Numero 6 - 1993

RATIO MATHEMATICA

Fascicolo dedicato alla
Crittografia

a cura di

Franco Eugeni e Giovanni Moro

INDICE

A bound for codes correcting random and low-density closed-loop burst errors .
(L. Berardi e B.K. Dass) .... pag. 1

Sul periodo delle matrici di permutazione .
(G. Campanini e A. Di Porto) ....pag. 6

Pseudorandom generators based on Lucas Sequences .
(A. Di Porto e W. Wolfowicz) ....pag. 15

I servizi crittografici delle Marine Britannica e Italiana.
(L. Donini) ....pag. 23

A Note on the Matrices of Maximum Order in GLH[k,p] and an Example of their Cryptographic Application.
(M. Elia) ....pag . 49

Osservazioni sulla distribuzione dei numeri primi dei tipi
(6n - 1) e (6n + 1) - n ≥ 1 intero.
(F. Eugeni e G. Moro) ....pag . 60

Note on cipher hypersystem
(S. Innamorati e F. Zuanni) ....pag . 74

Rappresentazione geometrica di parole.
(C. F. Manara) ....pag . 79

Su alcune strutture di spazio metrico con sostegno l'insieme delle variabili casuali associate a successioni di numeri a caso
(A. Maturo) ....pag . 84

A bound for codes correcting random and low-density closed-loop burst errors .

L. Berardi, Dip. di Ingegneria Elettrica, Università degli Studi dell'Aquila,
Monteluco di Roio, I-67100, L'Aquila, Italy
B.K. Dass, Dep. of Mathematics, P.G.D.A.V.Collage (Univ. of Delhi), Nehru Nagar,
New Delhi-110065, India

ABSTRACT

This paper presents a lower bound on the number of parity-check digits required for a linear code that corrects random errors and errors which are in the form of closed-loop low-density bursts.

INTRODUCTION

In some communication systems errors occur predominantly in the form of bursts. There are of course many situations in which errors occur in the form of a burst but not all digits inside the burst get corrupted, i.e. errors occur in the form of low-density bursts. In actual communication, while it is all important to consider correction of low-density bursts, care must be taken to correct at least up to a specific number of random errors no matter where they lie.

Most of the studies regarding the detection and correction of burst errors have been made with respect to what are called "open-loop burst" defined as: "An *open-loop burst* of length b is a vector whose only nonzero components are confined to b consecutive

[1] This work was carried out while the **second** author was Visiting Professor in L'Aquila (June-July, 1991) under C.N.R. grant.

positions, the first and the last of which are nonzero" [5].
There is another definition of the term *burst* which reads: "A *closed-loop burst* of length b, $2 \le b \le (n+1)/2$, is a vector $(a_1, a_2, \dots, a_n)$ whenever there is an index i such that $1 \le i \le b-1$, $a_i \cdot a_{n-b+i+1} \neq 0$ and $a_{i+1} = a_{i+2} = \dots = a_{n-b+i} = 0$ ".
This definition has also been found useful in certain communication systems though not much of the studies have been carried out with respect to it. Clearly, the definition of a closed-loop burst includes the definition of an open-loop burst, therefore, while considering the class of closed-loop bursts of length b or less, the set of open-loop bursts of length b or less is included in it.

Sharma and Dass [6] have given a lower bound over the number of parity-check digits for codes capable of correcting simultaneously random errors and low-density open-loop burst errors. In this paper, a lower bound over the number of parity-check digits for codes capable of correcting simultaneously random errors and low-density closed-loop burst errors has been derived.
In what follows, we shall confine ourselves to linear codes over GF(q) of length *n*. The weight of a vector is understood to be in the usual Hamming sense [3].

A LOWER BOUND

The following result presents a lower bound on the number of parity-check digits required for a linear code that corrects all random errors of weight m or less and all closed-loop bursts of length b or less with weight w or less. This result generalizes the well-known sphere-packing bound as well as results due to Campopiano [1], Dass and Muttoo [2], Muttoo and Tyagi [4].

