over all the columns we obtain:

$$d_{TOTAL} = M\sum_{j=1}^{n} v_j - \sum_{j=1}^{n} v_j^2 \quad . \tag{4.15}$$

Since $\sum_{j=1}^{n} v_j \leq Mr$ (4.13), it follows that:

$$\sum_{j=1}^{n} v_j = Mr - \Delta, \ \Delta \geq 0 \ .$$

Therefore, for some m_j, we have:

$$v_j = \frac{Mr-\Delta}{n} + m_j \quad \text{or}$$

$$\sum_{i=1}^{n} v_j = \sum_{i=1}^{n} \frac{Mr-\Delta}{n} + m_j$$

$$= n\left(\frac{Mr-\Delta}{n}\right) + \sum_{j=1}^{n} m_j$$

$$= Mr - \Delta + \sum_{j=1}^{n} m_j$$

$$= \sum_{j=1}^{n} v_j + \sum_{j=1}^{n} m_j \quad .$$

It follows then that $\sum_{j=1}^{n} m_j = 0$. We use this fact to obtain a bound on $\sum_{j=1}^{n} v_j^2$.

$$\sum_{j=1}^{n} v_j^2 = \sum_{j=1}^{n} \left(\frac{Mr-\Delta}{n} + m_j\right)^2$$

$$= \sum_{j=1}^{n} \left[\left(\frac{Mr-\Delta}{n}\right)^2 + 2\left(\frac{Mr-\Delta}{n}\right)m_j + m_j^2\right]$$

$$n\left(\frac{Mr-\Delta}{n}\right)^2 + 2\left(\frac{Mr-\Delta}{n}\right)\sum_{j=1}^{n} m_j + \sum_{j=1}^{n} m_j^2$$

Since $\sum_{j=1}^{n} m_j = 0$ and $\sum_{j=1}^{n} m_j^2 \geq 0$, we have:

$$\sum_{j=1}^{n} v_j^2 \geq n\left(\frac{Mr-\Delta}{n}\right)^2 \quad .$$

Then, from equation (4.15), we have:

$$d_{TOTAL} \leq M(Mr-\Delta) - n\left(\frac{Mr-\Delta}{n}\right)^2$$

$$= rM^2\left(1-\frac{r}{n}\right) - \Delta n\left(1-\frac{2r}{n}\right) - \frac{\Delta^2}{n}$$

$$\leq rN^2(1-\frac{r}{n}) = \Delta n(1-\frac{2r}{n}) .$$

Since $r < \frac{n}{2}$ it follows that:

$$d_{TOTAL} \leq rM^2(1-\frac{r}{n}) .$$

Of the $\binom{M}{2}$ distances at least one is not greater than the average. Denote this distance d. Then

$$d \leq \frac{d_{TOTAL}}{\binom{M}{2}}$$

$$\leq \frac{rM^2(1-\frac{r}{n})}{\frac{M(M-1)}{2}}$$

$$= 2r(1-\frac{r}{n})(\frac{M}{M-1}) \qquad \text{or}$$

$$\frac{d}{2n} \leq \frac{r}{n}(1-\frac{r}{n})(\frac{M}{M-1}) \qquad (4.16)$$

For large values of n, $\lim_{n\to\infty} \frac{M}{M-1} = 1$ and $\lim_{n\to\infty} \frac{r}{n} = F^{-1}(R)$ [3]. Therefore the limiting form of (4.16) is:

$$\frac{d}{2n} \leq F^{-1}(R)(1-F^{-1}(R)) . \qquad (4.17)$$

Inequality (4.17) is referred to as the Elias upper bound and is plotted in Figure 4.2.

McEliece Upper Bound

McEliece recently derived the following bound on $\frac{d}{2n}$ using linear programming techniques.

$$\frac{d}{2n} \leq \frac{1}{4} - \frac{1}{2}\sqrt{F^{-1}(1-R)[1-F^{-1}(R)]}$$

The McEliece upper bound is plotted in Figure 4.2. Note that the McEliece bound is tighter than the Elias bound on [0, .68].

Gilbert Lower Bound

The Gilbert lower bound on $\frac{d}{2n}$ as a function of code rate $R = \frac{k}{n}$ is derived through the construction of an (n,k) linear block code with large minimum distance. Theorem 2.2 is the basis for this construction. This theorem states that a block code that is the nullspace of a matrix H has minimum weight (and hence minimum distance) d if and only if every linear combination of d-1 or fewer columns of H is linearly independent.

A linear block code with n-k parity check symbols and minimum weight d can be constructed using the following method. Select any two nonzero n-k tuples as the first and second columns of a parity check matrix. The third column is chosen to be any nonzero n-k tuple which is not a linear combination of the first two columns. In general, the i^{th} column of the parity check matrix is chosen as any n-k tuple that is not a linear combination of d-2 or fewer preceding columns of the matrix. Note that this construction guarantees that no linear combination of d-1 or fewer columns of the parity check matrix will be zero. There are

$$\binom{j-1}{1} + \binom{j-1}{2} + \ldots + \binom{j-1}{d-2} \qquad (4.18)$$

linear combinations of d-2 or fewer columns out of a total of j-1 columns. In the worst case these linear combinations may all be distinct. If the number in (4.18) is less than $2^{n-k}-1$, the total number of

nonzero $n-k$ tuples, then there exists at least one $n-k$ tuple that is not a linear combination of $d-2$ or fewer of the $j-1$ columns. Therefore at least one more column could be added to the parity check matrix and we are assured by Theorem 2.2 that there exists a code of block length j with minimum distance d and $n-k$ parity check symbols.

