BOUNDS ON ERROR CORRECTING CODES (NON-RANDOM)

by

I. M. CHAKRAVARTI
University of North Carolina
Chapel Hill, N. C.

Institute of Statistics Mimeo Series No. 451

October 1965

This is a collection of results on bounds on different parameters of error correcting codes (non-random). The relationship between different criteria of optimality for codes is discussed. The well-known bounds due to Plotkin, Hamming and Rao, Varsharmov and Gilbert and Johnson are described. The asymptotic expressions of these bounds are also given.

This research was supported by the U. S. Army Research Office Contract No. DA-31-124-ARO-D-254.

DEPARTMENT OF STATISTICS
UNIVERSITY OF NORTH CAROLINA
Chapel Hill, N. C.

BOUNDS ON ERROR CORRECTING CODES (NON-RANDOM)*

by

I. M. CHAKRAVARTI

University of North Carolina

1. Introduction. Let us recall a few definitions and results. A block code is a code that uses sequences of n channel symbols or n-vectors or n-tuples. A q-nary channel transmits sequences formed from a set of q distinct symbols. The set of all q-nary n-vectors has q^n elements. Only a selected subset of n-vectors is transmitted. The subset is called a code and its elements - the n-vectors are called the code-words or code points. The Hamming distance $\delta(u,v)$ between two code-words u and v is the number of positions in which they differ. The Hamming weight $w(v)$ of a code-word v is the number of non-zero components in it. A code has minimum distance d if the distance between any two of its code-words is at least d. If $d = 2t+1$, a code with minimum distance d can correct at least t errors made during transmission through the channel.

If the q symbols are taken as the q elements of a field GF(q), then the q^n n-vectors form a vector space V_n. In this case, q is necessarily a prime number or a power of a prime number. If the n-vectors of a code form a subspace of the n-dimension vector space, then it is called a linear code

---

*Presented at the NATO Summer School on Coding and Information Theory, Royan, France, August 26 - September 8, 1965.

or a group code. The minimum distance for a linear code is equal to the minimum weight of its non-zero vectors.

A matrix G whose row-vectors form a basis of a linear code V is called a generator matrix for V. If V has dimension k, G is a k x n matrix with rank k and V has, then, q^k code words. Such a code is called an (n,k) linear code.

Consider the set V* of q-nary n-vectors which are orthogonal to every one of the vectors in V. Then V* is a subspace and thus defines a linear code. Let H define a generator matrix for V*. Then H is of the form (n-k) x n and it has rank n-k. H is called a parity-check matrix for V. Similarly, G is a parity check matrix for V*. It also follows that,

$$GH^T = 0 \quad . \tag{1.1}$$

For an (n,k) linear code V, n is the word length , k is the number of information places and n-k = r is called the redundancy or number of check digits.

Any generator matrix G can be put in the combinatorially equivalent form

$$G = [I_k \vdots G_1] \quad , \tag{1.2}$$

by elementary row operations and permutation of columns. Two combinatorially equivalent matrices generate the same code.

Given a generator matrix $G = [I_k \vdots G_1]$, the corresponding parity check matrix H is given by

$$H = \left[-G_1^T \vdots I_r \right] \quad , \tag{1.3}$$

where $r = n - k$.

Here we quote a theorem [4] without proof, connecting the weight of a code-word and the linear dependence relation between columns of the parity check matrix H.

Theorem 1.1. Let V be a linear code with parity check matrix H. Then for each code word of weight w there is a linear dependence relation between w columns of H.

Corollary: A linear code with parity check matrix H has minimum weight (and hence minimum distance) at least d, if and only if every subset of $d-1$ columns of H is linearly independent. Such a matrix is said to possess the P_{d-1} property.

2. Criteria of Optimality. A linear code that for some t has all patterns of weight t or less and no others as coset leaders is called a perfect code [17]. A code which for some t has all patterns of weight t or less and none of weight greater than $(t+1)$ as coset leaders is called quasi-perfect.

