Error Correcting, Error Detecting and Error Locating Codes

R. C. BOSE*,
The University of North Carolina at Chapel Hill

1. INTRODUCTION

Consider a channel which is capable of transmitting any one of q distinct symbols. Such a channel is called a q-ary channel. The special case $q = 2$ is of particular importance. In this case the channel is called binary. Similarly if $q = 3$, we have a ternary channel. The symbols successively presented to the channel for transmission constitute the 'input' and the symbols received constitute the 'output'. Due to the presence of noise a transmitted symbol may be received as one of the other $q-1$ symbols. When this happens we say that there is an error in transmitting the symbol.

In this paper we shall confine ourselves to the case when q is a prime or a prime power, say $q = p^h$ where p is a prime, and $h \geqslant 1$ is any integer. The symbols can then be put in a (1,1)

*This research was supported by the National Science Foundation Grant No. GP-3792 and the Air Force Office of Scientific Research Grant No. AF-AFOSR-760-65.

correspondence with the elements of the Galois field $GF(q)$. For the binary case the field $GF(2)$ contains only two symbols 0 and 1. Consider a set C of $v < q^n$ distinct n-vectors with elements belonging to $GF(q)$. Given a set of v distinct messages we can set up a (1,1) correspondence between the messages and the n-vectors belonging to C. The elements of C may be called code vectors or code words. Thus each message corresponds to a unique code vector (word). To transmit a message over the channel the n elements of the code vector corresponding to the message are presented in succession to the channel. The output is than an n-vector (not necessarily a vector of C) which belongs to the vector space V_n of all n-vectors with elements belonging to $GF(q)$. A decoder is obtained by setting up a decision rule, which specifies a unique vector of C, corresponding to any vector of V_n such that if this vector of V_n is received as an output, it is read as the corresponding vector of C. The code is called a group code if the set C of code words forms a group under vector addition. If C is a vector space (a subspace of V_n), then the code is said to be a *linear code*. Of course a linear code is always a group code. By a code C, we shall mean a code, for which the set of code words is C. The number n is called the length of the code[2].

2. THE HAMMING DISTANCE

Let $\mathbf{x}' = (x_1, x_2, \ldots, x_n)$ be any vector of V_n, the vector space of all vectors with elements belonging to $GF(q)$. Then the number of non-zero elements in $\mathbf{x}'$ is defined as the weight $w(\mathbf{x}')$ of $\mathbf{x}'$. Given two vectors

$$\mathbf{x}' = (x_1, x_2, \ldots, x_n),\ \mathbf{y}' = (y_1, y_2, \ldots, y_n),$$

both belonging to V_n, the Hamming [9] distance $d(\mathbf{x}', \mathbf{y}')$ between $\mathbf{x}'$ and $\mathbf{y}'$ is defined as the number of coordinates in which $\mathbf{x}'$ and $\mathbf{y}'$ disagree. Clearly

$$d(\mathbf{x}', \mathbf{y}') = w(\mathbf{x}' - \mathbf{y}') = w(\mathbf{y}' - \mathbf{x}').$$

[2] Here each code word is considered to be of the same length n. When this is not the case one has variable length codes.

It is readily seen that the Hamming distance satisfies the condition of a metric, i.e.,

(i) $d(\boldsymbol{x}', \boldsymbol{y}') = 0$, if and only if $\boldsymbol{x}' = \boldsymbol{y}'$

(ii) $d(\boldsymbol{x}', \boldsymbol{y}') = d(\boldsymbol{y}', \boldsymbol{x}')$

(iii) $d(\boldsymbol{x}', \boldsymbol{y}')+d(\boldsymbol{y}', \boldsymbol{z}') \geqslant d(\boldsymbol{x}', \boldsymbol{z}')$.

Let $\boldsymbol{g}_1$ and $\boldsymbol{g}_2$ be any words of a group code. Then $\boldsymbol{g}_1-\boldsymbol{g}_2$ is also a code word. Hence the distance between two code words is the weight of some code word. Also $\boldsymbol{0}$ is a code word. If $\boldsymbol{g}$ is an arbitrary code word then $w(\boldsymbol{g}) = d(\boldsymbol{g}, \boldsymbol{0})$. Hence

Theorem 2.1. *If d is the minimum distance between the words of a group code, then d is also the minimum weight of the code words.*

3. THE GENERATING MATRIX AND THE PARITY CHECK MATRIX OF A LINEAR CODE

Consider a linear code C. Then the set of code words is a vector space V_k of rank k. Any set of basis vectors of V_k, may be regarded as the set of row vectors of a $k \times n$ matrix

$$G = \begin{bmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{bmatrix}. \tag{3.1}$$

Every other code vector is a linear combination of the rows of $\boldsymbol{G}$. The matrix $\boldsymbol{G}$ is called the generating matrix of the code. Let $\boldsymbol{c}' = (c_1, c_2, \ldots, c_k)$ be any k-vector with elements from $GF(q)$, then $\boldsymbol{c}'\boldsymbol{G}$ is a code word. Since each of $c_1, c_2, \ldots, c_k$ can be taken in q ways, the total number of code words is q^k. Such a code is called a linear code.

Let V_r be the null space of V_k. Then

$$\text{Rank } V_r = n-k = r \text{ (say)}. \tag{3.2}$$

The number r is defined to be the redundancy of the linear code and k is called the number of information places. Let the row vectors of

$$(3.3)\qquad \boldsymbol{H} = \begin{bmatrix} h_{11} & h_{12} & \dots & h_{1n} \\ h_{21} & h_{22} & \dots & h_{2n} \\ \dots & \dots & \dots & \dots \\ h_{r1} & h_{r2} & \dots & h_{rn} \end{bmatrix}$$

from a basis of V_r. Then $\boldsymbol{H}$ is defined to be the parity check matrix of the linear code. If $\boldsymbol{H}'$ denotes the transpose of $\boldsymbol{H}$, then

$$(3.4)\qquad \boldsymbol{GH}' = \boldsymbol{0},$$

where $\boldsymbol{0}$ is the $k \times r$ null matrix.

The code words can be regarded as the set of independent solutions of the homogeneous linear equations

$$(3.5)\qquad \begin{aligned} h_{11}g_1 + h_{12}g_2 + \dots + h_{1n}g_n &= 0 \\ h_{21}g_1 + h_{22}g_2 + \dots + h_{2n}g_n &= 0 \\ \dots \quad \dots \quad \dots \quad \dots &= \dots \\ h_{r1}g_1 + h_{r2}g_2 + \dots + h_{rn}g_n &= 0 \end{aligned}$$

for the variables $g_1, g_2, \dots, g_n$. The equations (3.5) are called parity check equations. The rows of $\boldsymbol{G}$ are a set of independent solutions of the parity check equations.

Theorem 3.1. *$\boldsymbol{g}'$ is a code word if and only if $\boldsymbol{g}'\boldsymbol{H} = \boldsymbol{0}$ i.e., $\boldsymbol{Hg} = 0$.*

Theorem 3.2. *Let $\boldsymbol{g}'$ be a word of weight w, belonging to the linear code C, with parity check matrix $\boldsymbol{H}$. Let the i_1th, i_2th, ..., i_wth coordinates of $\boldsymbol{g}'$ be non-zero (all other coordinates being zero). Then there is a linear dependence relation, with non-zero coefficients among the i_1th, i_2th, ..., i_wth column vectors of $\boldsymbol{H}$ and conversely.*

Let $\boldsymbol{H} = (\boldsymbol{h}_1, \boldsymbol{h}_2, \dots, \boldsymbol{h}_n)$, and $\boldsymbol{g}' = (g_1, g_2, \dots, g_n)$. Then

$$\boldsymbol{Hg} = g_1\boldsymbol{h}_1 + g_2\boldsymbol{h}_2 + \dots + g_n\boldsymbol{h}_n = \boldsymbol{0}$$

Now $g_{i_1}, g_{i_2}, \ldots, g_{i_w}$ are non-zero, and the other g's are zero. Hence

$$g_{i_1}\boldsymbol{h}_{i_1}+g_{i_2}\boldsymbol{h}_{i_2}+\ldots+g_{i_w}\boldsymbol{h}_{i_w} = \mathbf{0}, \tag{3.6}$$

which proves the first part of the theorem. Conversely if (3.6) holds with non-zero coefficients, then from Theorem 3.1 there exists a code word whose i_1th, i_2th, …, i_wth coordinates are $g_{i_1}, g_{i_2}, \ldots, g_{i_w}$ and the other coordinates are all zero.