For each fixed value of $n-k$, let n be the largest value for which the following inequality holds:

$$\binom{n-1}{1} + \binom{n-1}{2} + \ldots + \binom{n-1}{d-2} < 2^{n-k}-1 .$$

Then there exists a code of block length n with minimum distance d and $n-k$ parity check symbols. This is alternately stated in the following theorem.

Theorem 4.1 Let n be the smallest value satisfying $\sum_{i=0}^{d-2}\binom{n}{i} \geq 2^{n-k}$.
Then there exists an (n,k) linear block code with minimum distance d.

The Chernoff bound on a certain sum of binomial coefficients is used to obtain the following inequality.

$$\begin{aligned}
2^{n-k} &\leq \sum_{i=0}^{d-2}\binom{n}{i} = \sum_{i=n-d+2}^{n}\binom{n}{i} \\
&\leq \left(\frac{n-d+2}{n}\right)^{-(n-d+2)}\left(\frac{d-2}{n}\right)^{-(d-2)} \\
&= 2^{\log_2\left(\frac{n-d+2}{n}\right)^{-(n-d+2)} + \log_2\left(\frac{d-2}{n}\right)^{-(d-2)}} \\
&= 2^{-(n-d+2)\log_2\left(\frac{n-d+2}{n}\right) - (d-2)\log_2\left(\frac{d-2}{n}\right)} \\
&= 2^{n\left[-\left(\frac{n-d+2}{n}\right)\log_2\left(\frac{n-d+2}{n}\right) - \left(\frac{d-2}{n}\right)\log_2\left(\frac{d-2}{n}\right)\right]}
\end{aligned}$$

$$= 2^{n[1-(1+(\frac{n-d+2}{n})\log_2(\frac{n-d+2}{n})+(\frac{d-2}{n})\log_2(\frac{d-2}{n})]}$$

$$= 2^{n[1-(1+(1-\frac{d-2}{n})\log_2(1-\frac{d-2}{n})+\frac{d-2}{n}\log_2(\frac{d-2}{n})]}$$

or

$$2^{n-k} = 2^{n[1-F(\frac{d-2}{n})]} \tag{4.19}$$

If we apply $\log_2(x)$ function to both sides of (4.19) the inequality becomes:

$$n-k \leq n[1-F(\frac{d-2}{n})] \quad \text{or}$$

$$1-R \leq 1-F(\frac{d-2}{n}) \quad \text{or}$$

$$R \geq F(\frac{d-2}{n}) \ . \tag{4.20}$$

If we apply F^{-1} to (4.20) the inequality is reversed and we obtain:

$$F^{-1}(R) \leq F^{-1}(F(\frac{d-2}{n})) = \frac{d-2}{n} \quad \text{or}$$

$$\frac{d}{2n} \geq F^{-1}(R) + \frac{2}{n} \ . \tag{4.21}$$

Since, $\lim_{n\to\infty} \frac{2}{n} = 0$, the limiting form of (4.21) is:

$$\frac{d}{2n} \geq F^{-1}(R) \ .$$

This asymptotic form is referred to as the Gilbert lower bound on $\frac{d}{2n}$ as a function of a code rate $R = \frac{k}{n}$ and is plotted in Figure 4.2.

The Gilbert and Hamming bounds were the first published bounds on the minimum distance of a block code. The gap between the two bounds has been decreased through derivations of tighter upper bounds. However the Gilbert lower bound was published in 1952 and still remains the tightest known asymptotic lower bound. There have been improvements on Gilbert's bound but only for block lengths in restricted ranges. Most coding theorists believe that the Gilbert bound is very close to the true value of $\frac{d}{2n}$ as a function of a fixed code rate for large block lengths.

Figure 4.1 Graph of F(P)