Consider a binary symmetric channel. Suppose there exists an (n,k) binary linear code which is quasi-perfect. Let q be the probability that the received symbol is the same as the transmitted one and $p = 1-q$ is the probability that the received symbol is other than the transmitted one. Then the probability of correct decoding is given by

$$\text{(2.1)} \qquad \text{Prob (correct decoding)} = \sum_{i=0}^{n} f_i \, p^i \, q^{n-i} \ ,$$

where f_i is the frequency of coset leaders of weight i and

$$\sum_{i=0}^{n} f_i = 2^{n-k}$$

If $p < q$, $p^i \, q^{n-i}$ decreases with increasing i and hence the probability of correct decoding is increased whenever one f_i is increased and

another f_{i+j} $(j > 0)$ is decreased. For a quasi-perfect code, f_i for $i = 0,1,2, \ldots, t$, is equal to the number of n-vectors of weight i and is thus as large as possible. The terms f_{t+2} and beyond are all zero and f_{t+1} accounts for the remaining cosets. Then the probability of correct decoding P is given by

$$P = \sum_{i=0}^{t} \binom{n}{i} p^i q^{n-i} + f_{t+1} p^{t+1} q^{n-t-1} , \tag{2.2}$$

where $f_{t+1} = 2^{n-k} - 1 - \binom{n}{1} - \ldots - \binom{n}{t} > 0$.

It is easy to see that P is as large as possible. In the case, where quasi-perfect codes do not exist, P provides an upper bound on the probability of correct decodings for any (n,k) linear group code.

The codes that have one information symbol repeated (2t+1) times correct all combinations of t or fewer errors and no patterns of more than t errors. These trivial codes, the Golay (23,12) code [12] and the Hamming codes [14] are the only known perfect binary codes. Certain codes found by omitting columns from Hamming codes and Bose-Chaudhuri double-error-correcting codes are quasi-perfect [13]. Quasi-perfect codes have been called optimal codes [17], since they maximize the probability of correct decoding.

Other criteria of optimality of non-random codes are discussed in [9]. A brief account is given here.

For a given value of q, a linear code involves three parameters, n, k and d. For fixed n and k, a linear code which maximizes d is called a maximum-minimum distance (or max-mini for short) code. For fixed n and d, a linear code which maximizes k, is a maximum size code. For fixed k and d, a linear code which minimizes n is called a minimum redundancy code. These definitions of optimality are related but not equivalent.

Let V_r denote the vector space of all r-vectors whose elements belong to GF(q). Let $n_d(r,q)$ denote the maximum number of r-vectors chosen from V_r, such that any d distinct vectors are independent. This number $n_d(r,q)$ is also the maximum number of points that can be chosen in the finite projective space PG(r-1,q), such that no d of the points lie on a flat space of dimension d-2 or less. Existence of a set of $n = n_{d-1}(r,q)$ q-nary r-vectors such that no d-1 of them are linearly dependent, implies the existence of a parity-check matrix H of the form r x n, whose columns are these r-vectors. H in its turn determines an (n,k) linear code having minimum distance d .

Given d and q, $n_d(r,q)$ is a monotonically increasing function of r .

Let $k_d(n,q)$ denote the maximum k for a linear code, given n, d and q. This implies the existence of a subspace of rank $k = k_d(n,q)$ in the vector-space V_n of all q-nary n-vectors.

The following theorem [6] establishes a relationship between $n_{d-1}(r,q)$, $n_{d-1}(r-1,q)$ and $k_d(n,q)$.

Theorem 2.1. If $n_{d-1}(r,q) \geq n > n_{d-1}(r,q)$, then $k_d(n,q) = n-r$.

In the following discussion, these two well-known results (see for instance [4]) are used.

$$n_2(r,q) = (q^r-1)/(q-1) . \tag{2.3}$$

$$n_3(r,2) = 2^{r-1} . \tag{2.4}$$

Since $k_3(8,2) = 4 = k_4(8,2)$, we note that $k_d(n,q)$ is not a strictly increasing function of d for all values of n. So, although, a code with parameters n = 8, k = 4 and d = 3 is of maximum size, it is not of maximum-minimum distance.

Again, $k_3(7,2) = 4 = k_3(8,2)$ shows that $k_d(n,q)$ is not a strictly increasing function of n. Hence a code with parameters n = 8, k = 4 and d = 3 is of maximum size but not of minimum redundancy.

Let $d_k(n,q)$ be the d for a maximum-minimum distance code with given n, k and q. Since $d_k(n,q)$ is not a strictly increasing function of n, a max-mini distance code is not necessarily of minimum redundancy .

