Sunil Kumar Muttoo; Shankar Lal

A reversible code over $GF(q)$

Kybernetika, Vol. 22 (1986), No. 1, 85--91

Persistent URL: http://dml.cz/dmlcz/125543

KYBERNETIKA — VOLUME 22 (1986), NUMBER 1

A REVERSIBLE CODE OVER $GF(q)$

SUNIL KUMAR MUTTOO*, SHANKAR LAL

This paper deals with the construction of codes over $GF(q)$, q prime, by annexing two triangular matrices, one upper triangular and the other lower triangular. The error-correction capabilities of such codes are also studied.

0. INTRODUCTION

An (n, k) linear code C of length n over $GF(q) \equiv F_q$, a Galios field of order q, where q is a prime, is a k-dimensional linear subspace of F_q^n, where F_q^n denotes the space of all n-tuples over $GF(q)$. A generator matrix G of this code is a $k \times n$ matrix whose rows form a basis of C. The parity-check matrix H of this code is an $(n - k) \times n$ matrix such that $Hv^T = 0$ for all vectors $v \in C$. The row space of $(n - k) \times n$ matrix H is an $(n, n - k)$ linear code $C^\perp$ called dual code of C. The Hamming weight of a vector is the number of non-zero elements in it. A code word in C consists of some k symbols as message or information symbols and the remaining symbols as check-digits [2].

A class of codes called 'reversible codes' introduced by Massey [3] is defined as follows:

Definition. A linear code C is called reversible if a vector obtained by reversing the order of the digits of a code word in C result in a code word in C, i.e., $(v_0, v_1, \ldots$ $\ldots, v_{n-1}) \in C$ implies that $(v_{n-1}, v_{n-2}, \ldots, v_1, v_0) \in C$.

Consider a $(k + 1) \times (2k + 1)$ matrix H_k over $GF(q)$ (q prime) formed by annexing two square triangular matrices, one upper triangular and the other lower triangular such that the last column of the first is the first column of the second, where the

* The author carried out this research work under a minor research project sponsored by U.G.C., India.

entries are chosen in a well-defined way viz. consider H_k of the type

$$H_k = \quad k+1 \updownarrow \begin{bmatrix} \multicolumn{6}{c}{\longleftarrow k \longrightarrow} & & \multicolumn{7}{c}{\longleftarrow k \longrightarrow} \\ x_1 & x_2 & x_3 & \dots & x_{k-1} & x_k & y & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & x_2 & x_3 & \dots & x_{k-1} & x_k & y & x_k & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & x_3 & \dots & x_{k-1} & x_k & y & x_k & x_{k-1} & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & \dots & x_{k-1} & x_k & y & x_k & x_{k-1} & x_{k-2} & \dots & 0 & 0 & 0 \\ \dots & & & & & & & & & & & & & \dots \\ \dots & & & & & & & & & & & & & \dots \\ 0 & 0 & 0 & \dots & 0 & x_k & y & x_k & x_{k-1} & x_{k-2} & \dots & x_3 & x_2 & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 & y & x_k & x_{k-1} & x_{k-2} & \dots & x_3 & x_2 & x_1 \end{bmatrix}$$

where $y,\ x_i \in (1, 2, \dots, q-1)$ and $(x_i, y) = 1$ and $(x_i, x_j) = 1$ for $i \neq j,\ i, j = 1, 2, \dots, k$.

The code obtained by considering H_k as the parity-check matrix will be a $(2k+1, k)$ linear code C_k. It will be shown that the code C_k which is the null space of H_k turns out to be reversible, as defined by Massey [3] and for further work one may refer to Tzeng and Hartmann [6]. It is also shown that such codes are capable of correcting a well-defined class of solid burst errors. Codes correcting solid bursts have also been studied by Shiva and Sheng [5].

In what follows, by a solid burst of length b we shall mean an n-tuple whose all the b non-zero components are among some b adjacent positions.