Corollary. *Let C be a linear code with parity check matrix $\boldsymbol{H}$: (i) If no m of the columns of $\boldsymbol{H}$ are dependent then each word of C has weight $\geqslant m+1$. (ii) Conversely if each word of C has weight $\geqslant m+1$, then any m columns of $\boldsymbol{H}$ must be independent.*

(i). Suppose there is a word of C, with weight $m-\alpha$, $\alpha \geqslant 0$. Then there is at least one set of $m-\alpha$ columns of $\boldsymbol{H}$ which are dependent. A set of m columns of $\boldsymbol{H}$ containing these is also dependent. This is a contradiction.

(ii). If a set of m columns of $\boldsymbol{H}$ is dependent, then there is a linear relation among these m columns in which there are $m-\alpha$, $\alpha \geqslant 0$, non-null coefficients. Hence there is a word of weight $m-\alpha$, $\alpha \geqslant 0$. This is a contradiction.

4. EQUIVALENT CODES

If $\boldsymbol{G}$ is the generating matrix of a linear code C, and $\boldsymbol{G}^*$ is obtained from $\boldsymbol{G}$ by column permutations, then $\boldsymbol{G}^*$ generates a linear code C^* defined to be equivalent to C.

The generator matrix $\boldsymbol{G}$ of a linear code C is not unique. If $\boldsymbol{G}_0$ can be obtained from $\boldsymbol{G}$ by elementary row operations (i.e., row multiplication and row addition) then $\boldsymbol{G}_0$ also generates C. If $\boldsymbol{G}^*$ is obtained from $\boldsymbol{G}_0$ by column interchanges, then $\boldsymbol{G}^*$ generates an equivalent code C^*. There is a (1,1) correspondence between the words of C and C^* such that corresponding words have the same weight.

It is readily proved that given an (n, k) linear code C, we can find an equivalent code C^*, for which the generating matrix is

$$G^* = [I_k, P], \tag{4.1}$$

where I_k is the $k \times k$ unit matrix, and P is a $k \times r$ matrix.

Every word of C^* is of the form $c'G^*$ where $c' = (c_1, c_2, \ldots, c_k)$. But $c'G^* = (c_1, c_2, \ldots, c_k; c_1p_{11}+c_2p_{21}+\ldots+c_kp_{k1}, \ldots, c_1p_{1r}+c_2p_{2r}+\ldots+c_kp_{kr})$.

Hence the first k coordinates of any word of C^* can be arbitrarily chosen, then the $(k+1)$th, ..., nth coordinates are certain linear combinations of these. A code of this type is called a systematic code. The first k coordinates of each word are called information symbols and the last r coordinates the check symbols. We thus have

Theorem 4.1. *Every linear code is equivalent to a systematic code.*

Let G^* be given by (4.1). Now

$$[I_k, P]\begin{bmatrix} -P \\ I_r \end{bmatrix} = -P+P = 0. \tag{4.2}$$

Hence if we put

$$H^* = [-P', I_r], \tag{4.3}$$

then the vector space generated by H^* is the null space of the vector space generated by G^*. Hence H^* given by (4.3) is the parity check matrix of the systematic code generated by G^* given by (4.1), and conversely.

5. SYNDROMES AND COSETS

Consider an (n, k) linear code C, with generator matrix G and parity check matrix H. Given any n-vector v', whether belonging to C or not, the syndrome of v' is defined to be the row vector

$$s' = v'H'.$$

From Theorem (3.1), v' belongs to C if and only if its syndrome is zero. Note that the syndrome of any n-vector is an r-vector.

Since the set of code words C, forms a subgroup of the group of all n-vectors, we can form the cosets of C in the usual manner.

Let

$$\mu = q^k - 1, \quad \nu = q^r - 1.$$

We form a table in which the elements of C are written in the first row, the null element being in the initial place.

TABLE I

C	$e'_0 = g'_0 = 0$	g'_1	g'_2	$\ldots$	g'_μ
C_1	e'_1	$g'_1+e'_1$	$g'_2+e'_1$	$\ldots$	$g'_\mu+e'_1$
C_2	e'_2	$g'_1+e'_2$	$g'_2+e'_2$	$\ldots$	$g'_\mu+e'_2$
	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
C	e'_ν	$g'_1+e'_\nu$	$g'_2+e'_\nu$	$\ldots$	$g'_\mu+e'_\nu$

Let e'_1 be any n-vector not belonging to C. Then the coset C_1 is obtained by adding e'_1 to the elements of C. The element $g'_i+e'_1$ of C_1 is written in the row corresponding to C_1, below g'_i. Now if e'_2 is any n-vector not belonging to C or C_1 we form the coset C_2 in an analogous manner. Proceeding in this manner we get $\nu+1 = q^r$ cosets counting C itself as one coset. Each n-vector with elements from $GF(q)$ belongs to one and only one coset.

The elements in the first column of Table I are called coset leaders. In forming the coset C_i instead of e'_i we might use and other element of C_i say $e'_i+g'_j$ as the coset leader. This will not change the coset C_i. Only the elements of C_i will now appear in a different order,

$$e'_i+g'_j,\ e'_i+g'_1+g'_j,\ \ldots,\ e'_i+g'_\mu+g'_j.$$

It is clear that two n-vectors belong to the same coset if and only if their difference belongs to C.

Theorem 5.1. *Two n-vectors belong to the same coset if and only if their syndromes are equal.*

Let v'_1 and v'_2 be two n-vectors with the same syndrome. Then $v'_1H' = v'_2H'$. Hence $(v'_1-v'_2)H' = 0$. Therefore $v'_1-v'_2$ belongs to C, which shows that v'_1 and v'_2 belong to the same coset.

Conversely if v_1' and v_2' belong to the same coset then $v_1'-v_2' = g'$ where g' belongs to C. Hence

$$(v_1'-v_2')H' = g'H' = 0.$$

Therefore $v_1'H' = v_2'H'$, i.e. v_1' and v_2' have the same syndrome.

6. USE OF SYNDROMES FOR ERROR DETECTION AND ERROR CORRECTION

If the code word g' is transmitted and the received vector is v', then the error vector is defined to be

$$e' = v'-g', \tag{6.1}$$

i.e. Received vector v' = Transmitted vector g'+Error vector e'.

If there is no transmission error $v' = g'$, and the error vector e' is null. If however w of the coordinates of g' have been wrongly transmitted, then v' and g' disagree in w coordinates. Hence the weight of e' is w. We say that w errors have occurred in transmitting g'.

Theorem 6.1. *If the minimum weight of the words of a linear code C is $2t+d+1$, $(t \geqslant 0,\ d \geqslant 0)$, then any t or a lesser number of errors can be corrected, and if the number of errors lies between $t+1$ and $t+d$, they can be detected.*

We shall first show that if e_1' and e_2' are any two n-vectors such that $w(e_1')+w(e') \leqslant 2t+d$, then the syndromes of e_1' and e_2' are different. If possible let the syndromes be equal. Then $e_1'H' = e_2'H'$ or $(e_1'-e_2')H' = 0$. Hence $e_1'-e_2'$ is a code word. Hence

$$2t+d+1 \leqslant w(e_1'-e_2') \leqslant w(e_1')+w(-e_2') = w(e_1')+w(e_2') \leqslant 2t+d$$

which is a contradiction.

Let Ω_1 be the set of all n-vectors of weight t or less. Also let Ω_2 be the set of all n-vectors whose weight is not less than $t+1$, and does not exceed $t+d$. Then the syndromes of any two vectors belonging to Ω_1 are different from each other. Let S_1 be the set of these syndromes. Then there is a (1,1) correspondence between the vectors of Ω_1 and S_1, such that a vector of

S_1, is the syndrome of the corresponding vector of Ω_1. Note that the null vector is contained in Ω_1, and corresponds to the null vector in S_1.

Again the syndrome of any vector belonging to Ω_1 is different from the syndrome of any vector belonging to Ω_2. In particular the syndrome of any vector belonging to Ω_2 is non-null.