Again $d_3(7,2) = 4 = d_2(7,2)$ shows that $d_k(n,q)$ is not a strictly decreasing function of k. So a code with n = 7, k = 2, q = 2 and d = 4, is of max-mini distance, but not of maximum size.

Let $N_d(k,q)$ denote the smallest possible n for a code with given d, k and q. We show following [9] that $N_d(k,q)$ is a strictly increasing function of k. Let V be a minimum redundancy code for given d, q and k, that is, $n = N_d(k,q)$.

Let V_i be a subspace of V consisting of all vectors in V, whose i-th coordinate is zero. We may choose i so that the i-th coordinate is not always zero in V, and then V_i is an (n, k-1) code with minimum weight d. Omitting the i-th coordinate of every vector in V_i, one obtains an (n-1,k-1) code with minimum weight d. Hence

$$N_d(k-1,q) < n = N_d(k,q) .$$

Since $N_d(k,q)$ is a strictly increasing function of k, a minimum redundancy code must be of maximum size.

Let V be a minimum redundancy code for given d, q and k, that is $n = N_d(k,q)$. Then choosing i so that the i-th coordinate is not always zero in V, we omit the i-th coordinate. This gives us an (n-1,k) code with weight at least d-1. Hence

$$N_{d-1}(k,q) \leq n-1 < N_d(k,q) .$$

Thus $N_d(k,q)$ is a strictly increasing function of d and hence, a minimum redundancy code is of max-mini distance.

Finally, the following example shows that a code can be both of max-mini distance and maximum size without being of minimum redundancy. Consider the binary code V consisting of the four vectors,

$$\underline{\alpha}_0' = (0\ 0\ 0\ \ 0\ 0\ 0\ \ 0\ 0\ 0\ \ 0\ 0\ 0\ 0)$$

$$\underline{\alpha}_1' = (1\ 1\ 1\ \ 1\ 1\ 1\ \ 1\ 1\ 0\ \ 0\ 0\ 0\ 0)$$

$$\underline{\alpha}_2' = (0\ 0\ 0\ \ 0\ 1\ 1\ \ 1\ 1\ 1\ \ 1\ 1\ 1\ 0)$$

$$\underline{\alpha}_3' = (1\ 1\ 1\ \ 1\ 0\ 0\ \ 0\ 0\ 1\ \ 1\ 1\ 1\ 0)$$

Here $n = 13$, $k = 2$ and $d = 8$. Since the last coordinate of all the vectors is zero, it can be omitted without affecting k or d. Hence V is not of minimum redundancy. But since codes with parameters $n = 13$, $k = 2$, $d = 9$ or $n = 13$, $k = 3$, $d = 8$, do not exist, V is of max-mini distance and maximum size. These results can be stated in the form of a theorem [9].

Theorem 2.2. If a code is of minimum redundancy then it is of maximum size, and of max-mini distance. The other possible implications between these three properties are not universally valid.

Definitions of optimality in terms of the probability of error detection or correction do not seem to be very closely related to the three optimalities defined in terms of redundancy, size or minimum distance. For instance, a quasi-perfect code maximizes the probability of correct decoding for a given n and k but it does not necessarily have the max-mini distance for that n and k. Conversely, a max-mini distance or minimum redundancy code may not maximize the probability of correct decoding.

On the other hand, several classes of codes which have been constructed

with the maximum size as a criterion of optimality turned out to be quasi-perfect and hence optimal in the probability sense. The Hamming codes with $d = 3$, the unreduced $d = 4$ codes, Golay codes (23,12) and the Bose-Chaudhuri $d = 5$ codes are examples in point.

