Kumamoto J. Math.
Vol. 14, 21-29 March (2001)



# A Singleton bound for linear codes over $Z/lZ$

Keisuke Shiromoto* and Tomoyuki Yoshida

(Received September 20, 2000
Revised February 26, 2001)

**Abstract**

Recently, there are many works on codes over finite rings (cf. [ConSl 93], [Shi 98], etc.). In this paper, we consider a Singleton bound for codes over $Z_l$. Let $C$ be a linear code of length $n$ with minimum distance $d(C)$ over $Z_l$. We have a Singleton bound as follows: $d(C) \leq n - \mathrm{rank}(C) + 1$.

## 1. Introduction

The Singleton bound is the simplest bound for linear codes over finite fields. Thus we are interested in such a kind of Singleton bound for linear codes over a finite (non-commutative) rings, for example, the residue rings $Z_4 = Z/4Z$, $Z_l$, a finite matrix ring $M_m(F_q)$, a finite group algebra $F_qG$, and so on. In this paper, we show a Singleton bound for linear codes over a residue ring $Z/lZ$, where $l$ is an integer greater than 2.

**Theorem** For a linear code $C$ of length $n$ with minimum distance $d(C)$ over $Z_l$,

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

In particular, this theorem gives the ordinary Singleton bound for linear codes over finite fields. This theorem is proved by the $Z_l$-version of an exact sequence (Proposition 1 in Section 3).

## 2. $Z_l$-modules

In this section, we shall summarize the properties of finitely generated $Z_l$-modules which we need later. The proofs are all omitted because all statements are well-known or are easily proved from others.

**(A)** A $Z_l$-module can be identified with an abelian group of exponent divisible by $l$; in particular, an indecomposable $Z_l$-module has the form $Z_l/fZ_l \cong Z/fZ$ for a positive integer $f$

*Research Fellow of the Japan Sociery for the Promorion of Science.

divisible by $l$. We have some fundamental results on the structure of $Z_l$-modules following directly from the fundamental theorem of finitely generated abelian groups.

( i ) If $V$ is a free $Z_l$-module of rank $n$ and $C$ is its submodule, then there exists a basis $\{v_1, v_2, \ldots, v_n\}$ and integers $1 \leq e_1 | e_2 | \ldots | e_r < l$ such that $\{e_1 v_1, e_2 v_2, \ldots, e_r v_r\}$ is a basis of $C$. In this case, we have

$$V/C \cong \bigoplus_{i=1}^{r} Z/e_i Z \oplus (Z/lZ)^{n-r},$$

$$C \cong \bigoplus_{i=1}^{r} Z/(l/e_i)Z.$$

( ii ) Any finitely generated $Z_l$-module $M$ is isomorphic to

$$Z_l/f_1 Z_l \oplus Z_l/f_2 Z_l \oplus \cdots \oplus Z_l/f_n Z_l, \tag{1}$$

where $f_1, \ldots, f_n$ are positive integers such that

$$f_1 | f_2 | \cdots | f_n | l.$$

Furthermore, the *type* $(f_1, f_2, \ldots, f_n)$ is uniquely decided by $M$ up to the $f_i$'s such that $f_i = 1$.

**(B)** Let $M$ be a finitely generated $Z_l$-module.

( i ) The *rank* of $M$, denoted by rank$(M)$, is the minimum number of generators of $M$ ; the *free rank* f-rank$(M)$ denotes the maximum of the ranks of $Z_l$-free submodules of $M$. If the invariant of $M$ is $(f_1, \ldots, f_n)$, then

$$\text{rank}(M) = \#\{i \mid f_i \neq 1\},$$
$$\text{f-rank}(M) = \#\{i \mid f_i = l\}.$$
$$|M| = f_1 \cdot f_2 \cdots f_n.$$

