Hokkaido Mathematical Journal Vol. 29 (2000) p. 149–157

Note on MDS codes over the integers modulo p^m

Keisuke SHIROMOTO

(Received January 22, 1999; Revised March 5, 1999)

Abstract. Recently, a number of papers have been published dealing with codes over finite rings. In this paper, we consider maximum distance separable (MDS) codes over the integers modulo p^m, where p is a prime number.

Key words: linear codes over rings, MDS code, module, Singleton bound, Hamming weight, generator matrix.

1. Introduction

In [4], Forney introduced a Singleton bound for codes over any finite alphabet A as follows;

$$d(C) \leq n - k + 1,$$

where C is a code of length n over A, $k = \log_{|A|} |C|$ and $d(C)$ is the minimum distance of C and proved several nonexistence results for MDS group codes over finite groups with respect to the above bound, that is, the group codes with $d(C) = n - k + 1$. Zain and Rajan [9] also proved that for a group code C over a cyclic group of m elements with generator matrix of the form $(I_k \mid M)$, where M is a $k \times (n-k)$ matrix over $\mathbb{Z}_m$, C is MDS iff the determinant of every $h \times h$ submatrix, $h = 1, 2, \ldots, \min\{n-k, k\}$, of M is a unit in $\mathbb{Z}_m$. Moreover, Dong, Soh and Gunawan [3] proved a similar matrix characterization of MDS (free) codes with parity check matrices of the form $(-M \mid I_{n-k})$ over modules.

Recently, Shiromoto and Yoshida [8] introduced a Singleton bound for linear codes over $\mathbb{Z}_k$ as follows:

Proposition 1 (Shiromoto and Yoshida [8]) *Let C be a linear code of length n over $\mathbb{Z}_k$ with the minimum weight $d(C)$. Then,*

$$d(C) \leq n - \operatorname{rank}(C) + 1.$$

In the next section, we shall introduce some definitions and notations

1991 Mathematics Subject Classification : 94B05, 94B60, 94B65.

for this bound. If the integer k is a prime number, then the above bound coincides with the Singleton bound for linear codes over a finite field ([6]) and if C is a free $\mathbb{Z}_k$-submodule, then the above bound coincides with the Singleton bound for codes over a finite alphabet ([4]).

In this paper, we study MDS (not necessary free) codes over $\mathbb{Z}_{p^m}$ with respect to the Singleton bound given in Proposition 1, i.e., the linear codes with $d(C) = n - \mathrm{rank}(C) + 1$. The following result is a main theorem of this paper.

Theorem 1 *Let C be a linear code of length n over $\mathbb{Z}_{p^m}$. If C is an MDS code, then the dual code $C^\perp$ is a freely MDS code.*

Using this theorem, we have an information on the weight distributions of the codes and give a characterization of generator matrices for the codes (Theorem 2 and Theorem 3 in Section 3).

2. Linear codes over $\mathbb{Z}_k$

Let $\mathbb{Z}_k = \{0, 1, 2, \ldots, k-1\}$ be the residue ring of k-elements and let $(\mathbb{Z}_k)^n$ be the free module of rank n consisting of all n-tuples of elements of $\mathbb{Z}_k$. A *linear code* C of length n over $\mathbb{Z}_k$ is a $\mathbb{Z}_k$-submodule of $V := (\mathbb{Z}_k)^n$. In particular, if C is a $\mathbb{Z}_k$-free submodule of V, we call that C is a *free code* over $\mathbb{Z}_k$. An element of C is called a *codeword* of C. For $N := \{1, 2, \ldots, n\}$, the (Hamming) *support* and the (Hamming) *weight* of $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in V$, denoted by $\mathrm{supp}(\mathbf{x})$ and $\mathrm{wt}(\mathbf{x})$, are respectively defined as follows:

$$\begin{aligned} \mathrm{supp}(\mathbf{x}) &:= \{i \in N \mid x_i \neq 0\}, \\ \mathrm{wt}(\mathbf{x}) &:= |\mathrm{supp}(\mathbf{x})| = |\{i \in N \mid x_i \neq 0\}|. \end{aligned}$$

The *minimum* (Hamming) *weight* $d(C)$ of C is defined by

$$d(C) := \min\{\mathrm{wt}(\mathbf{x}) \mid (\mathbf{0} \neq)\ \mathbf{x} \in C\}.$$