We now set up the following decision rule for decoding: Let $\boldsymbol{v}'$ be the received vector. If the syndrome of $\boldsymbol{v}'$ belongs to S_1, we conclude that the error vector is the corresponding vector of Ω_1. The transmitted vector is then obtained by subtracting this error vector from the received vector. If the syndrome of $\boldsymbol{v}'$ does not belong to S_1 we conclude that the received vector is different from the transmitted word. Thus an error is detected but we do not attempt to correct it.

We have now to show that this decision rule will correct up to t errors and detect up to $t+d$ errors in the transmission of any word. Suppose the transmitted word is $\boldsymbol{g}'$ and the error-vector is $\boldsymbol{e}'$. Then from (6.1),

$$\begin{aligned}\text{Syndrome } \boldsymbol{e}' &= \boldsymbol{e}'\boldsymbol{H}' \\ &= (\boldsymbol{v}'-\boldsymbol{g}')\boldsymbol{H}' \\ &= \boldsymbol{v}'\boldsymbol{H}' \\ &= \text{Syndrome } \boldsymbol{v}'.\end{aligned}$$

If t or a lesser number of errors have occurred $w(\boldsymbol{e}') \leqslant t$. Hence the syndrome of $\boldsymbol{v}'$ belongs to S_1. There is only one member of Ω_1, viz., $\boldsymbol{e}'$ which has the same syndrome as $\boldsymbol{v}'$. Hence our decision rule will correctly pick up the error vector, and then the transmitted word is correctly determined as $\boldsymbol{v}'-\boldsymbol{e}' = \boldsymbol{g}'$.

If between $t+1$ and $t+d$ errors have occurred, then $t+1 \leqslant w(\boldsymbol{e}') \leqslant t+d$. In this case the syndrome of $\boldsymbol{v}'$ will be non-null without belonging to S_1. Hence our decision rule will correctly indicate that errors have occurred in transmitting, but we will not be able to correct them.

If more than $t+d$ errors have occurred, then the syndrome of $\boldsymbol{v}'$ could belong to S_1. If this happens our decision rule would lead to a wrong conclusion.

Corollary. *If the minimum weight of the words of a linear code C is $2t+1$ any t or a lesser number of errors can be corrected. If the minimum weight is $d+1$, errors up to d in number can be detected.*

7. ONE ERROR DETECTING LINEAR CODES

Taking $t = 0$, $d = 1$ in Theorem 6.1, we see that for a one error detecting linear code the minimum weight of each code must be two. Let us take for $\boldsymbol{H}$, the parity check matrix, a single row vector, with non-zero elements from $GF(q)$. Then no column of $\boldsymbol{H}$ is dependent. From the corollary to Theorem 3.2, each word of the corresponding code has weight at least 2. Hence the code must be one error detecting. Thus if

$$\boldsymbol{H} = (h_1, h_2, \ldots, h_n), \quad h_i \neq 0 \text{ for } i = 1, 2, \ldots, n$$

then $\boldsymbol{g}' = (g_1, g_2, \ldots, g_n)$ is a code word if and only if

$$g_1h_1+g_2h_2+\ldots+g_nh_n = 0.$$

We can therefore construct a one error detecting $(n, n-1)$ code for any n. If $\boldsymbol{v}'$ is the received vector, we decide that there has been a transmission error if its syndrome

$$v_1h_1+v_2h_2+\ldots+v_nh_n,$$

is non-null, and that there has been no error if the syndrome is null. In case the error vector is non-null and belongs to the code C, the syndrome of the received word will be zero, and we shall wrongly decide that it has been correctly transmitted. In other cases error will be detected.

8. THE FUNCTION $n_m(r, q)$ AND THE PACKING PROBLEM

Let $m = 2t+d$, $t \geqslant 0$, $d \geqslant 0$. We have shown in Theorem 6.1 that if the minimum weight of the words of C is $m+1$, then we can correct any t or less errors, and detect up to $t+d$ errors.

From the corollary to Theorem 3.2 it follows that one way of obtaining C is to find an $r \times n$ matrix $\boldsymbol{H}$, which has the property (P_m), that no m columns of $\boldsymbol{H}$ are dependent. Then C would be the code with parity check mtrix $\boldsymbol{H}$. One might ask the following question :

For a given r, what is the maximum value of n, for which there exists an $r \times n$ matrix $\boldsymbol{H}$, with elements from $GF(q)$, possessing the property (P_m), that no m columns of $\boldsymbol{H}$ are dependent ? We shall denote this maximum value by $n_m(r, q)$.

The case $m = 1$ is trivial, since any non-null r-vector can be taken as a column of $\boldsymbol{H}$, and repeated as many times as we choose. Hence n does not have a finite maximum. In what follows we shall suppose $m \geqslant 2$.

If $m \geqslant 2$, and $\boldsymbol{H}$ is an $r \times n$ matrix with the property (P_m), then no two columns of $\boldsymbol{H}$ are dependent. The elements of a column vector $\boldsymbol{H}$ may be regarded as the coordinates of a point of the finite projective space $PG(r-1, q)$, distinct columns representing distinct points. Hence alternatively $n_m(r, q)$ is the maximum number of points we can choose in $PG(r-1, q)$ so that no m are dependent. The problem of finding such a set of points in $PG(r-1, q)$ may be called the packing problem.

Lemma 8.1. $n_m(r, q) \geqslant r+1$.

This is obvious since we can choose for columns of $\boldsymbol{H}$, the r unit vectors, and the vector all of whose columns are unity.

Lemma 8.2. *For a given prime power q and a given $m \geqslant 2$, $n_m(r, q)$ is a monotonically increasing function of r such that*

$$n_m(r+1, q) \geqslant 1+n_m(r, q) \tag{8.1}$$

There exists an $r \times n_m(r, q)$ matrix $\boldsymbol{H}$, no m columns of which are dependent. Add an $(r+1)$th null row to $\boldsymbol{H}$, and finally a last column for which the first r elements are zero and the $(r+1)$th element is 1. This extended matrix still has the property (P_m), which proves our result.

Theorem 8.1. *If $\boldsymbol{H}$ is an $r \times n_m(r, q)$ matrix, with elements from $GF(q)$, having the property (P_m), then rank $\boldsymbol{H} = r$.*

Rank $\boldsymbol{H} \leqslant \min[r, n_m(r, q)]$. Hence from Lemma 8.1 rank $\boldsymbol{H} \leqslant r$. Suppose then rank $\boldsymbol{H} = r_1 < r$. Then we can choose r_1 independent rows of $\boldsymbol{H}$, such that the remaining $r-r_1$ rows are dependent on these. The submatrix $\boldsymbol{H}_1$ of $\boldsymbol{H}$, consisting of these r_1 rows has the property (P_m), that no m columns are dependent. Hence $n_m(r_1, q)$ is not less than $n_m(r, q)$. However from Lemma 8.2, $n_m(r, q) \geqslant (r-r_1)+n_m(r_1, q)$. We thus have a contradiction. If follows that rank $\boldsymbol{H} = r$.

The following bounds for $n_m(r, q)$ are known [1], [8], [9], [12], [13]. If $n = n_m(r, q)$ then

$$\text{(i)}\quad 1+\binom{n}{1}(q-1)+\binom{n}{2}(q-1)^2+\ldots+\binom{n}{m-1}(q-1)^{m-1} \geqslant q^r,$$

(Gilbert, Varshamov)

$$\text{(ii) (a)}\quad q^r \geqslant 1+\binom{n}{1}(q-1)+\binom{n}{2}(q-1)^2+\ldots$$

$$+\binom{n}{t}(q-1)^t \text{ if } m = 2t, \qquad \text{(Rao, Hamming)}$$

$$\text{(b)}\quad q^r \geqslant 1+\binom{n}{1}(q-1)+\binom{n}{2}(q-1)^2+\ldots$$

$$+\binom{n}{t}(q-1)^t+\binom{n-1}{t}(q-1)^{t+1} \text{ if } m = 2t+1. \quad \text{(Rao)}$$

Theorem 8.2. *The maximum value of n, for which there exists an $(n, n-r)$ linear code with given redundancy r and such that each word has weight at least $m+1$, is $n_m(r, q)$.*

We can find an $r \times n_m(r, q)$ matrix $\boldsymbol{H}$, with elements belonging to $GF(q)$, such that no m columns are dependent. From Theorem 8.1 its rank is r. Let C be the linear code with has $\boldsymbol{H}$ for its parity check matrix, then C is an (n, k) code where $k = n-r$.