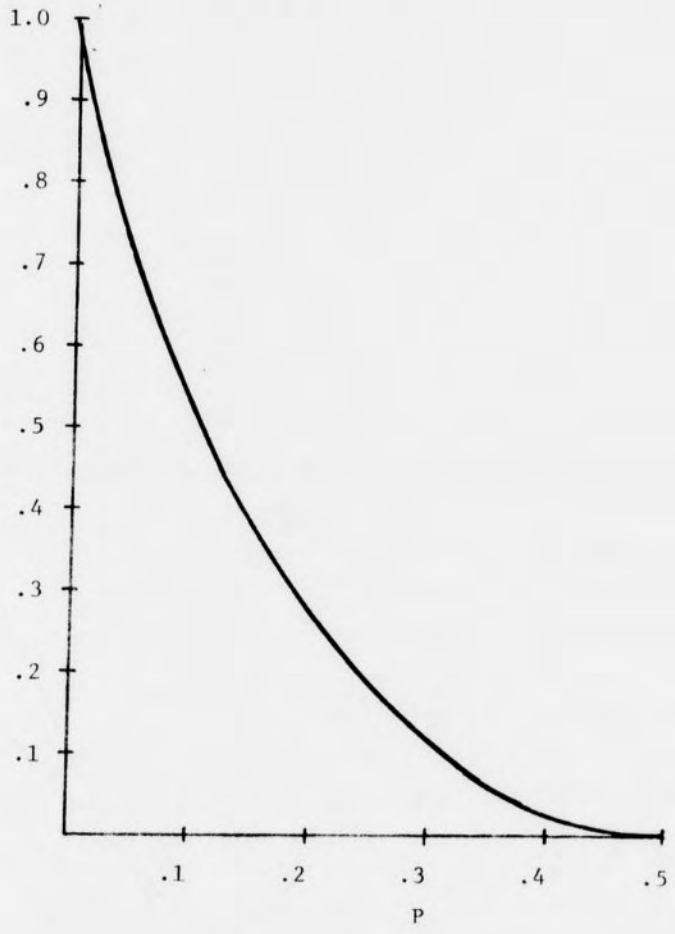
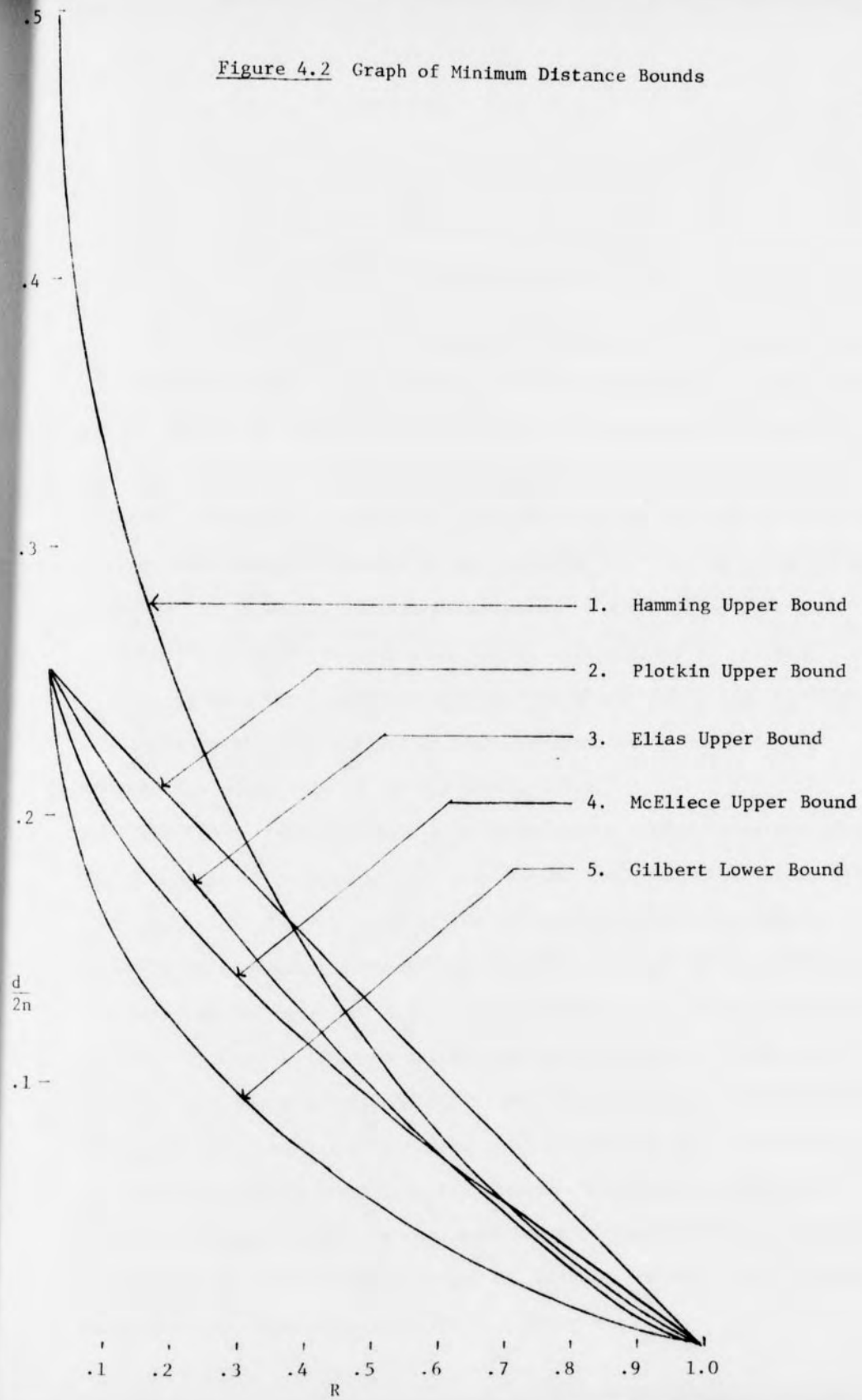


TABLE OF VALUES

P	F(P)
.00	1.0000
.02	.8585
.04	.7577
.06	.6725
.08	.5978
.10	.5310
.12	.4706
.14	.4158
.16	.3657
.18	.3120
.20	.2780
.22	.2400
.24	.2049
.26	.1732
.28	.1445
.30	.1186
.32	.0956
.34	.0752
.36	.0573
.38	.0419
.40	.0213
.42	.0185
.44	.0104
.46	.0046
.48	.0011
.50	.0000

Figure 4.2 Graph of Minimum Distance Bounds



CHAPTER V

A REFINEMENT OF THE GILBERT LOWER BOUND

In this chapter we will present a refinement of the argument used by Gilbert to derive a lower bound on the maximum number n, of columns in an $(n-k) \times n$ binary matrix H, any $d-1$ of which are linearly independent. Such a maximum parity check matrix H is constructed as follows. Successive columns are added on from left to right so that the linear independence condition is not violated; that is, each new column added to H is not a linear combination of $d-2$ or fewer previous columns. The reader is cautioned that not all choices of columns satisfying even this condition will lead to a maximum matrix. In this chapter we will further restrict this construction by assuming that columns are added onto H by increasing weight.

