SOME BOUNDS ON LINEAR CODES

by A. M. Malhotra, *Department of Mathematics, Dayal Singh College, New Delhi* 110 003

(*Received* 16 *June* 1976; *after revision* 22 *January* 1977)

The paper presents two bounds over the number of parity-check digits for codes that detect or correct certain specified types of errors.

1. Introduction

The occurrence of errors is usually found to be in the form of a burst in most of the communication systems. However, it is also noticed that during the transmission, all the digits inside the burst may not be disrupted. Therefore, it is uneconomical to use the usual burst-error detecting/correcting codes in such situations, necessitating thereby the need to develop codes capable of detecting/correcting bursts of low-density, high-density and moderate density. The problems of developing codes detecting/correcting these types of errors have been studied by Sharma and Dass (1974), Dass (1974, 1975), Gupta (1975, 1976) and others. Some work in this direction, by considering the sub-block structure, has also been done by Gupta and Malhotra (1976).

In this paper, we give two bounds for codes which detect/correct separately/simultaneously random errors and bursts of moderate density. These results generalize the study made by the authors mentioned above.

We shall confine ourselves to linear codes over $GF(q)$ having n as the code length. By a burst of length b, we shall mean an n-tuple whose only non-zero components are confined to the b consecutive digit positions, the first and the last of which are non-zero. The weight of a vector is understood to be in the usual Hamming sense (1950).

2. An Upper Bound

In this section, we give an upper bound over the number of check digits for a code with minimum weight at least w and having no burst of length b or less with weight lying between w_1 and w_2 as a code word. This bound ensures the existence of a code that can detect all error patterns which are either random errors of weight $(w - 1)$ or less or bursts of length b or less whose weight lies between w_1 and w_2.

Theorem 1—Given positive integers w, w_1, w_2 and b, such that $w \leqslant w_1 \leqslant w_2 \leqslant b$, there exists an (n, k)-linear code over $GF(q)$ with minimum weight at least w and having no burst of length b or less with weight lying between w_1 and w_2 as a code word satisfying

$$q^{n-k} \leqslant \sum_{i=0}^{w-2} \binom{n}{i} (q-1)^i + \sum_{i=w_1-1}^{w_2-1} \binom{b-1}{i} (q-1)^i . \qquad \ldots(1)$$

PROOF: We shall show the existence of the desired code by constructing a parity-check matrix H for the code.

Choose a non-zero $(n-k)$-tuple as the first column of the parity-check matrix H. Suppose that we have chosen $j-1$ columns $h_1, h_2, \ldots, h_{j-1}$ suitably. As the minimum weight of the code is required to be at least w, the column h_j should not be a linear combination of any $(w-2)$ or less previous columns, i.e.,

$$h_j \neq a_i h_{i_1} + a_2 h_{i_2} + \ldots + a_{w-2} h_{i_{w-2}}. \qquad \ldots(2)$$

The coefficient a_i, including the pattern of all zeros, can be chosen in

$$\sum_{i=0}^{w-2} \binom{j-1}{i} (q-1)^i \qquad \ldots(3)$$

ways. Also, no burst of length b or less, whose weight lies between w_1 and w_2, can be a code word; therefore, h_j should not be a linear combination of any $w_2 - 1$ or less but of $w_1 - 1$ or more columns among the immediately preceding $(b-1)$ columns, which can be chosen in

$$\sum_{i=w_1-1}^{w_2-1} \binom{b-1}{i} (q-1)^i \qquad \ldots(4)$$

ways. Thus, the total number of columns to which h_j cannot be equal, is

$$\sum_{i=0}^{w-2} \binom{j-2}{i} (q-1)^i + \sum_{i=w_1-1}^{w_2-1} \binom{b-1}{i} (q-1)^i \qquad \ldots(5)$$

At worst, if all the linear combinations in (5) for all possible choices of the coefficients in (2) yield a distinct sum, the column h_j can be added, provided these should not exhaust the whole set of q^{n-k} columns, i.e., if

$$q^{n-k} > \sum_{i=0}^{w-2} \binom{j-1}{i} (q-1)^i + \sum_{i=w_1-1}^{w_2-1} \binom{b-1}{i} (q-1)^i . \qquad \ldots(6)$$

The result now follows by taking n to be the largest value of j, satisfying the preceding inequality, i.e., by taking $j = n + 1$, the inequality in (6) will get reversed and in that case we shall get (1).