For linear codes D_1 and D_2 such that $D_1 \subseteq D_2$, we note that

$$d(D_2) \leq d(D_1). \tag{1}$$

Let C be a linear code over $\mathbb{Z}_k$. Then by the fundamental theorem of finitely generated abelian groups, C is isomorphic to

$$\mathbb{Z}_k/f_1\mathbb{Z}_k \oplus \mathbb{Z}_k/f_2\mathbb{Z}_k \oplus \cdots \oplus \mathbb{Z}_k/f_n\mathbb{Z}_k, \tag{2}$$

where $f_1, f_2, \ldots, f_n$ are positive integers such that $f_1|f_2|\cdots|f_n|k$. Moreover, the *type* $(f_1, f_2, \ldots, f_n)$ is uniquely decided by C up to the f_i's such that $f_i = 1$. We note that $|C| = f_1 \cdot f_2 \cdots f_n$. For a subset $\{\mathbf{g}_1, \mathbf{g}_2, \ldots, \mathbf{g}_m\} \subseteq C$, $\mathbf{g}_i$, $i = 1, 2, \ldots, m$ are called *generators* of C if $C = \sum_{i=1}^{m} \mathbb{Z}_k \mathbf{g}_i$. The *rank* of C, denoted by $\mathrm{rank}(C)$, is the minimum number of generators of C and the *free rank* of C, denoted by f-rank(C), is the maximum of the ranks of $\mathbb{Z}_k$-free submodules of C, that is,

$$\begin{aligned}\mathrm{rank}(C) &= |\{i \mid f_i \neq 1\}|,\\ \text{f-rank}(C) &= |\{i \mid f_i = k\}|.\end{aligned}$$

Let C_f be a $\mathbb{Z}_k$-free submodule of C such that $\mathrm{rank}(C_f) = \text{f-rank}(C)$ and let C_F be a $\mathbb{Z}_k$-free submodule of V such that $C \subseteq C_F$ and $\mathrm{rank}(C_F) = \mathrm{rank}(C)$. We note that

$$|C_f| = k^{\text{f-rank}(C_f)}, \quad |C_F| = k^{\mathrm{rank}(C)}.$$

If $d(C_f) = n - \mathrm{rank}(C_f) + 1$, then we will say that C is a *freely MDS code*.

Furthermore, the inner product of vectors $\mathbf{x} = (x_1, \ldots, x_n)$, $\mathbf{y} = (y_1, \ldots, y_n) \in (\mathbb{Z}_k)^n$ is defined by

$$\langle \mathbf{x}, \mathbf{y} \rangle = x_1 y_1 + \cdots + x_n y_n \pmod{k}.$$

The *dual code* of C is defined by

$$C^{\perp} := \{\mathbf{y} \in (\mathbb{Z}_k)^n \mid \langle \mathbf{x}, \mathbf{y} \rangle = 0 \quad (\forall \mathbf{x} \in C)\}.$$

If C has type $(f_1, f_2, \ldots, f_n)$, then the type of $C^{\perp}$ is $(k/f_n, \ldots, k/f_2, k/f_1)$. We also note that

$$\mathrm{rank}(C) + \text{f-rank}(C^{\perp}) = n.$$

The (Hamming) *weight enumerator* $W_C(z)$ of a linear code C is defined by

$$W_C(z) = \sum_{i=0}^{n} A_C(i) z^i,$$

where $A_C(i) = |\{\mathbf{x} \in C \mid \mathrm{wt}(\mathbf{x}) = i\}|$. For linear codes D_1 and D_2 such that $D_1 \subseteq D_2$, we note that

$$A_{D_1}(i) \leq A_{D_2}(i), \quad i = 0, 1, \ldots, n. \tag{3}$$

The following equation is well-known as a Mac Williams identity over $\mathbb{Z}_k$.

Proposition 2 (Klemm [5]) *For a linear code C of length n over $\mathbb{Z}_k$,*

$$W_{C}^{\perp}(z) = \frac{(1+(k-1)z)^n}{|C|} W_C\left(\frac{1-z}{1+(k-1)z}\right).$$

For a subset $M \subseteq N := \{1, 2, \dots, n\}$ and a $\mathbb{Z}_k$-submodule $D \subseteq V$, we define

$$\begin{aligned} D(M) &:= \{\mathbf{x} \in V \mid \mathrm{supp}(\mathbf{x}) \subseteq M\}, \\ D^* &:= \mathrm{Hom}_{\mathbb{Z}_k}(D, \mathbb{Z}_k). \end{aligned}$$