The first $(n-k)$ columns of a parity check matrix described above are chosen to be the $(n-k)$ tuples of weight one. Note that every linear combination of $d-1$ or fewer of the $(n-k)$ tuples of weight one is linearly independent. Also any $(n-k)$ tuple of weight greater than one and less than or equal to $d-2$ can be expressed as a linear combination of $d-2$ or fewer weight one columns and therefore these columns are not added to H. The next columns of H are chosen to be any $(n-k)$ tuples of weight $d-1$ which are not linear combinations of $d-2$ or fewer previous columns. Note that we are assured of adding at least one column of weight $d-1$ since no $(n-k)$ tuple of weight $d-1$ is a linear combination of $d-2$ or fewer weight one columns. Assume $r-1$ columns of weight $d-1$ have been added to H. There are

$$\sum_{j=1}^{d-2} \binom{n_1+(r-1)}{j}, \quad \text{where} \quad n_1 = (n-k), \tag{5.1}$$

ways of choosing $d-2$ or fewer columns from the existing matrix. If the number in (5.1) is less than the total number of non-zero $(n-k)$ tuples of weight $d-1$ or less, than at least one more column of weight $d-1$ can be added to the matrix; that is, if

$$\sum_{j=1}^{d-2} \binom{n_1+(r-1)}{j} < \sum_{L=1}^{d-1} \binom{n-k}{L}, \tag{5.2}$$

then there exists a code of block length (n_1+r) with minimum distance d and $(n-k)$ parity check symbols. Let n_{d-1} denote the largest value of r for which Inequality (5.2) holds. Then we are assured that at least n_{d-1} columns of weight $d-1$ can be added to H. The construction of H continues in the same manner with each subsequent weight considered. Assume we are at the step in the construction of H when columns of weight i are first being added to the matrix. At this stage not all additional columns added onto H are necessarily of weight i. Of course we would choose a column of weight i if it were available. Assume that at this step x columns of weight less than or equal to i have been added to H. If

$$\sum_{j=1}^{d-2} \binom{n_1+n_{d-1}+\ldots+(x-1)}{j} < \sum_{L=1}^{i} \binom{n-k}{L} \tag{5.3}$$

then there exists at least one more column of weight less than or equal to i that can be added to H. Let n_i be the largest value of x for which Inequality (5.3) holds. Then we are guaranteed that n_i additional columns of weight less than or equal to i can be added to H at this

stage. Thus there exists a block code of length $(n_1+n_{d-1}+\ldots+n_i)$ with minimum distance d and $(n-k)$ parity check symbols. This procedure is followed for each weight i, $d-1 \leq i \leq n-k$, as is stated in the following theorem.

Theorem 5.1 For a fixed $n-k$ and d, let $n = \sum_{i=1}^{n-k} n_i$ where n_i is defined as follows:

$n_1 = n-k$

$n_2 = n_3 = \ldots = n_{d-2} = 0$

$n_i (d-1 \leq i \leq n-k)$ is the largest value for which the following inequality holds:

$$\sum_{j=1}^{d-2} \binom{n_1+n_2+\ldots+(n_i-1)}{j} < \sum_{L=1}^{i} \binom{n-k}{L} .$$

Then there exists an (n,k) linear block code with minimum distance d. Notice that since the right side of the inequality above is a monotonically increasing function of i, each $n_i \geq 0$ and thus we could have defined each $n_i (d-1 \leq i \leq n-k)$ alternately as the smallest value satisfying:

$$\sum_{j=1}^{d-2} \binom{n_1+n_2+\ldots+n_i}{j} \geq \sum_{L=1}^{i} \binom{n-k}{L} .$$

However the following corollary shows that this lower bound is no better than the lower bound given by Gilbert.

Corollary 5.1 For a fixed $(n-k)$ and d, let $n_T = \sum_{i=1}^{n-k} n_i$ where n_i is defined in Theorem 5.1 and let n_G be the lower bound given by Gilbert. Then $n_T = n_G$.

Proof: n_G is the minimum value of n satisfying

$$\sum_{j=1}^{d-2} \binom{n}{j} \geq \sum_{L=1}^{n-k} \binom{n-k}{L} .$$

By Theorem 5.1 we know

$$\sum_{j=1}^{d-2} \binom{n_T-1}{j} < \sum_{L=1}^{n-k} \binom{n-k}{L} .$$

Since n_G is the maximum such value satisfying the above, $n_G \geq n_T$. It is also true that

$$\sum_{j=1}^{d-2} \binom{n_T}{j} \geq \sum_{L=1}^{n-k} \binom{n-k}{L} .$$

But n_G is the minimum such value satisfying the above. Therefore $n_G \leq n_T$ and thus $n_G = n_T$. Q.E.D.

Although the overall results of Theorem 5.1 are disappointing it can be shown, using the inequality in the theorem, that for certain values of $n-k$ and d, codes meeting the bound of the theorem (and Gilbert's bound) have parity check matrices consisting of low weight columns. For example, for $n-k = 7$, $d = 5$ there exists a 7×10 parity check matrix for a $(10, 3)$ linear block code which contains seven columns of weight one and 3 columns of weight 4.

The results of the following lemmas will be used in the proof of Theorem 5.2. The theorem provides bounds on the number of columns of weight i that can be added to a parity check matrix H. The argument used in the proof is a refinement of the proof of Theorem 5.1.

Lemma 5.1 Let u and v be n-tuples. Then $w(u+v) = w(u)+w(v)-2(u\cdot v)$, where $(u\cdot v)$ is the inner product of u and v.

Proof: Let $u = (u_1 u_2 \ldots u_n)$ and $v = (v_1 v_2 \ldots v_n)$. The numbers $w(u)$ and the $w(v)$ are the total number of 1's in u and v, respectively. There are $(u\cdot v)$ positions in which $u_i = v_i = 1$. If $u_i = v_i = 1$,

then $u_i + v_i = 0$. Therefore $w(u) + w(v)$ includes in its count $2(u \cdot v)$ 1's which do not contribute to the weight of $u + v$. Thus

$$w(u+v) = w(u) + w(v) - 2(u \cdot v) \ . \qquad \text{Q.E.D.}$$

The results of the preceding lemma are used in the derivation of the weight of the sum of an arbitrary number of n-tuples.