Alternative form—If we take B to be the largest value of b satisfying (6), then for $b = B + 1$ and $j = n$, we get

$$q^{n-k} \leqslant \sum_{i=0}^{w-2} \binom{n-1}{i} (q-1)^i + \sum_{i=w_1-1}^{w_2-1} \binom{B}{i} (q-1)^i. \qquad \ldots(7)$$

Asymptotic result—We shall now obtain the asymptotic form of the above result for $q = 2$ and $w_2 = b$.

For $q = 2$ and $w_2 = b$, the inequality (1) reduces to

$$2^{n-k} \leqslant \sum_{i=0}^{w-2} \binom{n}{i} + \sum_{i=w_1-1}^{b-1} \binom{b-1}{i}$$

$$= \sum_{i=n-(w-2)}^{n} \binom{n}{i} + \sum_{i=w_1-1}^{b-1} \binom{b-1}{i}$$

$$= \sum_{((n-w+2)/n)n}^{n} \binom{n}{i} + \sum_{i=[(w-1)/(b-1)](b-1)}^{b-1} \binom{b-1}{i}$$

Using the well-known Chernov-bound, viz.,

$$\sum_{i=\alpha n}^{n} \binom{n}{i} \leqslant \alpha^{-\alpha n} \beta^{-\beta n}, \quad \alpha > \tfrac{1}{2}, \beta = 1 - \alpha$$

$$\alpha, \beta \neq 0;$$

we get

$$2^{n-k} \leqslant \left(\frac{n-w+2}{n}\right)^{-(n-w+2)} \left(\frac{w-2}{n}\right)^{-(w-2)} + \left(\frac{w_1-1}{b-1}\right)^{-(w_1-1)}$$

$$\times \left(\frac{b-w_1}{b-1}\right)^{-(b-w_1)} n > 2(w-2), 2w_1 > b+1.$$

Using the binary entropy function

$$H(p) = -p \log_2 p - (1-p) \log_2 (1-p),$$

we get

$$2^{n-k} \leqslant 2^{nH(p_1)} + 2^{(b-1)H(p_2)};$$

where

$$H(p_1) = H\left(\frac{n-w+2}{n}\right),$$

and

$$H(p_2) = H\left(\frac{w_1-1}{b-1}\right).$$

We now give an example of a moderate-density burst detecting linear code having a minimum weight criterion.

EXAMPLE

The null space of the following 6×11 matrix

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

is a (11, 5) linear code, which has minimum weight $w = 3$ and has no burst of length $b = 5$ or less with weight lying between 3 and 4 as a code word.

Particular Cases

1. The bound in Theorem 1 has been obtained for $w \leqslant w_2$. If we take $w > w_2$, the idea of burst becomes superfluous and the resulting bound becomes the well-known Varshamov-Gilbert bound (cf. Peterson 1961, Theorem 4.4).

2. Setting $w = w_1$ in the bound obtained in (6) and taking $j = n$, we get

$$q^{n-k} > \sum_{i=0}^{w-2} \binom{n-1}{i} (q-1)^i + \sum_{i=w-1}^{w_2-1} \binom{b-1}{i} (q-1)^i.$$

This reduces to the result obtained by Dass (1976) giving an upper bound on the number of check-digits for the existence of an (n, k) code with minimum weight at least w and having no burst of length b or less with weight w_2 or less as a code word.

3. Setting $w_2 = b$ and $j = n$ in the bound obtained in (6), we get

$$q^{n-k} > \sum_{i=0}^{w-2} \binom{n-1}{i} (q-1)^i + \sum_{i=w_1-1}^{b-1} \binom{b-1}{i} (q-1)^i,$$

which gives an upper bound on the number of check-digits for the existence of an (n, k) code with minimum weight at least w and having no burst of length b or less with weight w_1 or more as a code word.

4. Setting $w = w_1$ and $w_2 = b$ in (6), and taking $j = n$, we get

$$q^{n-k} > \sum_{i=0}^{w-2} \binom{n-1}{i} (q-1)^i + \sum_{i=w-1}^{b-1} \binom{b-1}{i} (q-1)^i.$$

This reduces to a result obtained by Sharma and Dass (1974), which gives an upper bound on the number of check-digits for the existence of an (n, k) code with minimum weight at least w and having no burst of length b or less as a code word.