Clearly $D(M) = D \cap V(M)$ is also a submodule of V. From (2),

$$\begin{aligned} D^* &= \mathrm{Hom}_{\mathbb{Z}_k}(D, \mathbb{Z}_k) \\ &\cong \mathrm{Hom}_{\mathbb{Z}_k}(\oplus_i \mathbb{Z}_k/f_i\mathbb{Z}_k, \mathbb{Z}_k) \\ &\cong \oplus_i \mathrm{Hom}_{\mathbb{Z}_k}(\mathbb{Z}_k/f_i\mathbb{Z}_k, \mathbb{Z}_k) \\ &\cong \oplus_i \mathbb{Z}_k/f_i\mathbb{Z}_k. \end{aligned}$$

So we note that there exists a (non-natural) isomorphism:

$$D^* \cong D.$$

Then the following proposition is essential.

Proposition 3 (Shiromoto and Yoshida [8]) *Let D be a $\mathbb{Z}_k$-submodule of $V := (\mathbb{Z}_k)^n$ and $M \subseteq N := \{1, 2, \dots, n\}$. Then there is the following exact sequence as $\mathbb{Z}_k$-modules*:

$$0 \longrightarrow D(N-M) \xrightarrow{\mathrm{inc}} V(N-M) \xrightarrow{f} (D^{\perp})^* \xrightarrow{\mathrm{res}} D^{\perp}(M)^* \longrightarrow 0,$$

where the maps inc, res *denote the inclusion map, the restriction map, respectively, and the map f is defined by*

$$f : \mathbf{y} \longmapsto (\hat{\mathbf{y}} : \mathbf{x} \mapsto \langle \mathbf{x}, \mathbf{y} \rangle).$$

3. Main results

In this section, we only consider linear codes over $\mathbb{Z}_{p^m}$, where p is a prime number. For any $\mathbb{Z}_{p^m}$-submodule D of $V := (\mathbb{Z}_{p^m})^n$, we define

$$S(D) := \{\mathbf{x} \in D \mid p\mathbf{x} = \mathbf{0}\},$$

where $\mathbf{0} = (0, 0, \ldots, 0)$ $(\in V)$. Since there exists an element $\mathbf{x} \in S(D)$ such that $\mathrm{wt}(\mathbf{x}) = d(D)$, we note that

$$d(S(D)) = d(D). \tag{4}$$

Lemma 1 *If C is a linear code of length n over $\mathbb{Z}_{p^m}$, then*

$$d(C_F) = d(C).$$

Proof. We can assume that C has a generator matrix of the form

$$G = \begin{bmatrix} G_0 \\ pG_1 \\ \vdots \\ p^{m-1}G_{m-1} \end{bmatrix},$$

where the number of row vectors of G is equal to $\mathrm{rank}(C)$ (cf. [1]). Let C_F^0 be the linear code with generator matrix $G' = \begin{bmatrix} G_0 \\ \vdots \\ G_{m-1} \end{bmatrix}$. Since

$$S(C) = p^{m-1}C_F^0 := \{\mathbf{x} \in C_F^0 \mid p\mathbf{x} = \mathbf{0}\}$$

and $p^{m-1}C_F = p^{m-1}C_F^0$, we have

$$p^{m-1}C_F \subseteq C \subseteq C_F.$$

From (1) and (4), $d(C_F) \leq d(C) \leq d(p^{m-1}C_F) = d(C_F)$. □

Remark 1 Lemma 1 suggests that though we can take C_F in the various way for C, $d(C_F)$ is uniquely decided by $d(C)$ for all C_F.

Using Proposition 3, we can prove Proposition 1 (see [8]) and Theorem 1.

Proof of Theorem 1. We put $D := (C^\perp)_f$. Since $D^\perp(\supseteq C)$ is a $\mathbb{Z}_{p^m}$-free submodule of V and $\mathrm{rank}(D^\perp) = n - \mathrm{rank}(D) = \mathrm{rank}(C)$, then $D^\perp = C_F$. Take an arbitrary subset $M \subseteq N$ such that $|M| = d(C)-1$, then $D^\perp(M)^* = 0$ from Lemma 1. By Proposition 3,

$$0 \longrightarrow D(N-M) \xrightarrow{\mathrm{inc}} V(N-M) \xrightarrow{f} (D^\perp)^* \longrightarrow 0.$$