Lemma 5.2 Let $u_1, u_2, \ldots, u_n$ be (n-k) tuples. Then $w(u_1+u_2+\ldots+u_n) = \sum_{i=1}^{n} w(u_i) - 2\sum_{1 \le i \le j \le n} (u_i \cdot u_j)$.

Proof: We use induction on n. If n=1, then $w(u_1) = w(u_1)$. For the inductive step assume that

$$w(u_1+u_2+\ldots+u_k) = \sum_{i=1}^{k} w(u_i) - 2\sum_{1 \le i \le j \le k} (u_i \cdot u_j) \ .$$

Then $w(u_1+u_2+\ldots+u_k+u_{k+1}) = w(x+u_{k+1})$ where $x = u_1+u_2+\ldots+u_k$. Since $w(z+y) = w(z) + w(y) - 2(z \cdot y)$ it follows that

$$\begin{aligned}
w(u_1+u_2+\ldots+u_k+u_{k+1}) &= w(x+u_{k+1}) \\
&= w(x) + w(u_{k+1}) - 2(x \cdot u_{k+1}) \\
&= w(u_1+u_2+\ldots+u_k) + w(u_{k+1}) - 2((u_1+u_2+\ldots+u_k) \cdot u_{k+1}) \\
&= \sum_{i=1}^{k} w(u_i) - 2\sum_{1 \le i \le j \le k} (u_i \cdot u_j) + w(u_{k+1}) \\
&\quad - 2((u_i \cdot u_{k+1}) + (u_2 \cdot u_{k+1}) + \ldots + (u_k \cdot u_{k+1})) \\
&= \sum_{i=1}^{k+1} w(u_i) - 2\sum_{1 \le i \le j \le k} (u_i \cdot u_j) - 2\sum_{i=1}^{k} (u_i \cdot u_{k+1}) \\
&= \sum_{i=1}^{k+1} w(u_i) - 2\sum_{1 \le i \le j \le k+1} (u_i \cdot u_j) \ . \qquad \text{Q.E.D.}
\end{aligned}$$

From the above lemma we know that if the sum of the weights of a set of (n-k) tuples is odd (even) then the linear combination of the tuples is odd (even).

Theorem 5.2 For a fixed n-k and d, let $n = \sum_{i=1}^{n-k} n_i$ where n_i is defined as follows:

$n_1 = n-k$

$n_2 = \ldots = n_{d-2} = 0$

$n_i (d-1 \le i \le n-k)$ is the smallest value for which

$$(k_1 \ldots k_i)\binom{n_1}{k_1}\ldots\binom{n_i}{k_i} - \sum_{j=d-1}^{i} n_j \left[\binom{j}{x}\binom{n-k-j}{y}\right] \ge \binom{n-k}{i} .$$

$0 \le k_j \le n_j$; $1 \le x+y \le d-3$

$\Sigma k_j \le d-2$; $j+x+y \ge i$

$i \le \Sigma j k_j$ odd if i odd ; $(j-x)+y \ne i$

even if i even ; $(x+y)-(1+j)$ even

Then there exists an (n,k) linear block code C with minimum distance d. There exists a parity check matrix H for C such that H contains n_i columns of weight i.

Proof: A parity check matrix H for a linear block code with n-k parity check symbols and minimum distance d associated with the parameters $n_1, n_2, \ldots, n_{n-k}$ above can be constructed as follows. The first (n-k) columns of H are chosen to be the (n-k) tuples of weight one. Since any n-k tuple of weight greater than one and less than or equal to d-2 can be written as a linear combination of d-2 or fewer weight one columns, we set $n_2 = \ldots = n_{d-2} = 0$. Assume $n_j (1 \le j \le i-1)$

columns of weight j have been added to H without violating the condition that all $d-1$ or fewer columns are linearly independent and we are at the step in the construction of H where columns of weight i are being added. Further assume that r columns of weight i have already been included in H. There are

$$\begin{aligned} &\left(k_1 \overset{\Sigma}{\ldots} k_i\right)\binom{n_1}{k_1}\ldots\binom{n_{i-1}}{k_{i-1}}\binom{r}{k_i} \\ &0 \le k_j \le n_j \\ &1 \le \Sigma k_j \le d-2 \end{aligned} \tag{5.4}$$

linear combinations of $d-2$ or fewer columns of the existing matrix. For $(k_1 \ldots k_i)$, if $\Sigma j k_j < i$ or if $\Sigma j k_j$ is odd and i is even (or vice versa), then by Lemma 5.2 those column choices do not yield weight i tuples. Therefore of the linear combinations in (5.4) at most

$$\begin{aligned} &\left(k_1 \overset{\Sigma}{\ldots} k_i\right)\binom{n_1}{k_1}\ldots\binom{n_{i-1}}{k_{i-1}}\binom{r}{k_i} \\ &0 \le k_j \le n_j \\ &1 \le \Sigma k_j \le d-2 \\ &i \le \Sigma j k_j \begin{cases} \text{odd if } i \text{ odd} \\ \text{even if } i \text{ even} \end{cases} \end{aligned} \tag{5.5}$$

of them result in $(n-k)$ tuples of weight i. Consider the linear combination of a weight $j (d-1 \le j \le i)$ column and $d-3$ or fewer weight one columns. If x of the weight one columns have 1's in the positions where the weight j column has 1's and y of the weight one columns have 1's in positions where the weight j column has 0's, then the resulting $(n-k)$ tuple has weight $(j-x)+y$. If $(j-x)+y \neq i$ then the