THEOREM. The number of parity-check digits in an (n,k) linear code over GF(*q*) that corrects all combinations of m or fewer errors and all closed-loop bursts of length b or less with weight w or less, $1 \le m < w \le b < n/2$, is at least

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

where

$$[1+x]^{(m,r)} = \begin{cases} 1 + \binom{m}{1} x + \ldots + \binom{m}{r} x^r, & 0 < r \le m \\ 1 , & r = 0 \\ 0 , & r < 0 \end{cases} .$$

PROOF. Since the code is capable of correcting all errors of weight m and less, all n-tuples of weight m and less should be in different cosets of the standard array; their number, including the pattern of all zeros, is

$$[1 + (q-1)]^{(m,n)} \qquad (2)$$

Also, since the code corrects all those closed-loop bursts of length b or less which are of weight w or less, all such burst patterns must also be in different cosets except for those which are random errors of weight m or less. Since the closed-loop bursts of length m or less have weight m or less and hence are included in (2), we need only compute the number of closed-loop bursts of length m+1,m+2,...,b with weight greater than m but of weight less than or equal to w. The number of closed-loop bursts of length i (> m), i < n/2, with weight greater than m but of weight less than or equal to w is

$$n \sum_{j=m+1}^{w} \binom{i-2}{j-2} (q-1)^j \qquad (3)$$

which gives the number of closed-loop bursts of length m+1, m+2, ...,b with weight greater than m but of weight less than or equal to w as

$$n \sum_{i=m+1}^{b} \sum_{j=m+1}^{w} \binom{i-2}{j-2} (q-1)^j . \qquad (4)$$

Thus, the total number of errors to be corrected becomes

$$[1+(q-1)]^{(n,m)} + n \sum_{i=m+1}^{b} \sum_{j=m+1}^{w} \binom{i-2}{j-2} (q-1)^j . \qquad (5)$$

Since there must be at least this number of cosets, and the total number of available cosets is q^{n-k}, therefore we must have

$$q^{n-k} \geq [1+(q-1)]^{(n,m)} + n \sum_{i=m+1}^{b} \sum_{j=m+1}^{w} \binom{i-2}{j-2} (q-1)^{j}. \qquad (6)$$

The theorem now follows by taking the logarithm on both the sides of (6) to the base q. □

Incidentally, it can be shown that the result applies to non-linear codes also.

DISCUSSION

For $m \geq w$, the second term in (5) vanishes and the bound reduces to Hamming's sphere-packing bound (cf.[5,Th.4.5]).

For $w = b$, the lower bound on the number of parity-checks obtained in the theorem becomes

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

which coincides with a result due to Dass and Muttoo [2] obtained for a code that corrects random and closed-loop burst errors simultaneously.

Next, setting $m = 1$, the bound obtained in (1) reduces to

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

which coincides with a result due to Muttoo and Tyagi [4] obtained for a code that corrects low-density closed-loop burst errors.

Lastly, for $m = 1$ and $w = b$, the bound obtained in (1), as expected becomes

$$\log_q \left[1 + n(q-1)\, q^{b-1} \right] \quad ,$$

which was proved by Campopiano [1].

REFERENCES

[1] C.N.CAMPOPIANO, Bounds on Burst-Error-Correcting Codes, *IEEE Trans.*, IT,pp.257-259,1962.

[2] B.K.DASS and S.K.MUTTOO, Codes Correcting Random and Closed Loop Bursts, *Bull.Cal.Math.Soc.* (to appear).

[3] R.W.HAMMING, Error Detecting and Error Correcting Codes, *Bell Syst.Tech.J.*,Vol.29,pp.147-160,1950.

[4] S.K.MUTTOO and V.K.TYAGI, Bounds for Codes Correcting Low-Density Closed-Loop Bursts, Communicated.

[5] W.W.PETERSON and E.J.WELDON Jr.,*Error-Correcting Codes,* MIT Press, Mass.,1972.

[6] B.D.SHARMA and B.K.DASS, On Linear Codes Correcting Random and Low-Density Burst Errors, *Linear Algebra and its Applications,* Vol.16, No.1, pp.5-18,1977.