1. CHARACTERIZATION

In the following theorem we prove that the code C_k is a reversible code. We first prove a lemma.

Lemma 1. The number of non-zero components in any code word of C_k, in the first k-positions and in the last k-positions is same.

Proof. Let $h_1, h_2, \dots, h_{2k+1}$ denote the columns of H_k, h_i denoting the ith column. The formation of the last k-columns of H_k may be stated as

$$\begin{aligned} h_{k+2} &= a_1 h_{k+1} + b_1 h_1 \\ &\vdots \\ h_{2k+1} &= a_k h_{k+1} + b_k h_k \end{aligned}$$

or

$$h_{k+1+i} = a_i h_{k+1} + b_i h_i\,, \quad i = 1, 2, \dots, k$$

where $$0 < a_i \leqq q - 1\,, \quad 0 < b_i \leqq q - 1\,.$$

Let there be a code word with s non-zero components at the i_1th, i_2th, …, i_sth place in the last k positions. Then

$$(1) \qquad h_{k+1+i_1} + h_{k+1+i_2} + \ldots + h_{k+1+i_s} =$$
$$= (a_{i_1} + a_{i_2} + \ldots + a_{i_s})\, h_{k+1} + (b_{i_1}h_1 + b_{i_2}h_2 + \ldots + b_{i_s}h_s)\,.$$

Case I. When $a_{i_1} + a_{i_2} + \ldots + a_{i_s} = 0$.

The R.H.S. of (1) is clearly a sum of exactly s columns from the first k-columns, $h_1, h_2, \ldots, h_k$ of H_k. Thus there are exactly s non-zero components in the first and in the last k positions of the code word under discussion.

Case II. When $0 < a_{i_1} + a_{i_2} + \ldots + a_{i_s} \leqq q - 1$.

In this case, the R.H.S. of (1) is a sum of the $(k + 1)$th column h_{k+1} and exactly s columns from the first k columns $h_1, h_2, \ldots, h_k$ of H_k showing that there are exactly s non-zero components in the first k positions and the last k positions. □

Note that we have proved more than what has been stated in the lemma in view of the following corollary:

Corollary 2. A one-to-one correspondence between the non-zero components in the first k positions and the non-zero components in the last k positions exist, viz. the ith component $1 \leqq i \leqq k$ is related to the $(k + 1 + i)$th component.

Theorem 3. C_k is reversible.

Proof. Let $\bar{v} = (v_1, v_2, \ldots, v_{2k+1})$ be a code word of C_k. Then

$$(2) \qquad \sum_{i=1}^{2k+1} v_i h_i = 0\,.$$

We have

$$(3) \qquad h_{k+1+i} = a_i h_{k+1} + b_i h_i\,,$$

where

$$(4) \qquad b_i^{-1} = b_{k-i+1} \quad \text{and} \quad -a_i b_{k-i+1} = a_{k-i+1}$$

$i = 1, 2, 3, \ldots, k$; $a_i, b_i \in GF(q)$.

Equivalently,

$$(5) \qquad h_i = b_i^{-1} h_{k+1+i} - (a_i b_i^{-1})\, h_{k+1} = b_{k-i+1} h_{k+1+i} + a_{k-i+1} h_{k+1}\,.$$

Then (2) gives

$$\sum_{i=1}^{k} v_i h_i + v_{k+1} h_{k+1} + \sum_{i=1}^{k} v_{k+1+i} h_{k+1+i} = 0\,,$$

(using (3))

$$\Rightarrow \sum_{i=1}^{k} v_i h_i + v_{k+1} h_{k+1} + \sum_{i=1}^{k} v_{k+1+i} (a_i h_{k+1} + b_i h_i) = 0\,,$$

$$\Rightarrow \sum_{i=1}^{k} (v_i + b_i v_{k+1+i})\, h_i + \sum_{i=1}^{k} (a_i v_{k+1+i} + v_{k+1})\, h_{k+1} = 0\,.$$