Several other particular cases can also be discussed by relaxing the weight imposed over the code. These include, in particular, results due to Dass (1974) and Gupta (1976).

3. A Lower Bound

In this section, we extend the Hamming sphere-packing bound to a code, which is capable of correcting bursts of length b or less with weight lying between w_1 and w_2.

Theorem 2—An (n, k) linear code over $GF(q)$ that corrects all random errors of weight w or less and all bursts of length b or less with weight lying between w_1 and w_2 must have at least

$$\log_q \left[\sum_{i=0}^{w} \binom{n}{i}(q-1)^i + \sum_{t=w_1}^{b} (n-t+1) \sum_{i=w_1}^{w_2} \binom{t-2}{i-2}(q-1)^i\right], \quad w < w_1 \leqslant w_2 \leqslant b \qquad \ldots(8)$$

parity-check digits.

Proof: As the code corrects all random errors of weight w or less, all such vectors should belong to different cosets; their number, including the pattern of all zeros, is

$$\sum_{i=0}^{w} \binom{n}{i}(q-1)^i. \qquad \ldots(9)$$

Also, the code corrects all bursts of length b or less with weight lying between w_1 and w_2; therefore, all such error patterns should also be in different cosets. The number of bursts of length b that are of weight $i\,(i > 1)$ is

$$\binom{b-2}{i-2}(n-b+1)(q-1)^i.$$

Therefore, the number of bursts of length b that are of weight lying between w_1 and w_2 is

$$(n+b+1)\sum_{i=w_1}^{w_2} \binom{b-2}{i-2}(q-1)^i.$$

Since the length of a burst of weight t is at least t, the total number of bursts of length b or less that are of weight less than or equal to w_2, but greater than or equal to w_1, is

$$\sum_{t=w_1}^{b} (n - t + 1) \sum_{i=w_1}^{w_2} \binom{t-2}{i-2} (q-1)^i. \qquad \ldots(10)$$

Thus, the total number of error patterns to be corrected, is

$$\sum_{i=0}^{w_1} \binom{n}{i} (q-1)^i + \sum_{t=w_1}^{b} (n - t + 1) \sum_{i=w_1}^{w_2} \binom{t-2}{i-2} (q-1)^i. \qquad \ldots(11)$$

As the number of cosets should be as large as the number of patterns to be corrected we have

$$q^{n-k} \geqslant \sum_{i=0}^{w} \binom{n}{i} (q-1)^i + \sum_{t=w_1}^{b} (n - t + 1) \sum_{i=w_2}^{w_2} \binom{t-2}{i-2} (q-1)^i. \qquad \ldots(12)$$

The result now follows by taking the logarithm on both the sides.

Particular Cases

1. The result (8) has been proved for $w \leqslant w_2$. If we take $w > w_2$, the burst consideration becomes redundant and the resulting bound reduces to the well-known Hamming's sphere-packing bound (Hamming 1950) (cf. Peterson 1961, Theorem 4.5).

2. Setting $w_2 = b$ in (8), we get the number of parity-check digits for a code which corrects all random errors of weight w or less and bursts of length b or less with weight w_1 or more, as

$$\log_q \left[\sum_{i=0}^{w} \binom{n}{i} (q-1)^i + \sum_{t=w_1}^{b} (n - t + 1) \sum_{i=w_1}^{b} \binom{t-2}{i-2} (q-1)^i \right].$$

3. Setting $w_1 = w + 1$ in (8), we see that at least

$$\log_q \left[\sum_{i=0}^{w} \binom{n}{i} (q-1)^i + \sum_{t=w+1}^{b} (n - t + 1) \sum_{t=w+1}^{w_2} \binom{t-2}{i-2} (q-1)^i \right]$$

check-digits are required for a code that corrects all random errors of weight w or less and all bursts of length b or less whose weight is w_2 or less, a result proved by Sharma and Dass (1976).