Because of $(D^{\perp})^* \cong D^{\perp}$, we have the following relation:

$$V(N-M) \cong D(N-M) \oplus D^{\perp}.$$

Thus

$$\begin{aligned}(\mathrm{rank}(C) =)\ \mathrm{rank}(D^{\perp}) &\le \mathrm{rank}(V(N-M)) \\ &\qquad (\ = |N-M| = n - d(C) + 1).\end{aligned}$$

(We note that this inequality coincides with the Singleton bound for Proposition 1.) We assume that C is an MDS code, that is, $d(C) = n - \mathrm{rank}(C) + 1$. Since we note that $D(N-M) = \{\mathbf{0}\}$ for any M, so

$$\begin{aligned}|N-M| &\le d(D) - 1 \\ &\le n - \mathrm{rank}(D) \\ &= \mathrm{rank}(C) = |N-M|.\end{aligned}$$

Thus we have the following equation:

$$d(D) - 1 = n - \mathrm{rank}(D).$$

Hence the theorem follows. □

Using Theorem 1, in the case that C is a free code, we have the following corollary (a similar result for group codes over cyclic groups can be found in [9]).

Corollary 1 *Let C be a free code of length n over $\mathbb{Z}_{p^m}$. If C is an MDS code, then $C^{\perp}$ is also an MDS code.*

Remark 2 Theorem 1 also claims that though we can take $(C^{\perp})_f$ in the various way, if C is an MDS code, then $d((C^{\perp})_f)$ is uniquely decided by $d(C)$ for all $(C^{\perp})_f$.

We have an information on the number $A_C(i)$ for any MDS code C. We remark that a similar result for linear codes over finite fields is found in [6] and [7].

Theorem 2 *Let C be a linear code of length n and of* rank r *over $\mathbb{Z}_{p^m}$. If C is MDS, then*

$$A_C(i) \le \binom{n}{i} \sum_{j=0}^{i-d(C)} (-1)^j \binom{i}{j} (p^{m(i-d(C)+1-j)} - 1).$$

Proof. We put $D := (C^{\perp})_f$. By Theorem 1, both D and $D^{\perp}(\supseteq C)$ are MDS (free) codes. Since $|D| = (p^m)^{\text{f-rank}(C^{\perp})} = p^{m(n-r)}$, the equation of Proposition 2 can be written in the form

$$\sum_{i=0}^{n} A_{D^{\perp}}(i)z^i = \frac{1}{p^{m(n-r)}}\sum_{i=0}^{n} A_D(i)(1-z)^i(1+(p^m-1)z)^{n-i}.$$

Replacing z by z^{-1} and then multiplying by z^n in the above equation, we have

$$\sum_{i=0}^{n} A_{D^{\perp}}(i)z^{n-i} = \frac{1}{p^{m(n-r)}}\sum_{i=0}^{n} A_D(i)(z-1)^i(z+p^m-1)^{n-i}.$$

Differentiating this equation s times and substituting $z=1$, we have

$$\frac{1}{p^{mr}}\sum_{i=0}^{n-s}\binom{n-i}{s}A_{D^{\perp}}(i) = \frac{1}{p^{ms}}\sum_{i=0}^{s}\binom{n-i}{n-s}A_D(i).$$

We use the facts that $A_{D^{\perp}}(0)=1$, $A_{D^{\perp}}(i)=0$ for $i=1,\ldots,n-r$, and $A_D(0)=1$, $A_D(i)=0$ for $i=1,\ldots,r$. Then, for $s \le r$,

$$\sum_{i=n-r+1}^{n-s}\binom{n-i}{s}A_{D^{\perp}}(i) = \binom{n}{s}(p^{m(r-s)}-1), \quad s=0,1,\ldots,r-1.$$

From (3), we note that $A_C(i) \le A_{D^{\perp}}(i)$, $i=n-r+1,\ldots,n$. Hence, the theorem follows. □

Remark 3 We remark that if C is a free code, then the equality holds in Theorem 2.