Therefore, we must have

$$(6) \qquad v_i + b_i v_{k+1+i} = 0\,,$$
$$\sum_{i=1}^{k} a_i v_{k+1+i} + v_{k+1} = 0\,, \quad i = 1, 2, \ldots, k\,.$$

Consider the vector $\bar{v} = (v_{2k+1}, v_{2k}, \ldots, v_{k+2}, v_{k+1}, \ldots, v_2, v_1)$. Then

$$\bar{v}H^{\mathrm{T}} = S = v_{2k+1}h_1 + v_{2k}h_2 + \ldots + v_{k+3}h_{k-1} + v_{k+2}h_k +$$
$$+ v_{k+1}h_{k+1} + v_k h_{k+2} + \ldots + v_3 h_{2k-1} + v_2 h_{2k} + v_1 h_{2k+1}\,.$$

Using (5) and then (4), we get

$$S = (b_k v_{2k+1} + v_k)\,h_{k+2} + (b_{k-1}v_{2k} + v_{k-1})\,h_{k+3} + \ldots + (b_1 v_{k+2} + v_1)\,h_{2k+1} +$$
$$+ [a_k v_{2k+1} + a_{k-1}v_{2k} + a_{k-2}v_{2k-1} + \ldots + a_1 v_{k+2} + v_{k+1}]\,h_{k+1}$$

which on using (6) gives

$$S = 0\,.$$

Thus $\bar{v}$ is a code of C_k. Hence C_k is reversible. □

Remark. Taking $a_i = 1$, $b_i = 1$, $i = 1, 2, \ldots, k$, we have the relations

$$h_{k+1+i} = h_{k+1} + h_i\,.$$

The codes generated by the matrix satisfying the above conditions in the binary case i.e. over $GF(2)$ have been studied by Dass and Muttoo [1].

Theorem 4. The dual, $C_k^{\perp}$, of the reversible code C_k is reversible.

Proof. A parity check matrix of the code C_k is a generator matrix for the code $C_k^{\perp}$. The code words of $C_k^{\perp}$ are various linear combinations of the rows of H_k and the rows of H_k are such that the reverse of any row of H_k is again a row of H_k. Therefore, the reverse of a code word of $C_k^{\perp}$ is a code word of $C_k^{\perp}$.

This completes the proof of the theorem. □

2. ERROR CORRECTION CAPABILITIES

The following result determines the error-correction capabilities of the reversible codes considered in this paper.

Theorem 5. An (n, k) linear code C_k, $n = 2k + 1$, whose parity check matrix is H_k, is capable to correct,

(i) all solids bursts of odd lengths upto $2k - 1$, if $n - k$ is even, i.e. if k is odd,

(ii) all solids bursts of odd lengths upto $k - 1$, if $n - k$ is odd, i.e. if k is even.

Proof. Firstly, we shall derive an upper bound on the sufficient number of parity-check digits for the existence of a code that is capable to correct a solid burst of odd length, say b, by constructing a suitable parity-check matrix. The procedure involves suitable modifications of the technique used in deriving Varshamov-Gilbert-Sacks bound [4].

After having selected the first $(j-1)$ columns $h_1, h_2, \ldots, h_{j-1}$ of the parity-check matrix, the jth column h_j to be added to the matrix should be such that

$$h_j \neq (a_{j-b+1}h_{j-b+1} + a_{j-b+2}h_{j-b+2} + \ldots + a_{j-1}h_{j-1}) + b_ih_i + \\ + b_{i+1}h_{i+1} + \ldots + b_{i+b-1}h_{i+b-1},$$

where the columns h_i are any b-consecutive columns among the first $(j-i-1)$ columns, $i = 0, 2, 4, \ldots, b-1$, and all the coefficients a_i and b_i are non-zero. Thus, the coefficients a_i form a solid burst of even length $b-1$ or less and the coefficients b_i form a solid burst of odd length b or less in a $(j-i-1)$-tuple.

