ELSEVIER Linear Algebra and its Applications 277 (1998) 57–61

LINEAR ALGEBRA AND ITS APPLICATIONS

Matrix characterization of MDS linear codes over modules

Xue-Dong Dong, Cheong Boon Soh *, Erry Gunawan

Block S2, School of Electrical and Electronic Engineering, Nanyang Technological University, Nanyang Avenue, Singapore 639798, Singapore

Received 23 June 1997; accepted 13 August 1997

Submitted by R. Brualdi

Abstract

Let R be a commutative ring with identity, N be an R-module, and $M = (a_{ij})_{r\times k}$ be a matrix over R. A linear code C of length n over N is defined to be a submodule of N^n. It is shown that a linear code $C(k,r)$ with parity check matrix $(-M|I_r)$ is maximum distance separable (MDS) iff the determinant of every $h\times h$ submatrix, $h = 1,2,\ldots,\min\{k,r\}$, of M is not an annihilator of any nonzero element of N. This characterization is used to derive some results for group codes over abelian groups. © 1998 Elsevier Science Inc. All rights reserved.

Keywords: Linear codes; MDS codes; Codes over rings; Group codes; Codes over modules

1. Introduction

Recently, Zain and Rajan [1] gave a good algebraic characterization of maximum distance separable (MDS) group codes over cyclic groups. They pointed out that the algebraic approach can be extended to the general case of group codes over abelian groups using the complex theory of determinants of matrices over noncommutative rings [1]. In this short paper, the matrix characterizations of MDS codes over finite fields and MDS group codes over cyclic groups are extended to linear codes with systematic parity check matrices over

[*] Corresponding author. E-mail: cbsoh@auto.eee.ntu.ac.sg.

0024-3795/98/$19.00 © 1998 Elsevier Science Inc. All rights reserved.
PII: S0024-3795(97)10073-8

modules. This characterization is then used to derive some results for group codes over abelian groups by using the simple theory of determinants of matrices over commutative rings.

2. A characterization of MDS linear codes

In the rest of the paper, let R be a commutative ring with identity, N be an R-module and $M = (a_{ij})_{r\times k}$ be a matrix over R. A linear code C of length n over N is defined to be a submodule of N^n. Linear codes over fields and group codes studied in [1] are all linear codes over modules. We denote by $C(k, r)$ the linear code of length $n = k + r$ with systematic parity check matrix $(-M|I_r)$. It is clear that the first k columns of a codeword of $C(k, r)$ are arbitrary information symbols and the last r columns are the parity symbols computed from the information columns.

Definition 2.1. An element x in a commutative ring R is called annihilator of an element $y \neq 0$ in R-module n if $xy = 0$. If $N = R$, then an annihilator is called zero divisor of R.

Example 2.1. Let $R = Z_m$, the ring of integers modulo m, and let N be a cyclic group with m elements. Then N is an R-module, and $C(k, r)$ is a group code [1]. An element n in Z_m is an annihilator of some nonzero element in N iff n is not relatively prime to m. This is equivalent to n not being a unit of Z_m.

Theorem 2.1. *$C(k,r)$ is MDS iff the determinant of every $h \times h$ submatrix, $h = 1, 2, \ldots, \min\{k, r\}$, of M is not an annihilator of any nonzero element in N.*

Proof. Suppose every $h \times h$ submatrix, $h = 1, 2, \ldots, \min\{k, r\}$, of M has determinant which is not an annihilator of any nonzero element in N. Let $a = (a_1, a_2, \ldots, a_{k+r})$ be a nonzero codeword. Assume that only h elements in $\{a_1, a_2, \ldots, a_k\}$ are nonzero, those with indices $j_1, j_2, \ldots, j_h$. Then it is clear

$$a_{k+t} = a_{tj_1}a_{j_1} + a_{tj_2}a_{j_2} + \cdots + a_{tj_h}a_{j_h},$$

where $t = 1, 2, \ldots, r$. Suppose h of these are zeros and their indices are $\{k + i_1, k + i_2, \ldots, k + i_h\}$. Then we have

$$0 = a_{k+t} = a_{tj_1}a_{j_1} + a_{tj_2}a_{j_2} + \cdots + a_{tj_h}a_{j_h},$$

where $t = i_1, \ldots, i_h$. Let

$$M_h = \begin{bmatrix} a_{i_1j_1} & a_{i_1j_2} & \cdots & a_{i_1j_h} \\ a_{i_2j_1} & a_{i_2j_2} & \cdots & a_{i_2j_h} \\ \vdots & \vdots & \ddots & \vdots \\ a_{i_hj_1} & a_{i_hj_2} & \cdots & a_{i_hj_h} \end{bmatrix}. \qquad (1)$$