4. Setting $w_1 = w + 1$ and $w_2 = b$ in (8), we get at least

$$\log_q \left[\sum_{i=0}^{w} \binom{n}{i} (q-1)^i + \sum_{t=w+1}^{b} (n-t+1) \sum_{i=w+1}^{b} \binom{t-2}{i-2} (q-1)^i\right]$$

number of parity-check digits required for a code that corrects all random errors of weight w or less and all bursts of length b or less. This result has also been obtained by Sharma and Dass (1974).

5. Setting $w = 0$ in (8), we get

$$\log_q \left[1 + \sum_{t=w_1}^{b} (n-t+1) \sum_{i=w_1}^{w_2} \binom{t-2}{i-2} (q-1)^i\right]. \quad \text{...(13)}$$

This gives the necessary number of parity-check digits required for a code that corrects all bursts of length b or less with weight lying between w_1 and w_2. This result is valid only when $w_1 \neq 1$. If we take $w_1 = 1$, then in the summation given in (13), the value for $w_1 = 1$ is to be replaced by $n(q-1)$. The same result was obtained earlier by Gupta (1976).

The discussion made above for $w_1 = 1$ applies to the following three particular cases also.

6. Setting $w = 0$ and $w_2 = b$ in (8), we notice that an (n, k) linear code which corrects all bursts of length b or less whose weight is w_1 or more, should have at least

$$\log_q \left[1 + \sum_{t=w_1}^{b} (n-t+1) \sum_{i=w_1}^{b} \binom{t-2}{i-2} (q-1)^i\right]$$

number of parity-check digits.

7. Setting $w = 0$ and $w_1 = 1$ in (8), we get that at least

$$\log_q \left[1 + \sum_{t=1}^{b} (n-t+1) \sum_{i=1}^{w_2} \binom{t-2}{i-2} (q-1)^i\right]$$

parity-check digits are necessary for a code that corrects all bursts of length b or less whose weight is w_2 or less. This result has been proved by Sharma and Dass (1974).

8. Setting $w = 0$, $w_1 = 1$ and $w_2 = b$ in (8), we get

$$\log_q \left[1 + \sum_{t=1}^{b} (n-t+1) \sum_{i=1}^{b} \binom{t-2}{i-2} (q-1)^i\right]$$

as the number of parity-check digits necessary for an (n, k) code which corrects all bursts of length b or less. This result was proved by Fire (1959) in the binary case (cf. Peterson 1961, Theorem 4.9).

ACKNOWLEDGEMENT

The author sincerely thanks his research supervisor Dr. B. D. Sharma, Reader, Department of Mathematics, University of Delhi, for his help and guidance in the preparation of this paper. The author is also thankful to the referee for his helpful remarks on the original version of the paper.

REFERENCES

Dass, B. K. (1974). Bounds for codes detecting burst-errors with weight constraints. *Proc. Conf. on Measures of Information and Their Applications*, I.I.T., Bombay, August.

——— (1975). A sufficient bound for codes correcting bursts with weight constraints. *J. Ass. Comput. Mach.*, pp. 501–3.

——— (1976). A bound for burst detecting code. *J. Comb. Inf. System Sci.*, **1** (1), 21–24.

Fire, P. (1959). A Class of Multiple-Error-Correcting Binary Codes for Non-independent Errors. Sylvania Report RSL–E–2, Sylvania Reconnaissance System Laboratory, Mountain View, California.

Gupta, S. N. (1975). On the existence of moderate-density-burst codes. *J. math. Sci.*, **10**, 8–12.

——— (1976). A study of block-wise error correcting and protecting burst codes. *Ph.D. Thesis*, University of Delhi.

Gupta, S. N., and Malhotra, A. M. (1976). Linear codes having a sub-block structure. *J. Cybernatics*, **6**, 263-70.

Hamming, R. W. (1950). Error detecting and error correcting codes. *B.S.T.J.*, **29**, 147–60.

Peterson, W. W. (1961). Error Correcting Codes. The M.I.T. Press, Cambridge, Mass.

Sharma, B. D., and Dass, B. K. (1974). Extended Varshamov-Gilbert and sphere-packing bounds for burst correcting codes. *IEEE Trans. Inf. Theory*, *IT*-**20**, 291–92.

——— (1976). On linear codes correcting random and low-density-burst errors. *J. Linear Algeb. Applic.* (to appear).