Moreover, we give the matrix characterization of MDS codes over $\mathbb{Z}_{p^m}$, similar results are found in [3] and [9]. A nonzero linear code C over $\mathbb{Z}_{p^m}$ has a generator matrix which after a suitable permutation of the coordinates can be written in the form

$$G = \begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} & A_{0,3} & \cdots & \cdots & A_{0,m} \\ 0 & pI_{k_1} & pA_{1,2} & pA_{1,3} & \cdots & \cdots & pA_{1,m} \\ 0 & 0 & p^2I_{k_2} & p^2A_{2,3} & \cdots & \cdots & p^2A_{2,m} \\ \vdots & \vdots & 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & p^{m-1}I_{k_{m-1}} & p^{m-1}A_{m-1,m} \end{pmatrix}, \qquad (5)$$

where I_{k_i} denotes the $k_i \times k_i$ identity matrix for any i (cf. [2]). In this case, we remark that

$$\begin{aligned} k_0 + k_1 + k_2 + \cdots + k_{m-1} &= \mathrm{rank}(C), \\ k_0 &= \text{f-rank}(C). \end{aligned}$$

For a linear code C with generator matrix G of the form (5), let

$$G' := \begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} & A_{0,3} & \cdots & \cdots & A_{0,m} \\ 0 & I_{k_1} & A_{1,2} & A_{1,3} & \cdots & \cdots & A_{1,m} \\ 0 & 0 & I_{k_2} & A_{2,3} & \cdots & \cdots & A_{2,m} \\ \vdots & \vdots & 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & I_{k_{m-1}} & A_{m-1,m} \end{pmatrix}.$$

Then G' can be modified to the form $G'' := (I_r \mid M)$ by the elementary row transformation, where $r = \mathrm{rank}(C)$. Since $\mathbb{Z}_{p^m}$ is a $\mathbb{Z}_{p^m}$-module, we have the following lemma from Theorem 2.1 in [3].

Lemma 2 *Let D be a free code of length n and $\mathrm{rank}(D) = r$ over $\mathbb{Z}_{p^m}$ with parity check matrix of the form $(-M \mid I_{n-r})$. Then D is MDS iff the determinant of every $h \times h$ submatrix $h = 1, 2, \ldots, \min\{n-r, r\}$, of the matrix M is a unit in $\mathbb{Z}_{p^m}$.*

Using the above lemma, we get the matrix characterization of MDS codes over $\mathbb{Z}_{p^m}$.

Theorem 3 *Let C be a linear code of length n and $\mathrm{rank}(C) = r$ over $\mathbb{Z}_{p^m}$ with generator matrix G of the form (5). Then C is MDS iff the determinant of every $h \times h$ submatrix $h = 1, 2, \ldots, \min\{n-r, r\}$, of the matrix M of $G'' = (I_r \mid M)$ is a unit in $\mathbb{Z}_{p^m}$.*

Proof. Let D be the linear code with generator matrix G''. From Lemma 1, we note D is a free code of $\mathrm{rank}(D) = r$ and $d(D) = d(C)$. So C is MDS iff D is MDS. Furthermore, D has a parity check matrix $(-M^T \mid I_{n-r})$. Hence the theorem follows from Lemma 2. □

Acknowledgment The author would like to thank the referee for a careful reading. The author would like to thank adviser Professor. Tomoyuki Yoshida for his helpful suggestions and Hiroshi Horimoto for his helpful discussions and comments.

References

[1] Ashikhmin A., *On generalized Hamming weights for Galois rings linear codes.* Designs, Codes and Cryptography, **14** (1998), 107–126.

[2] Calderbank A.R. and Sloane N.J.A., *Modular and p-adic cyclic codes.* Designs, Codes and Cryptography, **6** (1995), 21–35.

[3] Dong X.D., Soh C.B. and Gunawan E., *Matrix characterization of MDS linear codes over modules.* Linear Algebra and Its Applications, **227** (1998), 57–61.

[4] Forney G.D., *On the Hamming distance properties of group codes.* IEEE Trans. Inform. Theory, **38** (1992), 1797–1801.

[5] Klemm M., *Über die identität von MacWilliams für die gewichtsfunktion von codes.* Arch. Math. **49** (1987), 400–406.

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

[7] Roman S., *Coding and Information Theory.* Springer-Verlag, Berlin-New York, GTM 134, 1992.

[8] Shiromoto K. and Yoshida T., *A Singleton bound for linear codes over $\mathbb{Z}/l\mathbb{Z}$.* (submitted).

[9] Zain A.A. and Rajan B.S., *Algebraic characterization of MDS group codes over cyclic groups.* IEEE Trans. Inform. Theory, **41** (1995), 2052–2056.

Department of Mathematics
Kumamoto University
2-39-1, Kurokami, Kumamoto 860-8555
Japan
E-mail: keisuke@math.sci.kumamoto-u.ac.jp