From the corollary to Theorem 3.2, each word of C has weight at least $m+1$.

Suppose there exists a linear code (n_1, n_1-r), $n_1 < n_m(r, q)$ with redundancy r, such that each word has weight at least $m+1$. Then its parity check matrix H_1 is an $r \times n_1$ matrix, with the property that no m columns of H_1 are dependent. Hence $n_m(r, q) \geqslant n_1$, which is a contradiction.

Theorem 8.3. *For any $c < k$, the existence of an (n, k) linear code, for which each word has weight at least $m+1$, implies the existence of an $(n-c, k-c)$ linear code for which each word has weight at least $m+1$.*

Let C be an (n, k) linear code for which each word has weight at least $m+1$. We can find an equivalent code C^*, for which the generator matrix G^* is in the cannonical form

$$G^* = [I_k, P],$$

where P is an $(n-k) \times k$ matrix. Let G_1^* be the matrix obtained from G^* by dropping the last c rows. Then each word of the code generated by G_1^*, belongs to C^*, and must therefore have weight at least $m+1$. Note that the $(k-c+1)$th, $(k-c+2)$th, ..., kth columns of G_1^* are null. Let G_2^* be the $(k-c)\times(n-c)$ matrix obtained from G_1^* dropping these columns. Then G_1^* generates an $(n-c, k-c)$ linear code, each word of which has weight at least $m+1$.

Corollary. *There exists an $[n_m(r, q)-c, n_m(r, q)-r-c]$ linear code, for which each word has weight at least $m+1$, for any c, $0 \leqslant c < n_m(r, q)-r$.*

This corollary follows at once from Theorems 8.2 and 8.3.

9. THE FUNCTION $k_m(n, q)$

Let $k_m(n, q)$ denote the maximum number of information places for a linear code of given length n, with symbols from $GF(q)$, and for which each world has weight at least $m+1$.

Theorem 9.1. *If* $n_m(r, q) \geqslant n > n_m(r-1, q)$, *then*

$$k_m(n, q) = n-r.$$

From the corollary to Theorem 8.3, there exists a linear code

$$[n_m(r, q)-c,\ n_m(r, q)-r-c],$$

for which each word has weight at least $m+1$. Taking $c = n_m(r, q)-n$, we get the existence of an $(n, n-r)$ linear code for which each word has weight at least $m+1$. Hence

$$k_m(n, q) \geqslant n-r.$$

If possible suppose

$$k_m(n, q) = n-r+\theta, \qquad \theta \geqslant 1.$$

Then there exists a linear code $(n, n-r+\theta)$, with redundancy $r^* = r-\theta$, for which each word has length at least $m+1$. Hence from Theorem 8.2

$$n_m(r-\theta, q) \geqslant n.$$

From Lemma 8.2,

$$n_m(r-1, q) \geqslant n.$$

This contradicts the hypothesis.

Corollary 1. *For a fixed* m, $k_m(n, q)$ *is a montonically increasing function of* n, *but it may stay the same for two consecutive values of* n.

Corollary 2. *If* $n_m(r, q) \geqslant n \geqslant n\ (r-1, q)$, *then the minimum redundancy for a code of given length* n, *and for which each word has weight at least* $m+1$, *is* r.

10. ONE ERROR CORRECTING (OR TWO ERROR DETECTING) HAMMING CODES

In Theorem 6.1 put $2t+d+1 = 3$, then either $t = 1, d = 0$ or $t = 0, d = 2$. We thus see that if each word of a linear code C has weight at least 3, then we can either use it to correct a single error or we can use it to detect up to two errors (without attempting any correction). The parity check matrix $\boldsymbol{H}$ of such a code must have the property (P_2), viz. no two columns are dependent. If $\boldsymbol{H}$ is an $r \times n$ matrix, then the columns of $\boldsymbol{H}$ may be regarded as points of $PG(r-1, q)$. The columns corresponding to any two district points are independent. Thus the maximum value of n for given r and q, viz. $n_2(r, q)$, is given by

$$(10.1) \qquad n_2(r, q) = \frac{q^r-1}{q-1},$$

which is the number of distinct points in $PG(r-1, q)$. Thus if we take an $r \times n_2(r, q)$ matrix $\boldsymbol{H}$, whose columns represent all the distinct points of $PG(r-1, q)$ and form the code for which H is the parity check matrix, then we obtain a one error correcting (or two error detecting) $\left(\frac{q^r-1}{q-1}, k\right)$ linear code, where $k = \frac{q^r-1}{q-1} - r$. Since

$$(10.2) \qquad n_2(r-1, q) = \frac{q^{r-1}-1}{q-1}.$$

we have :

Theorem 10.1. *For any given n, we can obtain a one error correcting (or two error detecting) q-ary code, with redundancy r given by*

$$(10.3) \qquad \frac{q^r-1}{q-1} \geqslant n > \frac{q^{r-1}-1}{q-1}$$

This is the minimum redundancy possible.

The proof follows from Corollary 2 to Theorem 9.1.

Example. Let $q = 3$, $n = 10$. Then

$$\frac{3^3-1}{3-1} \geqslant 10 > \frac{3^2-1}{3-1}.$$

Hence the minimum redundancy is 3, and we can get a (10,7) ternary code by taking for the columns of the parity check matrix

$\boldsymbol{H}$, the coordinates of any 10 district points of $PG(2,3)$. Thus we may take

$$\boldsymbol{H} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 2 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 2 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 2 & 1 & 0 & 1 \end{bmatrix}$$

To use the code for single error correction, we form the syndrome of the received vector $\boldsymbol{v}'$. If the error vector is $\boldsymbol{e}'$ we have shown that

$$\boldsymbol{v}'\boldsymbol{H}' = \boldsymbol{e}'\boldsymbol{H}'.$$

If $e' = (0,0, \ldots, e_i, 0, \ldots, 0)$. Then $\boldsymbol{v}'\boldsymbol{H}' = e_i\boldsymbol{h}_i'$, where $\boldsymbol{h}_i'$ is the ith row of $\boldsymbol{H}'$. Hence the decoding rule is : Form the syndrome of the received vector. If it is $e_i\boldsymbol{h}_i'$, conclude that the error $(0,0, \ldots e_i, 0, \ldots 0)$ has occurred.

In the example under consideration suppose

$$\boldsymbol{g}' = (1, 2, 2, 0, 1, 1, 2, 0, 1, 2),$$

was transmitted (it is readily verified that this is a code word) and suppose

$$\boldsymbol{v}' = (1, 2, 2, 0, 1, 1, , 2, 1, 2),$$

was received. Now

$$\boldsymbol{v}'\boldsymbol{H}' = (1, 0, 2) = 2\boldsymbol{h}_8'$$

where $\boldsymbol{h}_8'$ is the 8th row of $\boldsymbol{H}'$. Hence we conclude that

$$\boldsymbol{e}' = (0, 0, 0, 0, 0, 0, 0, 2, 0, 0).$$

Then $\boldsymbol{g}' = \boldsymbol{v}' - \boldsymbol{e}'$ is correctly reconstructed.

11. ONE ERROR CORRECTING AND TWO ERROR DETECTING HAMMING CODES

In Theorem 6.1 put $2t+d+1 = 4$, then either $t = 1$, $d = 1$ or $t = 0$, $d = 3$. This shows that if each word of a linear code C, has weight at least 4, then we can use it for correcting one error, and detecting two errors (or alternatively for detecting up to 3 errors without attempting any correction). The parity check matrix of such a code must have the property (P_3), that no three columns are dependent. As has been shown before the problem of finding for any given n, a code with the desired property, and minimum redundancy depends on the solution of the following packing problem: To find in $PG(r-1, q)$, the maximum number of points, so that no three are collinear. A complete answer to this problem is known when $q = 2$, and r is arbitrary, or when $r \leqslant 3$, and q is an arbitrary prime power.