Then we have

$$M_h^* M_h[a_{j_1}, a_{j_2}, \dots, a_{j_h}]^{\mathrm{T}} = [|M_h|a_{j_1}, |M_h|a_{j_2}, \dots, |M_h|a_{j_h}]^{\mathrm{T}} = 0,$$

where M_h^* is the adjoint matrix of M_h and $|M_h|$ is the determinant of M_h. It follows that $|M_h|a_{j_i} = 0, i = 1, \dots, h$. As $|M_h|$ is not an annihilator of any nonzero element in N, we have $a_{j_i} = 0, i = 1, \dots, h$, which is a contradiction. Hence in $\{a_{k+1}, a_{k+2}, \dots, a_{k+r}\}$ at most $h - 1$ elements are zeros and the weight of a is at least $h + [r - (h - 1)] = r + 1$, i.e., $C(k, r)$ is MDS.

Conversely, let $C(k, r)$ be MDS and let (1) be any submatrix of M, where $h \leqslant \min\{k, r\}$. If $|M_h|$ is an annihilator of some nonzero element in N, then from [2], I.G.1 Exercise, there are $a_{j_1}, a_{j_2}, \dots, a_{j_h}$ in N, which are not all zero, such that

$$M_h[a_{J_1}, a_{j_2}, \dots, a_{j_h}]^{\mathrm{T}} = 0.$$

Put $b_s = 0$ when $s \neq j_i$ and $b_{j_i} = a_{j_i}, i = 1, 2, \dots, h; s = 1, 2, \dots, k$. Let $[b_{k+1}, b_{k+2}, \dots, b_{k+r}]^{\mathrm{T}} = M[b_1, b_2, \dots, b_k]^{\mathrm{T}}$. Then $b_{k+i_1} = b_{k+i_2} = \cdots = b_{k+i_h} = 0$ and $(b_1, b_2, \dots, b_k, b_{k+1}, b_{k+2}, \dots, b_{k+r})$ is a codeword of $C(k, r)$ with weight $\leqslant h + (r - h) = r$, a contradiction. Thus $|M_h|$ is not an annihilator of any nonzero element N. □

Remark 2.1. Theorem 2.1. is a generalization of [3], ch. 11, Theorem 8, which is for codes over finite fields and [1], Theorem 2, which is for group codes over cyclic groups. When R is a finite field and $N = R$ these theorems coincide.

3. Some applications

In this section, let G be a finite abelian group. The r-fold sum $g + g + \cdots + g$ will be denoted by rg. Since the best group codes are over elementary abelian groups [4], we will focus on group codes over elementary abelian groups. Here by an elementary abelian group we mean that the exponent of the group is a prime p, i.e., if the order of every nonzero element is p. It is clear that an elementary abelian group with exponent p can be regarded as a Z_p-module, i.e., a vector space over Z_p.

Theorem 3.1. *Let $R = Z_p, N = G$, an elementary abelian group with exponent p. Then a group code $C(k, r)$ with parity check matrix $(-M|I_r)$ is MDS iff the determinant of every $h \times h$ submatrix, $h = 1, 2, \dots, \min\{k, r\}$, of M is not zero element of the field Z_p.*

Proof. It immediately follows from Theorem 2.1. □

Example 3.1. Let G be an elementary abelian group with exponent p, where p is an odd prime. Let

$$M = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}.$$

Then it is clear that the determinant of every square submatrix of M is not zero element of Z_p. By Theorem 3.1 the code $C(2,2)$ with parity check matrix $(-M|I_2)$ is a (4, 2, 3) MDS group code over G.