3. Bounds on Parameters of Codes.

3.1. Bounds on $n_d(r,q)$. We first quote a few results on bounds on $n_d(r,q)$ without proof. A full treatment is given in a paper [3] to be presented in one of the sessions of this school. The symbol $m_d(r,q)$ has also synonymously been used for $n_d(r,q)$ [5]. It has been shown [4] that,

(3.1) $$n_3(3,q) = q+1 \text{ when } q \text{ is odd.}$$

(3.2) $$n_3(3,q) = q+2 \text{ when } q \text{ is even,}$$

(3.3) $$n_3(r,2) = 2^{r-1} \text{ for } r > 3 ,$$

(3.4) $$n_3(4,q) = q^2+1 \quad \text{for } q \text{ odd.}$$

For q even ($q > 2$), it is shown [19] that,

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

For $r > 3$ and $q > 2$, it is known [21] that,

(3.6) $$n_3(r+1,q) < q^{r-1} + 1 .$$

In [20], it has been proved that

(3.7) $$n_3(5,q) \leq q^3 - q^2 + 8q - 14$$

for q odd and $q \geq 7$; also

(3.8) $$n_3(r+1,q) < q^{r+1} - q^{r-2} + 8q^{r-3} - 6 \sum_{i=0}^{r-4} q^i - 8$$

for $r > 4$, q odd $(q \geq 7)$.

Further some improvements on the inequalities are available in [2]. These are

(3.9) $$n_3(r+1,7) \leq 7^{n-1} - \sum_{i=1}^{r-3} 7^i \qquad \text{for } r > 4 ,$$

(3.10) $$n_3(5,5) \leq 124 \quad ,$$

(3.11) $$n_3(r+1,5) < 5^{r-1} - 10 \sum_{i=0}^{r-5} 5^i - 1 \quad \text{for} \quad r > 4 \quad .$$

It has been proved in [8], that for $q > 2$, $r \geq 4$, $n_3(r,q)$ cannot exceed the positive root of the equation

(3.12) $$x^2(q^2-q-1) - x\{(q^2-2q-1) + N_r(q-2)\} - 2N_r = 0 \ ,$$

where $N_r = (q^r - 1)/(q - 1)$. This provides the following improved inequalities.

(3.13) $$n_3(r+1,3) \leq (3^{r+1} + 23)/10 \quad \text{for } r \geq 4 \ ,$$

(3.14) $$n_3(5,q) \leq (q^3-1) \quad \text{for } q \text{ even and } q > 2 \ ,$$

(3.15) $$n_3(r+1,q) < \frac{q^2 - 2q-1 + \left(\sum_{i=0}^{r} q^i\right)(q-2)}{q^2 - q - 1} + 1$$

for q even ($q > 2$).

Finally, in [3] it has been shown that

(3.16) $$n_3(r+1,q) \leq q^{r-1} - 2\left(\sum_{i=1}^{r-4} q^i\right) - 1$$

for $r > 4$, $q > 2$ and q even.

3.2. Plotkin bound We first prove a lemma on the weight of code words.

Lemma 3.1. The sum of the weights of the code words of an (n,k) linear code with symbols taken from $GF(q)$ is $n\, q^{k-1}(q-1)$.

Proof: Let G be the generator matrix of an (n,k) linear code,

(3.17) $$G = \begin{bmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \cdot & \cdot & \cdots & \cdot \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{bmatrix} .$$

G has rank k and we can choose the columns of G so that none of them is a null vector. The q^k code words are the q^k linear combinations of the k row-vectors of G. Consider the linear equation

(3.18) $$x_1 g_{1i} + x_2 g_{2i} + \cdots + x_k g_{ki} = 0 .$$

There are q^{k-1} solutions $(x_1, x_2, \ldots, x_k)$ to this equation, x_i's being elements of GF(q). Hence if the q^k code words are written in the form of a $q^k \times n$ matrix, in each column there will be q^{k-1} zeros and $q^k - q^{k-1} = q^{k-1}(q-1)$ non-zero elements of GF(q). Hence the sum of the weights of the code words is equal to $n\, q^{k-1}(q-1)$.

This provides an upper bound on the minimum weight (equivalently, minimum distance) for a linear (n,k) code .

Theorem 3.1. The minimum weight d of a code word in an (n,k) linear code is at most $n\, q^{k-1}(q-1)/(q^k-1)$.

Proof: Since there are (q^k-1) code words with non-zero weight and since the minimum weight can be at most equal to the average weight, it follows that,

(3.19) $$d \leq n\, q^{k-1}(q-1)/(q^k-1) .$$

Consider an $(r \times n)$ parity check matrix H which determines an (n,k) linear code having minimum distance d and $k = n-r$. This implies that no $(d-1)$ columns of H are dependent. If any c columns of H are deleted the resulting matrix still retains the P_{d-1} property and hence determines an

$(n-c, k-c)$ $(c < k)$ linear code having minimum distance d. Hence we have the lemma,

Lemma 3.2. If there exists an (n,k) linear code with minimum distance d and if c is a positive integer less than k, then there exists an $(n-c,k-c)$ linear code with minimum distance d.