(a) First let us consider the case $q = 2$. Consider the finite projective space $PG(r-1,2)$. The coordinates of any point on a hyperplane Σ i.e. a linear subspace of dimension $r-2$, satisfy a linear equation

$$a_1x_1+a_2x_2+\ldots+a_rx_r = 0 \qquad (11.1)$$

where the a_i's are fixed constants (not all zero) belonging to $GF(2)$. Let S be the set of all points not lying on Σ. Any two distinct points of S, lie on a unique line, which meets Σ in a point. Since each line has exactly three points, it follows that no two points of S are collinear. The number of points in Σ is $2^{r-1}-1$, and the whole space has 2^r-1 points. Hence S contains exactly 2^{r-1} points.

Again from the Rao-Hamming bound on $n_m(r, q)$ given in Section 8, $n_3(r, 2) \leqslant 2^{r-1}$. Hence

$$n_3(r, 2) = 2^{r-1} \qquad (11.2)$$

For simplicity the equation of the hyperplane Σ may be taken to be

$$x_1+x_2+\ldots+x_n = 0. \qquad (11.3)$$

Then S consists of all points with an odd number of non-zero coordinates. Let $\boldsymbol{H}$ be the $r\times 2^{r-1}$ matrix whose columns represent the points of S. Then the $(2^{r-1}, 2^{r-1}-r)$ binary linear code which has $\boldsymbol{H}$ for its parity check matrix, has the property that each word has weight at least 4, and can be used for correcting one error and detecting two errors. These codes were first obtained by Hammng [9]. We can now state :

Theorem 11.1. *For any given n, we can obtain a one error correcting and two error detecting binary code, with redundancy r given by*

$$2^{r-1}-1 \geqslant n > 2^{r-2}-1. \tag{11.4}$$

This is the minimum redundancy possible.

(b) For odd $q > 2$, $r = 3$ it is known that [1],

$$n_3(3, q) = q+1. \tag{11.5}$$

If we take the set of $q+1$ points lying on a non-degenerate conic in the plane $PG(2, q)$, then no three will be collinear. In particular the equation of the conic may be taken as

$$x_1x_3 = x_2^2 \tag{11.6}$$

If the columns of a $3\times(q+1)$ matrix $\boldsymbol{H}$, represent the coordinates of the points lying on (11.6), then for the $(q+1, q-2)$ q-ary linear code which has $\boldsymbol{H}$ for its parity check matrix, each word will have weight at least four.

(c) Again when $q > 2$, $r = 4$, it is known [1], [11] that

$$n_3(4, q) = q^2+1.$$

If we take the set of q^2+1 points lying on a non-degenerate unruled quadric in $PG(3, q)$, then no three are collinear. The equation of the quadric may be taken as

$$a_{11}x_1^2+a_{12}x_1x_2+a_{22}x_2^2 = x_3x_4,$$

where $a_{11}t^2+a_{12}t+a_{22}$ is irreducible over $GF(q)$.

We can now use these points to construct a (q^2+1, q^2-3) q-ary linear code, for which each word has weight 4, and which may therefore be used for correcting one error and detecting two errors.

12. SOME TERNARY LINEAR CODES

Let $q = 3$. It can be proved by geometrical considerations [2], [3] that the set of 12 points of $PG(5, 3)$, whose coordinates are given by the columns of

$$(12.1) \qquad \boldsymbol{H} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 2 & 2 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 2 & 2 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 2 & 0 & 1 & 2 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 2 & 2 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 2 & 1 & 2 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

has the property that no 5 are dependent. From the Rao-Hamming bound given in Section 8, $n_5(6, 3) \leqslant 12$. Hence $n_5(6, 3) = 12$. From Section 4, the generating matrix of a ternary linear code C, with $\boldsymbol{H}$ for its parity check matrix can be written as

$$(12.2) \qquad \boldsymbol{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & 2 & 2 \\ 0 & 1 & 0 & 0 & 0 & 0 & 2 & 0 & 2 & 2 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 2 & 2 & 0 & 1 & 1 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 2 & 2 & 1 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 2 & 1 & 1 & 2 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 2 & 1 & 2 & 1 & 2 & 1 \end{bmatrix},$$

Since $\boldsymbol{H}$ has property (P_5), the minimum weight of the words of the linear code C, generated by $\boldsymbol{G}$ is 6. As a matter of fact it can be verified by actual computation, that all the words have weight 6, 9 or 12. Putting $2t+d+1 = 6$ in Theorem 6.1, we have the following solutions (*i*) $t = 2$, $d = 1$, (*ii*) $t = 1$, $d = 3$, (*iii*) $t = 0$, $d = 5$. Hence the (12, 6) linear code C, can be used either as a 2 error correcting and 3 error detecting code, or as a one error correcting and 4 error detecting code, or as a five error detecting code.

Let H_1 be the matrix obtained from H by dropping the last row and the last column. Thus

$$(12.3) \qquad H_1 = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 2 & 2 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 2 & 2 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 2 & 0 & 1 & 2 & 0 & 0 & 0 & 1 & 0 \\ 1 & 2 & 2 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

It is readily seen that no four columns of H_1 are dependent. In fact if any four columns of H_1 are dependent, then the corresponding 4 columns of H and the last column would be dependent contradicting the property (P_5) of H. Also from the bound given in Section 8, $n_4(5, 3) \leqslant 11$. Hence $n_4(5, 3) = 11$. If we construct the (11, 6) ternary linear code C_1 with H_1 as the parity check matrix, then each word of C_1 has weight at least 5. Hence C_1 can be used as a two error detecting code, or as a one error correcting, three error detecting code or as a four error detecting code.

Let the points corresponding to all 11 columns of H_1 be denoted by $P_0, P_1, P_2, \ldots, P_{10}$. In $PG(4,3)$, each line has 4 points. Hence the line P_0P_i has two other points say Q_i and Q_i^*. We shall show that the 20 points

$$(12.4) \qquad P_1, P_2, \ldots, P_{10}, \quad Q_1, Q_2, \ldots, Q_{10}$$

have the property that no three are collinear. Three of the points P, say P_i, P_j, P_k cannot be collinear, as in this case P_0, P_i, P_j, P_k would be coplanar. Again $P_iP_jQ_k$ cannot be collinear, since P lies in the plane determined by P_0 and the line $P_iP_jQ_k$. This would make P_0, P_i, P_j, P_k coplanar. Other cases can be similarly disposed of. This shows that $n_3(5,3) \geqslant 20$.

On the other hand it is known [6], that $n_3(5,3) \leqslant 26$. The exact value of $n_3(5,3)$ is not known. If we take for the coordinates of Q_i the sum of the columns corresponding to P_0 and P_i, then the matrix H whose column represent the 20 points (12.6) can be written as

$$(12.4) \quad \boldsymbol{H}_2 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 2 & 2 & 0 & 1 & 0 & 0 & 0 & 1 & 2 & 2 & 0 & 0 & 1 & 2 & 1 & 1 & 1 \\ 1 & 0 & 2 & 2 & 1 & 0 & 0 & 1 & 0 & 0 & 2 & 1 & 0 & 0 & 2 & 1 & 1 & 2 & 1 & 1 \\ 1 & 2 & 0 & 1 & 2 & 0 & 0 & 0 & 1 & 0 & 2 & 0 & 1 & 2 & 0 & 1 & 1 & 1 & 2 & 1 \\ 2 & 2 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 2 & 1 & 2 & 1 & 1 & 1 & 1 & 2 \end{bmatrix}$$

The (20, 15) ternary linear code C_2, with parity check matrix $\boldsymbol{H}_2$ has the property that each word has weight at least 4. It can be used either as a one error detecting and two error correcting code, or as a three error correcting code.