linear combination does not yield an (n-k) tuple of weight i. For each weight j, there are at least

$$n_j \sum_{\substack{x+y \le d-3 \\ j+x+y \ge i \\ (j-x)+y \neq i \\ (x+y)-(i+j) \text{ even}}} \left[\binom{j}{x}\binom{(n-k)-j}{}\right]$$

of the total number of linear combinations in (5.5) which involve one column of weight j and d-3 columns of weight one and do not result in an (n-k) tuple of weight i. Therefore there are at most

$$\sum_{\substack{0\le k_j\le n_j \\ 1\le \Sigma k_j\le d-2 \\ i\le \Sigma jk_j \begin{cases} \text{odd if } i \text{ odd} \\ \text{even if } i \text{ even} \end{cases}}} \binom{n_1}{k_1}\cdots\binom{n_{i-1}}{k_{i-1}}\binom{r}{k_i} - \left[\sum_{j=d-1}^{i-1} n_j\left[\binom{j}{x}\binom{(n-k)-j}{y}\right] + r\binom{i}{x}\binom{(n-k)-i}{y}\right]$$

$$\begin{array}{l} x+y\le d-3 \\ j+x+y\ge i \\ (j-x)+y \neq i \\ (x+y)-(i+j) \text{ even} \end{array} \qquad (5.6)$$

linear combinations of d-2 or fewer columns of the existing matrix which yield (n-k) tuples of weight i. If the number in (5.6) is less than $\binom{n-k}{i}$, the total number of (n-k) tuples of weight i, then another column of weight i can be added to the matrix. Let n_i-1 be the largest value of r such that the number in (5.6) is less than $\binom{n-k}{i}$. Then at least n_i columns of weight i can be added to the matrix. That is, let n_i be the smallest value satisfying

$$(k_1 \overset{\Sigma}{\ldots} k_i)\binom{n_1}{k_1}\ldots\binom{n_i}{k_i} - \sum_{j=d-1}^{i} n_j\left[\binom{j}{x}\binom{(n-k)-j}{y}\right] \geq \binom{n-k}{i}.$$

$0 \leq k_j \leq n_j$ $\qquad$ $x+y \leq d-3$

$1 \leq \Sigma k_j \leq d-2$ $\qquad$ $j+x+y \geq i$

$i \leq \Sigma j k_j$ $\begin{cases} \text{odd if } i \text{ odd} \\ \text{even if } i \text{ even} \end{cases}$ $\qquad$ $(j-x)+y \neq i$

$\qquad\qquad\qquad\qquad\qquad\qquad$ $(x+y)-(i+j)$ even

Then there exists an $(\sum_{j=1}^{i} n_j, k)$ linear block code C with minimum distance d. There exists a parity check matrix H for C such that H contains n_i columns of weight i. Q.E.D.

Lower bound values on the maximum block length n for a fixed $n-k$ $(5 \leq n-k \leq 11)$ and $d (4 \leq d \leq 10)$ given by Theorem 5.2 appear in Table 5.1. For each $n-k,d$ value, the value of n derived using Gilbert's bound is also given. In most cases Theorem 5.2 gives a tighter bound on n than does Gilbert. In addition Theorem 5.2 states that parity check matrices can be constructed for codes meeting the bound given by the theorem such that the parity check matrices contain n_i columns of weight i. For each $n-k,d,n$ value in Table 5.1 the values of the n_i's are also given.

TABLE 5.1

LOWER BOUNDS ON MAXIMUM BLOCK LENGTH

n-k \ d	4	5	6	7	8	9	10
5	6 16 (5,15,0,1)	6 6 (5,1,0)	6				
6	11 32 (6,20,0,6,0)	7 8 (6,2,0,0)	7 7 (6,1,0)	7 7 (6,1)			
7	16 64 (7,35,0,21,0,1)	9 10 (7,3,0,0,0)	8 9 (7,2,0,0)	8 8 (7,1,0)	8 8 (7,1)		
8	23 128 (8,56,0,56,0, 8,0)	12 12 (8,4,0,0,0,0)	9 11 (8,3,0,0,0)	9 10 (8,2,0,0)	9 9 (8,1,0)	9 (8,1)	
9	256 32 (9,84,0,126,0 36,0,1)	15 15 (9,6,0,0,0, 0,0)	11 13 (9,4,0,0,0,0)	10 11 (9,2,0,0,0)	10 10 (8,2,0,0)	10 10 (9,1,0)	10 10 (9,1)
10	45 512 (10,120,0,252, 0,120,0,10,0)	19 19 (10,7,0,2,0, 0,0)	13 16 (10,6,0,0,0, 0,0)	11 12 (10,2,0,0,0,0)	11 12 (10,2,0,0,0)	11 11 (10,1,0,0)	11 11 (10,1,0)
11	1024 64 (11,165,0,462,0, 330,0,55,0,1)	23 23 (11,8,2,2,0,0, 0,0,0)	16 18 (11,7,0,0,0,0, 0,0)	13 14 (11,2,1,0,0, 0,0)	12 13 (11,2,0,0,0,0)	12 12 (11,1,0,0,0)	12 12 (11,1,0,0)

Gilbert's lower bound on n for fixed n-k,d.

Theorem 5.2 lower bound on n for fixed n-k,d.
Parity check matrix parameters.

CHAPTER VI

A REFINEMENT OF THE HAMMING UPPER BOUND

In this chapter we will present a refinement of the Hamming upper bound on the maximum number n, of columns possible in an $(n-k) \times n$ parity check matrix H satisfying the condition that any set of $d-1$ columns is linearly independent. An alternate proof of Hamming's bound will first be given. Two other theorems whose results are also used in the derivation of the refinement will be presented.