Let $B(n,d)$ be the maximum possible q^k in a linear code for a given n with minimum distance at least d. By lemma 3.2, the existence of a linear code with parameters n,k and d, where $q^k = B(n,d)$, implies the existence of a linear code with parameters $n-c$, $k-c$ and d, if $c < k$. Hence $B(n-c,d) \geq q^{k-c}$ and

$$q^k = B(n,d) \leq q^c B(n-c,d) \quad . \tag{3.20}$$

From (3.19), we get

$$q^{k-1}(qd + n - nq) \leq d \quad . \tag{3.21}$$

From (3.20) and (3.21) it follows that

$$q^k = B(n,d) \leq \frac{q^c\, qd}{qd - (q-1)(n-c)} \quad , \tag{3.22}$$

where $c < k$, provided $c > n - \frac{(qd)}{(q-1)}$.

Assuming that c is sufficiently large so that the denominator is positive, one should use that value of c which minimizes the right hand side. Considering the ratio

$$\frac{q^c q\, d}{qd-(q-1)(n-c)} \Big/ \frac{q^{c+1} q\, d}{qd-(q-1)(n-c-1)}$$

$$= \frac{1}{q} + \frac{(q-1)}{q\{qd - (q-1)(n-c)\}} \quad ,$$

it is seen that it is greater than 1, provided that

$$qd - (q-1)(n-c) < 1 \quad ,$$

and in this case c should be increased to $c+1$. Otherwise, one should not.

The inequality $qd - (q-1)(n-c) < 1$, can be written as $c < n - (qd-1)/(q-1)$. Hence to optimize, one takes for c the smallest integer greater than or equal to $n - \frac{(qd-1)}{(q-1)}$. This is the Plotkin bound. This implies that if $n > \frac{qd-1}{q-1}$,

$$q^k \leq q^{n - \frac{qd-1}{q-1}} \, qd \, . \tag{3.23}$$

Taking logarithms to the base q, one has

$$k \leq n - \frac{qd-1}{q-1} + 1 + \log_q d \, . \tag{3.24}$$

This can be stated as follows:

Theorem 3.2. If $n > \frac{(qd-1)}{(q-1)}$, the number of check symbols required to achieve a minimum weight d is at least

$$\frac{qd}{(q-1)} - \frac{1}{(q-1)} - 1 - \log_q d \, .$$

If d is very large, the last three terms in the expression are negligible.

The Plotkin bound holds also for non-linear codes [18].

3.3. The Varsharmov-Gilbert bound. We try to construct a parity check matrix H whose columns are q-nary r-vectors having the property P_{d-1}, that is every d-1 columns or fewer are linearly independent. Any non-null q-nary r-vector may be chosen as the first column of H. Then the second column of H may be any non-zero q-nary r-vector other than the multiples of the first. The third column may be any q-nary r-vector which is not a linear combination of the first two. In general, the i-th column is chosen as any q-nary r-vector that is not a linear combination of any d-2 or fewer preceding columns. This method of construction assures that no linear combination of d-1 or fewer columns will be the null vector. As long as the set of all linear combinations of d-2 or few columns does not include all q-nary r-vectors, another column

can be added. In the worst possible case, all these linear combinations might be distinct. There are q^r-1 non-zero q-nary r-vectors. Hence if,

$$(3.25) \qquad \binom{n-1}{1}(q-1) + \binom{n-1}{2}(q-1)^2 + \ldots + \binom{n-1}{d-2}(q-1)^{d-2} < q^r - 1 ,$$

there exists a linear code with n digits and at most r parity check digits (hence with at least $k = n-r$ information symbols) with minimum distance d. The code is the null space of the matrix H of the form $r \times n$. Hence the theorem ([22], [11]),

Theorem 3.3. It is possible to construct a code of length n and minimum distance d with r parity check symbols where r is the smallest integer satisfying (3.25).