13. THE BOSE-CHAUDHURI HOCQUENGHEM CODES [4], [5], [10]

Let V_s be the vector space of all s-vectors with elements from $GF(q)$. We can institute a correspondence between the vector*

$$\alpha = (a_0, a_1, \dots, a_{s-1}),$$

of V_s, and the element

$$a_0 + a_1 x + a_2 x^2 + \dots + a_{s-1} x^{s-1},$$

of the $GF(q^s)$, where x is a primitive element of $GF(q^s)$. This is a (1,1) correspondence in which the null vector α_0 of V_s corresponds to the null element of $GF(q^s)$. The sum of any two vectors of V_s corresponds to the sum of the corresponding elements of $GF(q^s)$. We can therefore identify a vector α of V_s, with the corresponding element of $GF(q^s)$. This in effect defines a multiplication of the vectors of V_s and converts it into a field. Thus if

$$\alpha = (a_0, a_1, \dots, a_s), \quad \beta = (b_0, b_1, \dots, b_s),$$

are any two elements of V_s, then we can identify α and β with the element $a_0 + a_1 x + \dots + a_{s-1} x^{s-1}$, $b_0 + b_1 + \dots + b_s x^{s-1}$ of $GF(q^s)$.

Now x satisfies a certain minimum equation $\phi(x) = 0$ where $\phi(x)$ is a polynomial of the sth degree with coefficients from $GF(q)$. We can form the product of the elements α and β of $GF(q^s)$. Thus let

$$\alpha\beta = \gamma = c_0+c_1x+\ldots+c_{s-1}x^{s-1}.$$

Then the product of the vectors α and β is $\gamma = (c_0, c_1, \ldots, c_{s-1})$.

Each element of $GF(q^s)$ can then be regarded as an s-vector with elements from $GF(q)$.

Let α be a non-zero element of $GF(q^s)$, and let $c > 0$, and $2 \leqslant m \leqslant q-2$, be integers.

Consider the matrix

$$\boldsymbol{H}' = \begin{bmatrix} 1 & 1 & 1 & \ldots & 1 \\ \alpha^c & \alpha^{c+1} & \alpha^{c+2} & \ldots & \alpha^{c+m-1} \\ (\alpha^c)^2 & (\alpha^{c+1})^2 & (\alpha^{c+2})^2 & \ldots & (\alpha^{c+m-1})^2 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ (\alpha^c)^{n-1} & (\alpha^{c+1})^{n-1} & (\alpha^{c+2})^{n-1} & \ldots & (\alpha^{c+m-1})^{n-1} \end{bmatrix},$$

where we shall suppose that $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ are all distinct. Then $\boldsymbol{H}'$ can either be regarded as an $n \times m$ matrix with elements from $GF(q^s)$ or as $n \times ms$ matrix with elements from $GF(q)$. In this later case the element 1 of $GF(q^s)$ is to be regarded as the vector $(1, 0, 0, \ldots, 0)$ of V_s. When we form the transpose of $\boldsymbol{H}'$ i.e.,

$$\boldsymbol{H} = \begin{bmatrix} 1 & \alpha^c & (\alpha^c)^2 & \ldots & (\alpha^c)^{m-1} \\ 1 & \alpha^{c+1} & (\alpha^{c+1})^2 & \ldots & (\alpha^{c+1})^{n-1} \\ 1 & \alpha^{c+2} & (\alpha^{c+2})^2 & \ldots & (\alpha^{c+2})^{n-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & \alpha^{c+m-1} & (\alpha^{c+m-1})^2 & \ldots & (\alpha^{c+m-1})^{n-1} \end{bmatrix},$$

then $\boldsymbol{H}$ is an $m \times n$ matrix with elements from $GF(q^s)$ or an $ms \times n$ matrix with elements from $GF(q)$. Now elements of $GF(q^s)$ must be regarded as column s-vectors with elements from $GF(q)$.

We shall show that $\boldsymbol{H}$ when regarded in the first way has the property (P_m) that no m columns of $\boldsymbol{H}$ are dependent over $GF(q^s)$, and hence over $GF(q)$. From this it would follow that when $\boldsymbol{H}$ is regarded as a matrix with elements from $GF(q)$, then no m columns would be dependent over $GF(q)$.

Let $\boldsymbol{M}$ be the matrix formed by taking any distinct m columns of $\boldsymbol{H}$. Then

$$\boldsymbol{M} = \begin{bmatrix} (\alpha^c)^{j_1} & (\alpha^c)^{j_2} & \cdots & (\alpha^c)^{j_m} \\ (\alpha^{c+1})^{j_1} & (\alpha^{c+1})^{j_2} & \cdots & (\alpha^{c+1})^{j_m} \\ \cdots & \cdots & \cdots & \cdots \\ (\alpha^{c+m-1})^{j_1} & (\alpha^{c+m-1})^{j_2} & \cdots & (\alpha^{c+m-1})^{j_m} \end{bmatrix}$$

where $0 \leqslant j_1 < j_2 < \cdots < j_m \leqslant n-1$.

$$\det \boldsymbol{M} = \alpha^{c(j_1+j_2+\cdots+j_m)} \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \alpha^{j_1} & \alpha^{j_2} & \cdots & \alpha^{j_m} \\ \cdots & \cdots & \cdots & \cdots \\ (\alpha^{j_1})^{m-1} & (\alpha^{j_2})^{m-1} & \cdots & (\alpha^{j_m})^{m-1} \end{vmatrix}$$

$$= \alpha^{c(j_1+j_2+\cdots+j_m)} \qquad \Pi\,(\alpha^{j_u}-\alpha^{j_v}),$$

where $1 \leqslant u \leqslant v \leqslant m$. But by hypothesis $1, \alpha, \ldots, \alpha^{n-1}$ are all distinct. Hence $\det \boldsymbol{M} \neq 0$. This shows that the columns of $\boldsymbol{M}$ are independent and proves the required result.

Now let $\boldsymbol{H}$ be regarded as an $ms \times n$ matrix over $GF(q)$ which has the property (P_m) that no m columns are dependent. Its rank is $r \leqslant ms$. If we now construct the $(n, n-r)$ q-ary linear code C with parity check matrix $\boldsymbol{H}$, then each word will have weight at least $m+1$.

It can happen that many rows of $\boldsymbol{H}$ (or columns of $\boldsymbol{H}'$) are dependent on others and so can be dropped without changing the code C. This will now be illustrated by considering certain examples and special cases.

(a) Let $q = 2$, $s = 6$. We then extend $GF(2)$ to $GF(2^6)$. Let α be a primitive element of $GF(2^6)$. Let us take $c = 1$, $m = 6$, and $n = 63$. We note that $1, \alpha, \alpha^2, \ldots, \alpha^{62}$ are all distinct since α is a primitive root. Then

$$\boldsymbol{H}' = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ \alpha^2 & (\alpha^2)^2 & (\alpha^3)^2 & (\alpha^4)^2 & (\alpha^5)^2 & (\alpha^6)^2 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \alpha^{61} & (\alpha^2)^{61} & (\alpha^3)^{61} & (\alpha^4)^{61} & (\alpha^5)^{61} & (\alpha^6)^2 \\ \alpha^{62} & (\alpha^2)^{62} & (\alpha^3)^{62} & (\alpha^4)^{62} & (\alpha^5)^{62} & (\alpha^6)^{62} \end{bmatrix}$$

Now $x \to x^2$ is an automorphism of the field $GF(2^6)$. We also note that if c is an element of $GF(2)$, then $c^2 = c$. Hence to any linear relation with coefficients from $GF(2)$, between the elements of column 1 of $\boldsymbol{H}'$, there corresponds the same relation between the elements of the columns 2 and 4 of $\boldsymbol{H}'$. Hence if we drop the columns 2 and 4 of $\boldsymbol{H}'$, then the code C for which $\boldsymbol{H}$ is the parity check matrix will not change. Also the rank of $\boldsymbol{H}$ will not change. In the same way we see that we can drop the column 6. The matrix $\boldsymbol{H}'$ has now been reduced to the form,

$$\boldsymbol{H}_1' = \begin{bmatrix} 1 & 1 & 1 \\ \alpha & \alpha^3 & \alpha^5 \\ \alpha^2 & (\alpha^2)^3 & (\alpha^2)^5 \\ \cdots & \cdots & \cdots \\ \alpha^{61} & (\alpha^{61})^3 & (\alpha^{61})^5 \\ \alpha^{62} & (\alpha^{62})^3 & (\alpha^{62})^5 \end{bmatrix}$$

Regarded as a matrix over $GF(2)$ it is of order (63×18). Since $m = 6$, the (63,45) binary linear code with $\boldsymbol{H}_1$ as parity check matrix has words of weight at least 7 and can be used as a 3 error correcting code.