( ii ) For a prime $p$, the *p-rank* rank$_p(M)$ of the $Z_l$-module $M$ is the rank of the $p$-torsion part $M_p$ of $M$. Thus if $f_1 | f_2 | \cdots | f_n$ is the type of $M$, then

$$\text{rank}_p(M) = \#\{i \mid f_i \equiv 0 \pmod p\}.$$

**(C)** We denote by $\text{Tor}_m^{Z_l}(A, B)$ the group of $m$-th torsions ([Wi 94]). ( i ) Since

$$\cdots \xrightarrow{f} Z_l \xrightarrow{l/f} Z_l \xrightarrow{f} Z_l \xrightarrow{\text{pr}} Z_f \longrightarrow 0$$

is a projective resolution of the $Z_l$-module $Z_f = Z_l/fZ_l$, where $f$ is a divisor of $l$, we have the following :

$$\mathrm{Tor}_m^{Z_l}(Z_f, B)=\begin{cases} B/fB & (m=0) \\ {}_fB/(l/f)B & (m=\text{odd}>0), \\ {}_{l/f}B/fB & (m=\text{even}>0 \end{cases} \tag{2}$$

where ${}_fB:=\{x\in B\,|\,fx=0\}$.

(ii) If $B$ is finitely generated, then

$$\frac{|\mathrm{Tor}_0^{Z_l}(Z_f, B)|}{|\mathrm{Tor}_1^{Z_l}(Z_f, B)|}=|(l/f)B|, \tag{3}$$

$$|\mathrm{Tor}_{m+1}^{Z_l}(Z_f, B)|=|\mathrm{Tor}_m^{Z_l}(Z_f, B)| \quad (m\geq 1). \tag{4}$$

(iii) Let $p^r$ be the largest power of $p$ dividing $l$ and $B$ a finitely generated $Z_l$-module with $p$-torsion part $B_p$ isomorphic to

$$B\cong \bigoplus_i Z/p^{\lambda_i}Z\cong \bigoplus_{j=1}^{r} (Z/p^jZ)^{\mu_j},$$

where $\mu_j$ is the number of $i$'s such that $\lambda_i=j$. Then we have

$$\log_p\left(\frac{|\mathrm{Tor}_0^{Z_l}(Z/p^sZ, B)|}{|\mathrm{Tor}_1^{Z_l}(Z/p^sZ, B)|}\right)=\sum_{\lambda_i>r-s}(\lambda_i-r+s)=\sum_{j=1}^{s} j\mu_{j+r-s} \tag{5}$$

**(D)** For any $Z_l$-module $M$, we have the dual $Z_l$-module $M^*$ by

$$M^*:=\mathrm{Hom}_{Z_l}(M, Z_l)$$

with $Z_l$-action defined by $a\lambda: m\mapsto a\lambda(m)$ for all $a\in Z_l$, $\lambda\in M^*$. The dual module $M^*$ is isomorphic to the character group of $M$ as a group. Each $Z_l$-homomorphism $f: M\to N$ induces a $Z_l$-homomorphism

$$f^*: N^*\to M^*;\ \mu\mapsto \mu\circ f,$$

and so we have a duality functor $*=\mathrm{Hom}_{Z_l}(-, Z_l)$ on $Z_l$-modules.

(i) Note that if $M$ is finitely generated, then there exists a (non-natural) isomorphism:

$$M^*\cong M. \tag{6}$$

(ii) The functor $*$ is an exact contravariant functor, and so if

$$0\longrightarrow L\xrightarrow{f} M\xrightarrow{g} N\longrightarrow 0$$

is an exact sequence of $Z_l$-modules, then

$$0 \longrightarrow N^* \xrightarrow{g^*} M^* \xrightarrow{f^*} L^* \longrightarrow 0 \tag{7}$$

is also an exact sequence.