Writing

$$(3.26) \qquad S = \sum_{i=0}^{d-2} \binom{n-1}{i}(q-1)^i ,$$

it is easy to show that,

$$(3.27) \qquad S < \binom{n-1}{n-d+1} (q-1)^{d-2} \frac{\lambda (q-1)}{\lambda(q-1)-\mu} ,$$

provided $\lambda(q-1) > \mu$, where $\lambda = 1 - \frac{d-2}{n-1}$ and $\mu = \frac{d-2}{n-1}$.

Using Stirling's approximation for the factorials, one can then show that the right hand side of (3.27) is asymptotically equal to

$$(3.28) \qquad -(n-1)\left\{ (1 - \tfrac{d-2}{n-1}) \log (1 - \tfrac{d-2}{n-1}) + \tfrac{d-2}{n-1} \log \tfrac{d-2}{n-1} \right\} + (d-2)\log(q-1) ,$$

as $d \to \infty$, $n \to \infty$ such that $0 < b_1 < \frac{d-2}{n} < b_2 < 1$, where b_1 and b_2 are two preassigned constants. Hence, asymptotically, if

$$(3.29) \qquad (1 - \tfrac{k}{n}) \geq (1 - \tfrac{1}{n}) H (\tfrac{n+1-d}{n-1}) + (\tfrac{d-2}{n}) \log(q-1) ,$$

or more simply if ,

(3.30) $$\left(1 - \frac{k}{n}\right) \geq H\left(\frac{n-d}{n}\right) + \frac{d}{n} \log(q-1) ,$$

then there exists a code of word length n with minimum distance at least d and with at least k information places for large n and d. For $q = 2$, (3.30) simplifies to

(3.31) $$1 - \frac{k}{n} \geq H\left(\frac{n-d}{n}\right) .$$

In the above expressions $H(x) = -x \log x - (1-x) \log (1-x)$.

3.4. The Hamming-Rao bound. Suppose there exists an (n,k) linear code with minimum weight d. There are two cases to be considered,

(i) $d = 2t + 1$ and (ii) $d = 2t+2$.

Case (i), $d = 2t + 1$; In this case one can correct with certainty all patterns of t or fewer errors. Hence all q-nary n-vectors of weight t or less must be coset leaders.

The number of q-nary n-vectors with weight t or less is given by

$$1 + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \ldots + \binom{n}{t}(q-1)^t .$$

This must be less than or equal to the number of cosets q^r where $r = n-k$. Hence,

(3.32) $$1 + \binom{n}{1}(q-1) + \ldots + \binom{n}{t}(q-1)^t \leq q^r .$$

Case (ii), $d = 2t + 2$: In this case, one can correct with certainty any pattern of t errors and detect with certainty any pattern of $(t+1)$ errors. As in case (i), the number of cosets whose leaders are n-vectors of weight t or less is given by

$$1 + \binom{n}{1}(q-1) + \ldots + \binom{n}{t}(q-1)^t .$$

All n-vectors of weights $(t+1)$ must lie in other cosets. Consider vectors whose last coordinate is non-zero. The number of such vectors of weight $(t+1)$

is $\binom{n-1}{t}(q-1)^{t+1}$.

The distance between any two such vectors is at most (2t+1). No two of these can be in the same coset because otherwise there will exist two code-words with distance between them equal to 2t+1 or less. But this contradicts the hypothesis that $d = 2t+2$. Hence,

$$(3.33) \qquad 1 + \binom{n}{1}(q-1) + \ldots + \binom{n}{t}(q-1)^t + \binom{n-1}{t}(q-1)^{t+1} \leq q^r \quad .$$

The Hamming-Rao bounds apply to non-linear codes as well [14].

The left hand side of (3.32) is asymptotically equal to

$$q^{n\,H_q(\frac{t}{n}) + t\log(q-1)} \quad .$$

Thus for large n and d, an (n,k) linear code with minimum distance d does not exist if

$$(3.34) \qquad k/n > 1 - H_q\left(\frac{d-1}{2n}\right) - \frac{d-1}{2n}\log(q-1) \quad .$$

For binary linear codes (3.34) takes the form

$$(3.35) \qquad \frac{k}{n} > 1 - H_q\left(\frac{d-1}{2n}\right) \quad .$$

$\frac{k}{n}$ is called the transmission rate. For a binary symmetric channel $1 - H(p)$ is the channel capacity where p is the probability of a transmitted symbol being received as the other one.