(b) Now let $q = 2$ and let $s \geqslant 2$ be any positive integer. Let $GF(q)$ be extended to $GF(q^s)$. Let $m = 2t$, $c = 1$, and let α be a primitive element of $GF(q^s)$. Then reasoning as before it is easy to see that if we obtain $\boldsymbol{H}_1'$ from $\boldsymbol{H}'$ by dropping the 2nd, 4th, ..., $(2t)$th columns of $\boldsymbol{H}'$, then the rank of $\boldsymbol{H}_1'$ will be the same as that of $\boldsymbol{H}'$. Hence this rank (when $\boldsymbol{H}_1'$ is regarded as a matrix over $GF(q)$), will be $R \leqslant st$. Hence by following the method explained we shall obtain a $(2^s-1,\ 2^s-1-R)$, t error correcting binary code where $R \leqslant st$.

The estimate st is only an upper bound for the rank of $\boldsymbol{H}'$. The actual rank may be less than this. This is illustrated by the example which follows.

(c) Let $q = 2$, $s = 6$ as in (a). Let $c = 1$, $m = 10$, and as before let α be a primitive element of $GF(q^6)$. We can as explained before drop the even numbered columns of $\boldsymbol{H}'$ and obtain

$$\boldsymbol{H}_1' = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ \alpha & \alpha^3 & \alpha^5 & \alpha^7 & \alpha^9 \\ \alpha^2 & (\alpha^3)^2 & (\alpha^5)^2 & (\alpha^7)^2 & (\alpha^9)^2 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \alpha^{62} & (\alpha^3)^{62} & (\alpha^5)^{62} & (\alpha^7)^{62} & (\alpha^9)^{62} \end{bmatrix},$$

such that

$$\text{Rank } \boldsymbol{H}' = \text{Rank } \boldsymbol{H}_1' \leqslant 30.$$

Now $(\alpha^9)^7 = \alpha^{63} = 1$. Thus α^9 and its powers constitute a subfield of order 2^3 of $GF(2)$ and α^9 satisfies a third degree equation with coefficients from $GF(2)$. Hence the elements of the last column of $\boldsymbol{H}_1'$ (when regarded as a matrix over $GF(q^s)$)

can be expressed as a linear combination of 1, α^9, α^{18} with coefficients from $GF(2)$. When H_1' is regarded as a matrix over $GF(2)$ then only three of the six columns corresponding to

$$\begin{bmatrix} 1 \\ \alpha^9 \\ (\alpha^9)^2 \\ \cdots \\ (\alpha^9)^{62} \end{bmatrix},$$

are independent. Hence rank $H_1' = 27$. Thus the code for which H_1 is the parity check matrix is a (63,36), 5 error correcting binary code.

(d) We can now see how the rank of H' can be obtained in the general case. Consider the factors of $X^{q^s-1}-1$, irreducible over $GF(q)$. Thus let

$$X^{q^s-1}-1 = \phi_1(X)\phi_2(X)\ldots\phi_u(X),$$

where $\phi_i(X)$ is a polynomial in X, with coefficients from $GF(q)$ and irreducible over $GF(q)$. If β is an element of $GF(q^s)$, then β is a root of one and only one polynomial out of $\phi_1(X)$, $\phi_2(X)$, ..., $\phi_u(X)$. On the other hand if β_i is a root of $\phi_i(X)$, then the other roots are β_i^q, $\beta_i^{q^2}$, ... Thus if v is the smallest integer such that $\beta_i^{q^v} = \beta_i$, then the degree of $\phi_i(x)$ is v, and β_i must belong to a subfield of order q^v of $GF(q^s)$. We will say that the index of β_i is v.

Now if among the elements of the set

(13.1) $$\alpha^c, \alpha^{c+1}, \alpha^{c+2}, \ldots, \alpha^{c+m-1},$$

more than one are the roots of the same polynomial $\phi_i(X)$, then we can immediately drop from H' columns corresponding to all but one. For example in (a), $\alpha, \alpha^2, \alpha^4$ are the roots of the same irreducible factor of $X^{2^6}-1$ and we therefore can drop the

the columns corresponding to α^2 and α^4. Let α^u be an element of the set (13.1) the column corresponding to which has been retained. When $\boldsymbol{H}_1'$ is now considered over $GF(q)$, this column will become a matrix with s columns. However if v_u is the index of α^u, then out of these s columns only v_u will be independent. This gives us the following rule for the rank of $\boldsymbol{H}'$.

Consider the set of distinct factors of $X^{p^{s-1}}-1$, irreducible over $GF(q)$, whose roots occur one or more times in (13.1). Then the rank of $\boldsymbol{H}'$ is the sum of the degrees of these factors, the degree of each factor counting only once, even if it has more than one root in the set (13.1).

We shall conclude this section with a few more examples :

(3) Let $q = 2$, $s = 6$, $c = 1$, $m = 4$. Let α be the cube of a primitive element of $GF(2^6)$. We can take $n = 21$ since, $1, \alpha, \alpha^2, \ldots, \alpha^{20}$ are all different but $\alpha^{21} = 1$. The set $\alpha^c, \ldots, \alpha^{c+m-1}$ is now

$$\alpha, \alpha^2, \alpha^3. \alpha^4. \tag{13.2}$$

Now $\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \alpha^{32} = \alpha^{11}$ are the roots of $\phi_1(X)$ a polynomial of the sixth degree ($\alpha^{64} = \alpha^{22} = 1$). Thus $\phi_1(X)$ has roots among (13.2). Again $\alpha^3, \alpha^6, \alpha^{12}$ are the roots of $\phi_2(X)$ a third degree polynomial ($\alpha^{24} = \alpha^3$). Hence the rank of $\boldsymbol{H}'$ is 9, the sum of the degrees of $\phi_1(X)$ and $\phi_2(X)$, and the general method described will lead to a 2 error correcting (21,12) binary code.

(f) Let $q = 3$, $s = 3$. Let $GF(3)$ be extended to $GF(3^3)$. Let $c = 12$, $m = 3$. Let α be a primitive element of $GF(3^3)$ and let $n = 26$. Now consider the set

$$\alpha^{12}, \alpha^{13}, \alpha^{14}.$$

$\alpha^{12}, \alpha^{10}, \alpha^4$ are the roots of a third degree polynomial $\phi_1(X)$, $\alpha^{14}, \alpha^{16}, \alpha^{22}$ are the roots of another third degree polynomial $\phi_2(X)$ and α^{13} is the root of a linear polynomial X-2. Hence we can obtain a (26,19) ternary code correcting one error and detecting two errors,

14. ERROR LOCATING CODES

Elspas and Wolf [14], [15] have recently introduced a new class of codes called error locating codes, with properties intermediate between error detecting codes and error correcting codes. Consider the case of a q-ary channel; where q is a prime power. In an error locating $(n, n-r)$ q-ary code each word is supposed to be divided into N subwords each of length n_0. Thus $n = nN_0$. If errors belonging to a certain class of patterns E_d occur within sub-words, and if the sub-words within which the errors occur belong to a certain class of patterns E_t, then we can detect the presence of transmission errors, and can locate the erroneous sub-words, but cannot actually pin point the errors. For example E_d may be the class of patterns consisting of d or a lesser number of errors in a sub-words, and E_t may be the class of patterns consisting of t or a lesser number of erroneous sub-words. Then it is required to find an $(n, n-r)$ linear q-ary code, such that if errors occur in not more than t sub-words, and consist of not more than d wrongly transmitted symbols in any sub-word, then it should be possible to detect the presence of transmission errors, and locate the erroneous sub-words. We shall now prove the following theorem due to Wolf.