Example 3.2. Let G be an elementary abelian group with exponent 11. Let

$$M = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \\ 1 & 2^2 & 3^2 & 4^2 \end{bmatrix}$$

be a matrix over Z_{11}. It is easily verified that the determinant of every square submatrix of M is not zero element of Z_{11}. By Theorem 3.1 the code $C(4,3)$ with parity check matrix $(-M|I_3)$ is a (7, 4, 4) MDS group code over G.

Corollary 3.1. *Let G be an elementary abelian group with exponent p. Then*

1. Over G, $(1+r,1)$ MDS group codes exist for all values of r and p.

2. Over G, $(k+1,k)$ MDS group codes exist for all values of k and p.

Proof. Let $M = [(1,\ldots,1)^{\mathrm{T}}]_{r\times 1}$, where 1 is identity of Z_p. Then by Theorem 3.1, $C(1,r)$ with the parity check matrix $(-M|I_r)$ is a $(1+r,1)$ MDS group code.

Let $M = (1,\ldots,1)_{1\times k}$, where 1 is identity of Z_p. Then by Theorem 3.1, $C(k,1)$ with the parity check matrix $(-M|1)$ is a $(k+1,k)$ MDS group code. □

Corollary 3.2. *Let $R = Z_p$ and $N = G$, an elementary abelian group with exponent p, and let $M = (a_{ij})_{r\times k}$ be any matrix over Z_p. Then MDS group codes $C(k,r)$ with parity check matrix $(-M|I_r)$ do not exist if* $\max\{k,r\} \geqslant p$.

Proof. If there is an MDS group code $C(k,r)$ with parity check matrix $(-M|I_r)$, then by Theorem 3.1, the determinant of every $h\times h$ submatrix, $h = 1,2,\ldots,\min\{k,r\}$, of M is not zero element of the field Z_p. Let

$$M_1 = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ a_{11}^{-1}a_{21} & a_{12}^{-1}a_{22} & \cdots & a_{1k}^{-1}a_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ a_{11}^{-1}a_{r1} & a_{12}^{-1}a_{r2} & \cdots & a_{1k}^{-1}a_{rk} \end{bmatrix}.$$

Then the determinant of every square submatrix of M_1 is equal to a product of some unit of Z_p and the determinant of some square submatrix of M. It follows that the determinant of every square submatrix of M_1 is not zero element of Z_p. If $k \geqslant p$, then in $\{a_{11}^{-1}a_{21}, \ldots, a_{1k}^{-1}a_{rk}\}$, at least two elements are congruent modulo p. Assume $a_{1i}^{-1}a_{2i} = a_{ij}^{-1}a_{2j} (\bmod p)$. Then the determinant of the matrix

$$\begin{bmatrix} 1 & 1 \\ a_{1i}^{-1}a_{2i} & a_{ij}^{-1}a_{2j} \end{bmatrix}$$

is equal to $a_{1j}^{-1}a_{2j} - a_{1i}^{-1}a_{2i} = 0 \ (\bmod p)$. This is a contradiction. So we must have $k < p$. By similar arguments we can show $r < p$. Thus MDS group codes $C(k,r)$ with parity check matrix $(-M|I_r)$ do not exist if $\max\{k,r\} \geqslant p$. □

Remark 3.1. Although MDS group codes $C(k,r)$ with parity check matrix $(-M|I_r)$ do not exist if $\max\{k,r\} \geqslant p$, it is possible that there are MDS group codes $(k+r,r)$ without systematic parity check matrix $(-M|I_r)$ even if $\max\{k,r\} \geqslant p$. Zain and Rajan [1] gave a example of (4, 2, 3) MDS group code over the elementary abelian group $Z_2 \otimes Z_2$.

References

[1] A.A. Zain, B.S. Rajan, Algebraic characterization of MDS group codes over cyclic groups, IEEE Transactions on Information Theory 41 (1995) 2052–2056.

[2] B.R. McDonald, Linear Algebra over Commutative Rings, Marcel Dekker, New York, 1984.

[3] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, New York, 1977.

[4] G.D. Forney Jr., On the Hamming distance property of group codes, IEEE Transaction on Information Theory 38 (1992) 1797–1801.