**(E)** Suppose the free module $V:=(\boldsymbol{Z}_l)^n$ is equipped with a non-degenerate symmetric inner product $\langle\, , \rangle$. For a submodule $C$ of $V$, let $C^\perp$ be the orthogonal complement of $M$:

$$C^\perp:=\{v\in V \mid \langle u, v\rangle=0 \quad \text{for all } u\in C\}$$

Then there is a $\boldsymbol{Z}_l$-homomorphism

$$\wedge: V\to C^* \tag{8}$$

$$; v\mapsto(\hat{v}: u\mapsto\langle u, v\rangle).$$

(i) The map $\wedge$ is surjective and induces an isomorphism:

$$V/C^\perp\cong C^*. \tag{9}$$

In particular, when $C=V$, the map $\wedge: V\to V^*$ is an isomorphism.

(ii) For any submodule $C$, $D$ of $V$,

$$C^{\perp\perp}=C, (C+D)^\perp=C^\perp\cap D^\perp, (C\cap D)^\perp=C^\perp+D^\perp. \tag{10}$$

(iii) Let $C$ be a submodule of $V$ of type $(f_1, \ldots, f_n)$. Then type of $C^\perp$ is $(l/f_n, \ldots, l/f_2, l/f_1)$. In particular,

$$\text{rank}(C)+\text{f-rank}(C^\perp)=n. \tag{11}$$

## 3. Linear codes over $\boldsymbol{Z}_l$.

In this section we prove "the basic exact sequence" for linear codes over the ring $\boldsymbol{Z}_l$. Let $V:=(\boldsymbol{Z}_l)^n$ be the free $\boldsymbol{Z}_l$-module of rank $n$, and let $N:=\{1, 2, \ldots, n\}$. Then the (Hamming) *support* supp$(v)$, the (Hamming) *weight* wt$(v)$, the (Hamming) *distance* $d(u, v)$ for $u=(u_1, \cdots, u_n)$, $v=(v_1, \cdots, v_n)\in V$ are, respectively, defined as follows:

$$\begin{aligned}\text{supp}(v)&:=\{i\in N \mid v_i\neq 0\},\\ \text{wt}(v)&:=|\text{supp}(v)|=\#\{i\in N \mid v_i\neq 0\},\\ d(u, v)&:=\text{wt}(u-v)=\#\{i\in N \mid u_i\neq v_i\}.\end{aligned}$$

Furthermore, the inner product of vectors $u=(u_1, \cdots, u_n)$, $v=(v_1, \cdots, v_n)\in V$ is, as usual, defined by

$$\langle u, v\rangle := \sum_{i\in N} u_i v_i \pmod{l}.$$

A *linear code* $C$ over $Z_l$ is a $Z_l$-submodule of $V=(Z_l)^n$; the integer $n$ is called *length* of $C$. The *minimum* (Hamming) *distance* $d(C)$ of $C$ is defined by

$$d(C) := \mathrm{Min}\{\mathrm{wt}(u) \mid 0 \neq u \in C\}.$$

A *generator matrix* of $C$ is an $r\times n$ matrix over $Z_l$ whose row vectors are minimal generators of $C$, where $r=\mathrm{rank}(C)$. The *dual code* $C^\perp$ is the orthogonal complement to $C$ with respect the above inner product:

$$C^\perp := \{v\in V \mid \langle u, v\rangle = 0 \quad \text{for all } u\in C\}.$$

Then we have

$$C^* \cong V/C^\perp.$$

Let $C\subseteq V := Z_l^n$ be a linear code over $Z_l$. For a subset $M$ of $N=\{1, 2, ..., n\}$, we define

$$V(M) := \{v\in V \mid \mathrm{supp}(v)\subseteq M\}.$$
$$C(M) := C\cap V(M) = \{u\in C \mid \mathrm{supp}(u)\subseteq M\}.$$