The following theorem states that every linear combination of $\frac{d-1}{2}$ or fewer columns of an $(n-k) \times n$ parity check matrix H produces a distinct $(n-k)$ tuple.

Theorem 6.1 Let H be a parity check matrix for a linear block code with minimum distance d. Then every linear combination of $\frac{d-1}{2}$ or fewer columns of H is distinct.

Proof: By Theorem 2.2 we know that every linear combination of $d-1$ or fewer columns of H is linearly independent. Assume not all linear combinations of $\frac{d-1}{2}$ or fewer columns of H are distinct. Let $\{m_{i1}, m_{i2}, \cdots m_{ij}\}$, $j \leq \frac{d-1}{2}$, and $\{r_{i1}, r_{i2}, \cdots r_{iq}\}$, $q \leq \frac{d-1}{2}$, be columns of H. If

$$m_{i1} + m_{i2} + \ldots + m_{ij} = r_{i1} + r_{i2} + \ldots + r_{iq},$$

then

$$m_{i1} + m_{i2} + \ldots + m_{ij} + r_{i1} + r_{i2} + r_{iq} = 0.$$

But this is a linear dependence relationship among d-1 or fewer colunms of H. Therefore every linear combination of $\frac{d-1}{2}$ or fewer columns of H is distinct. Q.E.D.

The results of the preceding theorem are used in the following proof of Hamming's upper bound.

Theorem 6.2 Let C be an (n,k) linear block code with minimum distance d. Then n satisfies the following inequality:

$$\sum_{i=1}^{\frac{d-1}{2}} \binom{n}{i} \leq 2^{n-k}-1 .$$

Proof: Let H be an (n-k) × n parity check matrix for C. Then by Theorem 6.1 every linear combination of $\frac{d-1}{2}$ or fewer columns of H is distinct. Since the number of distinct linear combinations cannot exceed the total number of nonzero (n-k) tuples, it follows that:

$$\sum_{i=1}^{\frac{d-1}{2}} \binom{n}{i} \leq 2^{n-k}-1 .$$ Q.E.D.

The following theorem states that a parity check matrix of maximum block length satisfying the linear independence condition has full rank.

Theorem 6.3 Let H be an (n-k) × n parity check matrix containing the maximum number n, of columns possible such that every set of d-1 or fewer columns of H is linearly independent. Then H has rank n-k.

Proof: Assume H has rank <n-k. Then H can be row reduced to a matrix H' containing at least one row of zeroes, say row i. Every linear combination of d-1 or fewer columns of H' is linearly

independent since row reduction does not affect the linear independence relationships among the columns. Column e_i (1 in the i^{th} position) can be added to H' and every set of d-1 or fewer columns of H' will still be linearly independent since every other column has a 0 in the i^{th} position. But this contradicts the fact that H, and therefore H', is maximum size. Therefore the rank of H is n-k. Q.E.D.

For a given parity check matrix H, the following lemma provides bounds on the weight of the linear combination of certain columns of H.

Lemma 6.1 Assume H is an (n-k) × n parity check matrix for an (n,k) linear block code with minimum distance d and H contains all the n-k unit columns. If u_j, is a column of weight $\neq 1$ from H, then

$$w(\sum_{i=1}^{j} u_i) \geq d-j \ .$$

Proof: Clearly $w(u_j) \geq d-1$ since H contains all the (n-k) tuples of weight one and each (n-k) tuple of weight $< d-1$ is a linear combination of d-2 or fewer weight one columns. Assume

$$w(\sum_{i=1}^{j} u_i) < d-j \ .$$

Let $x = w(\sum_{i=1}^{j} u_i)$. Then

$$x < d-j$$

$$x+j < d \quad \text{or}$$

$$x+j \leq d-1.$$

Let $\sum_{i=1}^{x} u_i = v$. Then v contains x ones. The linear combination of v with the x unit columns which have 1's in the same positions as v is equal to zero. But that is a linear combination of $\leq d-1$ columns of H since $x+j \leq d-1$ and $v = \sum_{i=1}^{j} u_j$. Therefore $w(\sum_{i=1}^{j} u_i) \geq d-j$. Q.E.D.

The following theorem provides a bound on the maximum number n of columns possible in an $(n-k) \times n$ parity check matrix H such that the linear independence condition is satisfied. It is assumed that H contains $n-k$ columns of weight one since by Theorem 6.3 any maximum parity check matrix can be row reduced to a matrix containing all the $(n-k)$ tuples of weight one.

Theorem 6.4 For a fixed $n-k$ and d, d even, let H be an $(n-k) \times n$ parity check matrix containing the maximum number, $N(=n)$, of columns possible such that every set of $d-1$ of fewer columns of H is linearly independent. Let n_i denote the columns of H of weight i where $n_1 = n-k$, $n_2 = \ldots = n_{d-2} = 0$, $\sum_{i=d-1}^{n-k} n_i = N-(n-k)$. Then

$$\sum_{j=1}^{[\frac{d-1}{2}]} \binom{N}{j} \leq \sum_{\substack{m=1 \\ m \neq \frac{d}{2}}}^{n-k} \binom{n-k}{m} .$$

Proof: Let $[x]$ denote the largest integer smaller than or equal to x and let (x) denote the smallest integer larger than or equal to x. Consider the linear combination of $[\frac{d-1}{2}]$ or fewer columns of H involv- involving x columns, $1 \leq x \leq 1[\frac{d-1}{2}]$ of weight $\geq d-1$ and y columns, $y \leq [\frac{d-1}{2}]-x$, of weight one. Let u denote the sum of the x columns of weight d-1. Then by Lemma 6.1, $w(u) \geq d-x$. Let v denote the sum of the y columns of weight one. Then $w(v) = y$ and if $y = 0$, then