3.5. <u>The Johnson bound.</u> A new upper bound on the size of non-linear binary error-correcting codes and its asymptotic form have been derived in [15] and [16]. The problem is stated as follows: Find the maximum subset of vertices of an n-dimensional unit cube such that any two vertices of this subset are at least Hamming distance d apart, that is, their coordinate vectors differ in at least d places, where $d = 2t+1$ for a t-error correcting code.

Let $A(n,d)$ be the maximum number of rows in a matrix of n columns with entries of zeros and ones, with the property that any two row vectors differ in at least d places.

Let $R(m, r, \lambda)$ be the maximum number of vectors each having r ones and $(m-r)$ zeros, with the property that the inner product of any two of the vectors is $\leq \lambda$.

Then for any two binary n-vectors with weights r_i and r_j having inner product λ_{ij} and the Hamming distance d_{ij},

$$r_i + r_j = 2\lambda_{ij} + d_{ij} \quad . \tag{3.36}$$

Let E_n be the set of 2^n vertices of the n-dimensional unit cube to be divided into disjoint subsets as follows:

$$E_n = S_0 + S_1 + \ldots + S_{d-1} \quad , \tag{3.37}$$

where S_0 is the desired maximum subset of vertices at least Hamming distance d apart from each other and S_k is the subset of vertices at distance k from S_0.

Let $|X|$ denote the number of points in a point set X.

Then,

$$A(n,d) = |S_0| \tag{3.38}$$

and

$$2^n = |S_0| + |S_1| + \ldots + |S_{d-1}| \tag{3.39}$$

For $r \leq t$, we have

$$|S_r| = \binom{n}{r} |S_0| \quad . \tag{3.40}$$

Then the Hamming bound for a non-linear code can be easily obtained as

$$2^n > |S_0| \sum_{i=0}^{t} \binom{n}{i} \quad . \tag{3.41}$$

An improvement on the Hamming bound is given in [15] by considering the sets of S_k for $k > t$. This can be stated as follows:

$$(3.42) \qquad 2^n \geq |S_0| \left\{ \sum_{i=0}^{t} \binom{n}{i} + \frac{\binom{n}{t+1} - \binom{d}{t} R(n,d,t)}{\left[\frac{n}{t+1}\right]} \right\},$$

where $\left[\frac{n}{t+1}\right]$ is the largest integer contained in $\frac{n}{t+1}$. A further improvement on (3.42) has been obtained and an asymptotic expression derived in [16]. This expression involves a complicated function $g(F)$ where F is defined as $F = n/t$, which has been tabulated in [16] for several values of F. For an (n,k) linear code Johnson's bound can be stated as

$$(3.43) \qquad 1 - \frac{k}{n} \geq H\left(\frac{1+g(F)}{F}\right) .$$

The following graph taken from [16], shows the different asymptotic upper and lower bounds for binary linear codes.

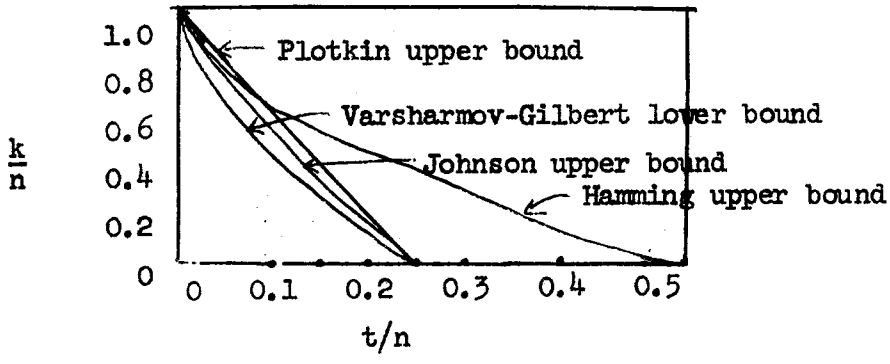

Fig. 1 Comparison of asymptotic bounds.

Improved lower bounds on the size of non-linear binary codes are given in [1].