Thereom 14.1. *Let C_0 be a q-ary (n_0, n_0-r_0) linear code which detects the class of error-patterns E_d. Let $Q = q^{r_0}$. Let C^* be a $(N, N-R)$, Q-ary linear code for which the transmission symbols are elements of $GF(Q)$ and which is capable of correcting errors belonging to a class of patterns E_t. Then we can construct an $(n, n-r)$ linear q-ary code, with $n = n_0N$, and $r = r_0R$, such that if errors belonging to E_d occur within a pattern of sub-words belonging to E_t, then the errors can be detected and erroneous sub-words located.*

Let H_0 be the parity check matrix of C_0, where H_0 is of order $r_0 \times n_0$. For example if $q = 2$, $n_0 = 7$, $r_0 = 3$, and E_d is the class of patterns consisting of two or fewer errors in any word of length 7, then we may take H_0 as

$$(14.1) \qquad H_0 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}$$

The columns of H_0 can be regarded as elements of $GF(q^{r_0})$ or $GF(Q)$. Thus in the example if α is a primitive element of $GF(2^3)$, satisfying the equation $\alpha^3+\alpha^2+1 = 0$, we can write

$$(14.3) \qquad H_0 = [1 \; \alpha \; \alpha^2 \; \alpha^3 \; \alpha^4 \; \alpha^5 \; \alpha^6]$$

In the general case H_0 is a row-vector of length n_0 with elements from $GF(Q)$.

Let H^* be the parity check matrix of C^*, the order of H^* being $R\times N$ (when regarded as a matrix over $GF(Q)$. Let γ_{ij} be element in the ith row and jth column of H^*. Let be the Kronecker product of H^* and H_0 (regarded as a row vector over $GF(Q)$). Thus

$$(14.3) \qquad H = H^*\otimes H_0 = \begin{bmatrix} \gamma_{11}H & \gamma_{12}H & \cdots & \gamma_{1N}H \\ \gamma_{21}H & \gamma_{22}H & \cdots & \gamma_{2N}H \\ \cdots & \cdots & \cdots & \cdots \\ \gamma_{R1}H & \gamma_{R2}H & \cdots & \gamma_{RN}H \end{bmatrix}$$

When H is regarded as a matrix over $GF(Q)$, it is of order $R\times n_0N$. However each element of H can be regarded as a column vector of length r_0, with elements from $GF(q)$. Thus when H is regarded as a matrix over $GF(q)$ it is of order $r_0R\times n_0N$ or $r\times n$. Let C be the code (with symbols from $GF(q)$, which has H (regarded in the second way) for its parity check matrix. Then C is the required $(n, n-r)$ error locating q-ary linear code.

Let us now consider the error-correcting capabilities of C. First consider the situation where errors occur only in the jth sub-word, the errors belonging to the class E_d. Then the error vector can be divided into N sub-blocks. All the sub-blocks are null except the jth which is say $(e_1, e_2, \ldots, e_{n_0})$, this vector belonging to E_d. Let

$$H_0 = (h_1, h_2, \ldots, h_{n_0}).$$

Then the resulting syndrome will contain the components

$$S_i = (e_1 h_1 + e_2 h_2 + \ldots + e_{n_0} h_{n_0})\gamma_{ij} = a_{ij}\gamma_{ij},$$

where a_{ij} is a non-zero element of $GF(Q)$. If errors occur within several sub-words say $j_1, j_2, \ldots, j_v$ and if the errors within each sub-word are contained in E_d, whereas the pattern of sub-words in which the errors occur belongs to E_t, the resulting syndrome will contain components

$$S_i = a_{j_1}\gamma_{ij_1} + a_{j_2}\gamma_{ij_2} + \ldots + a_{j_v}\gamma_{ij_v}.$$

Note that $a_{j_1}, a_{j_2}, \ldots, a_{j_v}$ are non-zero elements of $GF(Q)$ and do not depend on i. Now if in the code C^* the error vector has as its j_1th j_2th, ..., j_vth coordinates the elements $a_{j_1}, a_{j_2}, \ldots, a_{j_v}$, and the other coordinates are zero, then the resulting syndrome will have exactly the components S_i. Since C^* corrects all patterns belonging to E_t, it is clear that the syndromes resulting from all permissible errors in the error locating code C, are all different. This proves our theorem.

To continue our example let C^* be the (63,55) two error correcting Bose-Chaudhuri octic code ($Q = 2^3$). Let θ be a primitive element of $GF(2^6)$. We can take θ as a root of the equation $\theta^6+\theta+1 = 0$ [7, page 262]. Then the elements of the subfield $GF(2^3)$ of $GF(2^6)$ are θ^{9i} ($i = 0,1,2,3,4,5,6$). Let $\theta^9 = \alpha$, then $\alpha^3+\alpha^2+1 = 0$ and α is a primitive root of $GF(2^3)$. Using the relation $\theta^2 = \alpha^3\theta+\alpha$, we can express each element of $GF(2^3)$ in the form $\beta\theta+\delta$ where β and δ belong to $GF(2^3)$ so that elements of $GF(2^6)$ can be regarded as 2-vectors over $GF(2^3)$. Now we can take for the parity check matrix of C^* the matrix

$$(14.4) \quad H^* = \begin{bmatrix} 1 & \theta & \theta^2 & \theta^3 & \cdots & \theta^{62} \\ 1 & \theta^2 & (\theta^2)^2 & (\theta^2)^3 & \cdots & (\theta^2)^{62} \\ 1 & \theta^3 & (\theta^3)^2 & (\theta^3)^3 & \cdots & (\theta^3)^{62} \\ 1 & \theta^4 & (\theta^4)^2 & (\theta^4)^2 & \cdots & (\theta^4)^{62} \end{bmatrix},$$

where $\boldsymbol{H}^*$ is of order 8×63, when regarded as a matrix over $GF(2^3)$, Hence using the method explained we first form the Kronecker product $\boldsymbol{H} = \boldsymbol{H}^* \otimes \boldsymbol{H}_0$. This is of order 24×441 over $GF(2)$, and then construct the code C which has $\boldsymbol{H}$ as a parity check matrix. We thus obtain a (441,417) binary linear code in which each word is to be divided into 63 sub-words of length 7. If then there are not more than two errors in not more than two sub-words, then we can detect them and locate the erroneous sub-words.

References

[1] Bose, R. C. (1947). "Mathematical Theory of Symmetrical Factorial Designs," *Sankhyā*, **8**, 107–166.

[2] Bose, R. C. (1961). "On Some Connections Between the Design of Experiments and Information Theory," *Bull. Inter. Stat. Inst.*, **38**, pt. 4, 257–271.

[3] Bose, R. C. (1961). "Some Ternary Error Correcting Codes and Fractionally Replicated Designs," *Colloque Inter. du C.M.R.S. le Plan d'Experiences*, No 110, 21–32. Editions du C.M.R.S.

[4] Bose, R. C. and Ray-Chaudhuri, D. K. (1960). "On a Class of Error Correcting Binary Group Codes," *Information and control*, **3**, 68–79.

[5] Bose, R. C. and Ray-Chauhuri, D. K. (1960). "Further Results on Error Correcting Group Codes," *Information and control*, **3**, 279–290.

[6] Bose, R. C. and Srivastava, J. N. (1964). "On a Bound Useful in the Theory of Factorial Designs and Error Correcting Codes," *Ann. Math. Statist.*, **35**, 780–794.

[7] Carmichael, R. D. (1956). *Introduction to the Theory of Groups of Finite Order*, Dover, New York.

[8] Gilbert, E. N. (1952). "A Comparison of Signalling Alphabets," *Bell System Tech. J.*, **31**, 504–522.

[9] Hamming, R. W. (1950). "Error Detecting and Error Correcting Codes," *Bell System Tech. J.*, **29**, 147–160.

[10] Hocquengham, A. (1959). "Codes Correctuers d'Erreurs," *Chiffres*, **2**, 147–156.

[11] Qvist, B. (1952). "Some Remarks Concerning Curves of the Second Degree in a Finite Plane," *Ann. Acad. Sci. Fenn. Ser. A.I.*, **134**.

[12] Rao, C. R. (1947). "Factorial Experiments Derivable from Combinatorial Arrangements of Arrays," *Supp. J. Roy. Stat. Soc.*, **9**, 128–139.

[13] Varshamov, R. R. (1957). "Estimate of the Number of Signals in Error Correcting Codes," *Dokaldy A.N.S.S.R.*, **117**, no. 5, 739–741.

[14] Wolf, J. K. (1965). "On an Extended Class of Error Locating Codes. *Information and control*, **8**, 163–169.

[15] Wolf, J. K. and Elspas, B. (1963). "Error Locating Codes—A New Concept in Error Control," *IEEE Trans. Inform. Theory* ***IT*-9**, 20–28.

(Received Jan. 1, 1966.)