The number of choices of these coefficients can be calculated as follows:

If a solid burst of even length is of length $(b-1)$ then the number of solid bursts of odd length b or less in a $(j-b)$ - tuple is

(7_{b-1})
$$(j-b)(q-1) + (j-b-2)(q-1)^3 + \ldots + (j-b-b+1)(q-1)^b.$$

If a solid burst of even length is of length $(b-3)$ then the number of solid bursts of odd length b or less in a $(j-b+2)$-tuple is

(7_{b-3})
$$(j-b+2)(q-1) + (j-b)(q-1)^3 + \ldots + (j-b+2-b+1)(q-1)^b$$
$$\vdots \qquad\qquad \vdots \qquad\qquad \vdots$$

If the solid burst of even length is of length zero, then the number of solid bursts of odd length b or less in a $(j-1)$-tuple is

(7_0) $$(j-1)(q-1) + (j-3)(q-1)^3 + \ldots + (j-b)(q-1)^b.$$

Therefore, the total number of possible choices of the coefficients a_i and b_i are

$$(q-1)^{b-1}(7_{b-1}) + (q-1)^{b-3}(7_{b-3}) + \ldots + (7_0)$$

which on simplification gives

(8) $$\left[\sum_{i=1}^{(b+1)/2} (j-2i+1)(q-1)^{2i-1} - \sum_{i=1}^{(b-1)/2} q_i(q-1)^{2i+1}\right] \sum_{i=0}^{(b-1)/2} (q-1)^{2i}.$$

At worst, if all the linear combinations yield a distinct sum, then the jth column h_j can be added to H_k if

(9) $$q^{n-k} > (8).$$

But for an (n, k) linear code to exist, the inequality in (9) should hold for $j = n$, and we get

(10) $$q^{n-k} > \left[\sum_{i=1}^{(b+1)/2} (n-2i+1)(q-1)^{2i-1} - \sum_{i=1}^{(b-1)/2} 2i(q-1)^{2i+1}\right] \cdot \\ \cdot \sum_{i=0}^{(b-1)/2} (q-1)^{2i}.$$

We now prove the main result.

Case (i). Let k be odd.

The solid bursts of odd lengths upto $2k-1$ are the solid bursts of lengths $2k-1, 2k-3, \ldots, 3, 1$. For these values of b, the inequality in (10) has the form

$$q^{k+1} > [2\sum_{i=1}^{k-s} A_i - 2\sum_{i=1}^{k-s-1} B_i][\sum_{i=1}^{k-s-1} C_i] \tag{11}$$

where $A_i = (k-i+1)(q-1)^{2i-1}$, $B_i = i(q-1)^{2i+1}$, $C_i = (q-1)^{2i}$, $s = 0, 1, 2, \ldots, k$.

To prove the above claim, we employ induction technique. We wish to prove that

$$q^{k+3} > [2\sum_{i=1}^{k-s+2} A_i - 2\sum_{i=1}^{k-s+1} B_i][\sum_{i=1}^{k-s+1} C_i].$$

Now

$$q^{k+1} > [2\sum_{i=1}^{k-s} A_i - 2\sum_{i=1}^{k-s-1} B_i][\sum_{i=1}^{k-s-1} C_i] =$$

$$= [X - 2(A_{k-s+1} + A_{k-s+2} - B_{k-s} - B_{k-s+1})][Y - C_{k-s} - C_{k-s+1}]$$

where $X = 2\sum_{i=1}^{k-s+2} A_i - 2\sum_{i=1}^{k-s+1} B_i$, $Y = \sum_{i=1}^{k-s+1} C_i$. Thus

$$q^{k+1} > [XY - X(C_{k-s} + C_{k-s+1}) - 2Y(A_{k-s+1} + A_{k-s+2} - B_{k-s} - B_{k-s+1}) + \\ + 2(C_{k-s} + C_{k-s+1})(A_{k-s+1} + A_{k-s+2} - B_{k-s} - B_{k-s+1})].$$