Then $V(M)$ and $C(M)$ are submodules of $V$; in fact, for any $v, v'\in V(M)$, we have that if $(v+v')_i\neq 0$, then $v_i\neq 0$ or $v'_i\neq 0$, and so $i\in M$, that is, $\mathrm{supp}(v+v')\subseteq M$. The map cut : $C\to V(M)$ is defined by

$$\mathrm{cut} : (u_i)_{i\in N} \mapsto (u_i)_{i\in M}.$$

**Proposition 1 (the basic exact sequences)** *For a linear code $C\subseteq V=(Z_l)^n$ and a subset $M\subseteq N=\{1, 2, ..., n\}$, the following sequences are exact:*

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

$$0 \longrightarrow C^\perp(N-M) \xrightarrow{\mathrm{inc}} C^\perp \xrightarrow{\mathrm{cut}} V(M) \xrightarrow{\wedge} C(M)^* \longrightarrow 0.$$

**Proof.** Interchanging $C$ with $C^\perp$ and applying the duality functor $* = \mathrm{Hom}_{Z_l}(-, Z_l)$, the exactness of the second sequence follows from the one of the fist one. The proof of the exactness of the first sequence is similar to the one of binary case. (1) The map inc is clearly injective. (2) If $v\in C^\perp(M)$, then $\hat{v}(u)=\langle v, u\rangle=0$ for all $u\in C$, that is, $\hat{v}=0$, and so $v\in \mathrm{Ker}(\wedge)$. Conversely, if $v\in\mathrm{Ker}(\wedge)$, then $\langle v, u\rangle=0$ for all $u\in C$, and so $v\in C^\perp\cap V(M)= C^\perp(M)$, proving the exactness at $V(M)$. (3) If $v\in V(M)$, then $\hat{v}(u)=\langle v, u\rangle=0$ for all $u\in C(N$

$-M$), and so $\hat{v}\in\mathrm{Ker}(\mathrm{res})$. Conversely, let $\lambda\in\mathrm{Ker}(\mathrm{res})$. Since $\wedge: V\to C^*$ is surjective, there exists $v\in V$ such that $\lambda=\hat{v}$. Then $\langle v, u\rangle=0$ for all $u\in C(N-M)$, and so

$$v\in C(N-M)^{\perp}=(C\cap V(N-M))^{\perp}=C^{\perp}+V(N-M)^{\perp}$$
$$=C^{\perp}+V(M),$$

and so $v=v_1+v_2$ for some $v_1\in C^{\perp}$ and $v_2\in V(M)$. Since $\hat{v}_1=0$ on $C$, we have

$$\lambda=\hat{v}=\hat{v}_2\in\mathrm{Im}(\wedge).$$

(4) Finally, the map res is surjective by the exactness of the duality functor $*=\mathrm{Hom}(-, \boldsymbol{Z}_l)$. The proposition is proved. □

## 4. A Singleton bound.

**Theorem 2** *For a linear code $C$ over $\boldsymbol{Z}_l$ of length $n$ with minimum distance $d(C)$,*

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

**Proof.** Take an arbitrary subset $M$ of $N=\{1, 2, \ldots, n\}$ such that

$$|M|=d(C)-1,$$

so that $C(M)^*=0$. Thus the second exact sequence of Proposition 1 implies the following short exact sequence:

$$0\longrightarrow C^{\perp}(N-M)\longrightarrow C^{\perp}\longrightarrow V(M)\longrightarrow 0.$$

Since $V(M)\cong(\boldsymbol{Z}_l)^{|M|}$ is a projective module, this short exact sequence is split, that is,

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

Thus

$$\text{f-rank}(C^{\perp})\geq\text{f-rank}(V(M))=|M|=d(C)-1.$$

Hence the theorem follows from the formula $\text{f-rank}(C^{\perp})+\mathrm{rank}(C)=n$. □

Here are some examples of linear codes over $\boldsymbol{Z}_l$ meeting the Singleton bound (Theorem 2), that is, MDS codes over $\boldsymbol{Z}_l$ with respect to the bound. So the bound is the best.