$v = 0$. By Lemma 5.1, it follows that

$$w(u+v) = w(u) + w(v) - 2w(u\cdot v) \geq d-x+y - 2(u\cdot v).$$

The most number of corresponding 1's that u and v can have is $w(v) = y$. Therefore $(u\cdot v)\leq y$ and

$$\begin{aligned} w(u+v) &\geq d-x + y - 2y \\ &= d-x-y \\ &= d-(x+y) \end{aligned}$$

Since $x + y \leq [\frac{d-1}{2}]$,

$$w(u+v) \geq d-[\frac{d-1}{2}] = (\frac{d+1}{2}).$$

Therefore each linear combination of $[\frac{d-1}{2}]$ or fewer columns of H involving at least one column of weight $\geq d-1$ yields an $(n-k)$ tuple of weight $\geq (\frac{d+1}{2})$. There are

$$\sum_{\substack{x+y\leq [\frac{d-1}{2}] \\ x\geq 1}} \binom{n-k}{y}\binom{N-(n-k)}{x} \tag{6.1}$$

such linear combinations. Since these are linear combinations of $[\frac{d-1}{2}]$ or fewer columns of H, by Theorem 6.1, they are distinct and since each yields an $(n-k)$ tuple of weight $\geq(\frac{d+1}{2})$, the number in 6.1 cannot exceed the total number of $(n-k)$ tuples of weight $\geq(\frac{d+1}{2})$. That is,

$$\sum_{\substack{x+y\leq [\frac{d-1}{2}] \\ x\geq 1}} \binom{n-k}{y}\binom{N-(n-k)}{x} \leq \sum_{m=(\frac{d+1}{2})}^{n-k} \binom{n-k}{m} . \tag{6.2}$$

The number on the left side of the above inequality is the total number of linear combinations of $[\frac{d-1}{2}]$ or fewer columns of H except those which involve only columns of weight one. Therefore

$$\sum_{\substack{x+y\le[\frac{d-1}{2}] \\ x\ge 1}} \binom{n-k}{y}\binom{N-(n-k)}{x} = \sum_{j=1}^{[\frac{d-1}{2}]} \binom{N}{j} - \sum_{i=1}^{[\frac{d-1}{2}]} \binom{n-k}{i} .$$

Then (6.2) becomes:

$$\sum_{j=1}^{[\frac{d-1}{2}]} \binom{N}{j} - \sum_{i=1}^{[\frac{d-1}{2}]} \binom{n-k}{i} \le \sum_{m=(\frac{d+1}{2})}^{n-k} \binom{n-k}{m} , \text{ or}$$

$$\sum_{j=1}^{[\frac{d-1}{2}]} \binom{N}{j} \le \sum_{i=1}^{[\frac{d-1}{2}]} \binom{n-k}{i} + \sum_{m=(\frac{d+1}{2})}^{n-k} \binom{n-k}{m} \qquad (6.3)$$

If d is odd, then

$$[\tfrac{d-1}{2}] + 1 = \tfrac{d-1}{2} + 1 = \tfrac{d+1}{2} = (\tfrac{d+1}{2})$$

and the right side of (6.3) is equal to $2^{n-k}-1$. The inequality then yields Hamming's bound. However, if d is even, then

$$[\tfrac{d-1}{2}] + 1 = (\tfrac{d-1}{2} - \tfrac{1}{2}) + 1 = \tfrac{d}{2} = (\tfrac{d+1}{2} + \tfrac{1}{2}) - 1 = (\tfrac{d+1}{2}) - 1$$

and the term $\binom{n-k}{d/2}$ does not appear in the sum. Therefore for even d,

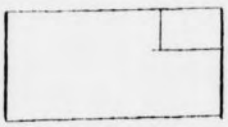
$$\sum_{j=1}^{[\frac{d-1}{2}]} \binom{N}{j} \leq 2^{n-k}-1-\binom{n-k}{\frac{d}{2}} = \sum_{\substack{m=1 \\ m\neq\frac{d}{2}}}^{n-k} \binom{n-k}{m}. \qquad \text{Q.E.D.}$$

Upper bounds given by Theorem 6.4 on the maximum value of n for a fixed $n-k (7 \leq n-k \leq 12)$ and even d $(6 \leq d \leq 10)$ are presented in Table 6.1. The value of n given by Hamming for each $n-k$, d value also appears in the table. Notice that Theorem 6.4 gives a tighter bound on n than does Hamming for each $n-k,d$ value shown.

TABLE 6.1

UPPER BOUNDS ON MAXIMUM BLOCK LENGTH

n-k \ d	6	8	10
7	13	8	
	15	9	
8	19	10	
	22	11	
9	28	13	10
	31	14	10
10	42	16	11
	44	18	12
11	60	21	14
	63	23	15
12	87	27	17
	90	29	18



Hamming's bound

Theorem 6.4 bound

BIBLIOGRAPHY

[1] Berlekamp, Elwyn. Algebraic Coding Theory. New York: McGraw Hill Book Company, 1968.

[2] Feinstein, A. Foundations of Information Theory. New York: McGraw Hill Book Company, 1958.

[3] Peterson, W. Wesley and Weldon, E.J. Jr. Error-Correcting Codes. Cambridge: The M.I.T. Press, 1972.

[4] Shannon, C. E. "A Mathematical Theory of Communication." Bell System Technical Journal, V. 27 (1948), 379-423.

[5] van Lint, Jacobus H. "Coding Theory." Lecture Notes in Mathematics. New York: Springer-Verlag, 1971.