As $k - s \geqq 1$, $s + 1 \geqq 1$, therefore

$$q^{k+3} > q^{k+1} + X(C_{k-s} + C_{k-s+1}) + 2Y(A_{k-s+1} + A_{k-s+2} - B_{k-s} - B_{k-s+1}) - \\ - 2(C_{k-s} + C_{k-s+1})(A_{k-s+1} + A_{k-s+2} - B_{k-s} - B_{k-s+1}) > XY.$$

Thus the inequality in (10) is true for all odd values of k. Hence the case (i).

Case (ii). Let k be even.

The solid bursts of odd lengths up to k are the bursts of lengths $k-1, k-3, \ldots, 5, 3, 1$. For these values of b the bound in (10) has the form

$$q^{k+1} > [2\sum_{i=1}^{(k-2s)/2} A_i - 2\sum_{i=1}^{(k-2s-2)/2} B_i]\sum_{i=0}^{(k-2s-2)/2} C_i, \quad s = 0, 1, 2, \ldots, (k-2)/2, \tag{12}$$

where A_i, B_i and C_i are as in (11). To prove that this is true, we shall use the induction technique. We wish to prove that

$$q^{k+3} > [2\sum_{i=1}^{(k-2s+2)/2} A_i - 2\sum_{i=1}^{(k-2s)/2} B_i]\sum_{i=0}^{(k-2s)/2} C_i.$$

Using the technique of case (i), the result follows. □

Example. Consider the following (4×7) matrix H_3 over $GF(5)$:

$$H_3 = \begin{bmatrix} 1 & 3 & 3 & 4 & 0 & 0 & 0 \\ 0 & 3 & 3 & 4 & 3 & 0 & 0 \\ 0 & 0 & 3 & 4 & 3 & 3 & 0 \\ 0 & 0 & 0 & 4 & 3 & 3 & 1 \end{bmatrix}$$

The columns of this matrix satisfy the relations

$$h_{k+1+i} = a_i h_{k+1} + b_i h_i , \quad i = 1, 2, 3$$

where

$$a_1 = 2 , \quad b_1 = 2 ,$$
$$a_2 = 2 , \quad b_2 = 4 ,$$
$$a_3 = 4 , \quad b_3 = 3 .$$

It can be seen that the null space of H_3, is a reversible code and corrects all solid bursts of lengths 1, 3, 5.

ACKNOWLEDGEMENT

The authors are thankful to Dr. B. K. Dass, Department of Mathematics, P. G. D. A. V. College, (University of Delhi), for his fruitful suggestions.

(Received June 14, 1984.)

REFERENCES

[1] B. K. Dass and S. K. Muttoo: A reversible code and its characterization. Presented at the 46th Conference of the Indian Mathematical Society held at Bangalore, December 27—29, 1980.

[2] F. J. Mac Williams and N. J. A. Sloane: The Theory of Error Correcting Codes. North Holland, Amsterdam 1978.

[3] J. L. Massey: Reversible Codes. Inform. and Control 7 (1964), 369—380.

[4] W. W. Peterson and E. J. Weldon, Jr.: Error Correcting Codes. Second edition. MIT Press, Cambridge, Mass. 1972.

[5] S. G. S. Shiva and C. L. Sheng: Multiple solid burst-error-correcting binary codes. IEEE Trans. Inform. Theory *IT-15* (1969), 188—189.

[6] K. K. Tzeng and C. R. P. Hartmann: On minimum distance of certain reversible cyclic codes. IEEE Trans. Inform. Theory *IT-16* (1970), 644—646.

Dr. Sunil Kumar Muttoo, Department of Mathematics, S. G. T. B. Khasa College, University of Delhi, Delhi-110007. India. Shankar Lal, Department of Mathematics, Zakir Hussain College (E), University of Delhi, Delhi-110006. India.