**Example 1.** Let $C$ be the linear code over $\boldsymbol{Z}_{14}$ with the generator matrix

$$G=\begin{pmatrix} 1 & 7 & 7 & 1 & 3 & 13 & 3 & 11 \\ 0 & 8 & 0 & 4 & 6 & 6 & 4 & 6 \\ 0 & 0 & 8 & 10 & 6 & 10 & 8 & 4 \end{pmatrix}.$$

Then $n=8$, $\mathrm{rank}(C)=3$ and $d(C)=6$.

**Example 2.** Let $C$ be the linear code over $Z_{22}$ with the generator matrix

$$G=\begin{pmatrix} 1 & 11 & 11 & 1 & 3 & 17 & 21 & 15 & 17 \\ 0 & 12 & 0 & 8 & 14 & 18 & 20 & 20 & 10 \\ 0 & 0 & 12 & 14 & 6 & 10 & 4 & 10 & 6 \end{pmatrix}.$$

Then $n=9$, $\mathrm{rank}(C)=3$ and $d(C)=7$.

**Example 3.** Let $C$ be the linear code over $Z_{22}$ with the generator matrix

$$G=\begin{pmatrix} 1 & 11 & 11 & 1 & 3 & 17 & 21 & 15 & 21 & 17 \\ 0 & 12 & 0 & 8 & 14 & 18 & 20 & 20 & 18 & 10 \\ 0 & 0 & 12 & 14 & 6 & 10 & 4 & 10 & 6 & 6 \end{pmatrix}.$$

Then $n=10$, $\mathrm{rank}(C)=3$ and $d(C)=8$.

**Example 4.** Let $C$ be the linear code over $Z_{22}$ with the generator matrix

$$G=\begin{pmatrix} 1 & 11 & 11 & 11 & 21 & 7 & 1 & 13 & 9 & 21 & 9 \\ 0 & 12 & 0 & 0 & 4 & 4 & 14 & 4 & 10 & 2 & 6 \\ 0 & 0 & 0 & 12 & 4 & 10 & 20 & 2 & 12 & 18 & 2 \end{pmatrix}.$$

Then $n=11$, $\mathrm{rank}(C)=4$ and $d(C)=8$.

**Example 5.** Let $C$ be the linear code over $Z_{26}$ with the generator matrix

$$G=\begin{pmatrix} 1 & 13 & 13 & 1 & 3 & 19 & 23 & 15 & 21 & 15 & 23 & 7 \\ 0 & 14 & 0 & 10 & 18 & 24 & 2 & 4 & 4 & 2 & 24 & 12 \\ 0 & 0 & 14 & 16 & 6 & 10 & 2 & 8 & 2 & 10 & 6 & 20 \end{pmatrix}.$$

Then $n=12$, $\mathrm{rank}(C)=3$ and $d(C)=10$.

**Example 6.** Let $C$ be the linear code over $\boldsymbol{Z}_{26}$ with the generator matrix

$$G=\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 20 & 2 & 14 & 18 & 12 & 22 & 22 & 12 & 18 & 14 \\ 0 & 0 & 2 & 22 & 14 & 12 & 18 & 20 & 18 & 12 & 2 & 14 & 22 \end{pmatrix}.$$

Then $n=13$, $\mathrm{rank}(C)=3$ and $d(C)=11$.

**Example 7.** Let $C$ be the linear code over $\boldsymbol{Z}_{26}$ with the generator matrix

$$G=\begin{pmatrix} 1 & 13 & 13 & 13 & 25 & 9 & 3 & 18 & 17 & 9 & 7 & 23 & 17 & 15 \\ 0 & 14 & 0 & 0 & 4 & 2 & 10 & 18 & 16 & 20 & 20 & 6 & 20 & 20 \\ 0 & 0 & 14 & 0 & 20 & 6 & 20 & 20 & 16 & 18 & 10 & 2 & 4 & 6 \\ 0 & 0 & 0 & 14 & 4 & 10 & 20 & 22 & 4 & 6 & 16 & 22 & 12 & 24 \end{pmatrix}.$$

Then $n=14$, $\mathrm{rank}(C)=4$ and $d(C)=11$.