3.6. Discussion on bounds. Among the known codes, the Hamming codes and the equivalent highest rate Reed-Muller codes and Bose-Chaudhuri codes meet the Plotkin bound. Hence these codes have the maximum-minimum distance.

For large n their rates all approach 0 or 1. In the middle rate range, for both the Reed-Muller and the best available estimate for the Bose-Chaudhuri codes with any fixed non-zero rate, the ratio d/n approaches 0 as n approaches infinity. There is no known coding system for which it has been proved that d/n remains finite as n approaches infinity with the transmission rate k/n held fixed, though the Varsharmov-Gilbert bound shows that such codes exist. For the binary symmetric channel, Elias' error-free coding [10] is known to be capable of achieving a probability or error which tends to zero, maintaining a transmission rate k/n which is bounded away from zero with large n. But the rate for Elias' code is much below channel capacity.

According to Shannon's fundamental theorem for noisy channels, for any rate k/n less than the channel capacity 1 - H(p) there exist codes for which the probability of error is arbitrarily small. But no non-random coding is known to achieve this. For a more detailed account see [17].

REFERENCES

1. Bambah, R. P., Joshi, D. D. and Luthar, I. S. (1961). Some lower bounds on the number of code points in a minimum distance binary code. Inf. and Control, 4, 313-323.

2. Barlotti, A. (1957). Una limitzione superiore per il numero di punti appartenenti a una k-calotta C(k,0) di uno spazio lineare finito. Boll. Un. Mat. Ital: (3), 12, 67 - 70.

3. Barlotti, A. (1965). Bounds for k-caps in PG(r,q) useful in the theory of error-correcting codes. To be presented at the École d'été sur le Codage, Royan, France.

4. Bose, R. C. (1947). Mathematical theory of the symmetrical factorial designs. Sankhya, 8, 107-166.

5. Bose, R. C. (1961). On some connections between the design of experiments and information theory. Bull. Inter. Statist. Inst. 38, 257-271.

6. Bose, R. C. and Ray-Chaudhuri, D. K. (1960). On a class of error-correcting group codes. Inf. and Control, 3, 68-79.

7. Bose, R. C. and Ray-Chaudhuri, D. K. (1960). Further results on error-correcting binary group codes. Inf. and Control, 3, 279-290.

8. 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, 408-414.

9. Burton, R. C. (1964). An application of convex sets to the construction of error-correcting codes and factorial designs. Ph. D. thesis submitted to the University of North Carolina at Chapel Hill, Institute of Statistics, Mimeo series No. 393.

10. Elias, P. (1954). Error-free coding. IRE Trans., PGIT-4, 29-37.

11. Gilbert, E. N. (1952). A comparison of signalling alphabets. Bell System Tech. J., 31, 504-522.

12. Golay, M. J. E. (1949). Notes on digital coding. Proc. IRE, 37, correspondence, 657.

13. Gorenskin, D., Peterson, W. W. and Zierler, N. (1960). Two-error-correcting Bose-Chaudhuri codes are quasi-perfect. Inf. and Control, 3, 291-294.

14. Hamming, R. W. (1950). Error detecting and error correcting codes. Bell System Tech. J., 29, 147-160.

15. Johnson, S. M. (1962). A new upper bound for error-correcting codes. IRE Trans., IT-8, 203-207.

16. Johnson, S. M. (1963). Improved asymptotic bounds for error-correcting codes. IEEE Trans., IT-9, 198-205.

17. Peterson, W. W. (1961). Error-correcting codes, The M.I.T. Press and John Wiley and Sons, Inc., New York.

18. Plotkin, M. (1960). Binary codes with specific minimum distance. IRE Trans., IT-6, 445-450.

19. Quist, B. (1952). Some remarks concerning curves of the second degree in a finite plane. Ann. Acad. Sci. Fenn. Ser. A., I, No. 134

20. Segre, B., (1957). Le geometrie di Galois, Ann. Mat. Pura Appl. (4), 1-97.

21. Tallini, G. (1956) Sulle k-calotte di uno spazio lineare finito. Ann. Mat. Pura Appl. (4), 42, 119-164.

22. Varsharmov, R. R. (1957). Estimate of the number of signals in error-correcting codes. Doklady A.N.S.S.S.R., 117, No. 5, 739-741.