**Remark 1.** Observing the proof of the theorem, we notice that the minimum distance $d(C)$ can be replaced by

$$\mathrm{Min}\{|M| \mid M\subseteq N,\ C(M)=0\}.$$

**Remark 2.** In [Shi 98], Shiromoto has proved another Singleton type bound by using the first exact sequence of Proposition for linear codes over finite commutative Frobenius rings. But the result does not contain our maim result in this paper. Indeed, for a linear code of length $n$ over $\boldsymbol{Z}/l\boldsymbol{Z}$, let $M$ be a subset of $N$ with $|M|=n-d(C)+1$, so that $C(N-M)^*=0$, and so we have a short exact sequence

$$0 \longrightarrow C^{\perp}(M) \longrightarrow V(M) \longrightarrow C^* \longrightarrow 0. \tag{12}$$

Thus we have

$$l^{n-d(C)+1}=|V(M)|=|C^{\perp}(M)|\cdot|C|\geq|C| \tag{13}$$

$$\Leftrightarrow \quad d(C)\leq n-\log_l|C|+1, \tag{14}$$

but this inequality is weaker than the Singleton bound proved in the main theorem, because of $\log_l|C|\leq \mathrm{rank}(C)$.

**Remark 3.** The long exact sequence for the Tor-functor $\mathrm{Tor}_m^{Z_l}(\boldsymbol{Z}_f,-)$, where $f$ is a divisor of $l$, on the short exact sequence (12) gives an isomorphism and an exact sequence as follows:

$$\mathrm{Tor}_{m+1}^{Z_l}(\boldsymbol{Z}/f\boldsymbol{Z}, C^*) \cong \mathrm{Tor}_m^{Z_l}(\boldsymbol{Z}/f\boldsymbol{Z}, C^{\perp}(M)) \quad (m \geq 1),$$

$$0 \longrightarrow \mathrm{Tor}_1^{Z_l}(\boldsymbol{Z}/f\boldsymbol{Z}, C^*) \longrightarrow \mathrm{Tor}_0^{Z_l}(\boldsymbol{Z}/f\boldsymbol{Z}, C^{\perp}(M))$$
$$\longrightarrow \mathrm{Tor}_0^{Z_l}(\boldsymbol{Z}/f\boldsymbol{Z}, V(M)) \longrightarrow \mathrm{Tor}_0^{Z_l}(\boldsymbol{Z}/f\boldsymbol{Z}, C^*) \longrightarrow 0.$$

Using this, we have some inequalities like the Singleton bounds for codes. But unfortunately, they are all proved by the main theorem and we do not have any new inequalities.

## References


[ConSl 93] J. H. Conway and N. J. A. Sloane, Self-dual codes over the integers modulo 4, *Journal of Combinatorial Theory.*, A **62** (1993), 30-45.

[McwSl 77] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*, North Holland, Amsterdam, 1977.

[Shi 98] Keisuke Shiromoto, Singleton bounds for codes over finite rings. *Journal of Algebraic Combinatorics.*, **12** (2000), 95-99.

[Wi 94] C. A. Weibel, *An introduction to homological algebra*, Cambridge University Press, 1994.

[Yos 93] Tomoyuki Yoshida, MacWilliams identities for linear codes with group actions, *Kumamoto Journal of Mathematics.*, **6** (1993), 29-45.



Keisuke Shiromoto
Department of Mathematics,
Kumamoto University
Kumamoto 860-8555, JAPAN
keisuke@math.sci.kumamoto-u.ac.jp

Tomoyuki Yoshida
Department of Mathematics,
Hokkaido University
Sapporo 060-0810, JAPAN
yoshidat@math.sci.hokudai.ac.jp