QF RINGS AND DIRECT SUMMAND CONDITIONS

MANABU MATSUOKA

Abstract. In this paper we investigate the rings with the direct summand condition, and we give the applications to coding theory. We study the linear codes over the finite ring with this condition. In particular, we consider dual codes and cyclic codes.

Key Words: direct summand conditions, dual codes, cyclic codes.

2010 *Mathematics Subject Classification*: Primary 94B05; Secondary 94B15, 16D40.

1. Introduction

For a ring R, we consider the condition that every finitely generated free submodule N of a finitely generated free R-module M is a direct summand of M. For example QF rings satisfy this condition. In [4], Y. Hirano proved that a commutative artinian ring satisfies this condition. He also found some class of noncommutative rings with this condition.

In [10], T. Sumiyama studied maximal Galois subrings of finite local rings. Y. Hirano characterized finite frobenius rings in [3]. By the way, since several years, codes over finite Frobenius rings draw considerable attension in coding theory. In [2], M. Greferath investigated splitting codes over finite rings. In [1], A. A. Andrade and Palazzo Jr. studied linear codes over finite rings. J. A. Wood established the extension theorem and MacWilliams identities over finite Frobenius rings in [11]. K. Shiromoto and L. Storme gave a Griesner type bound for linear codes over finite QF rings in [9].

Throughout this paper, R denotes a ring with $1 \neq 0$, n denotes a natural number with $n \geq 2$, unless otherwise stated.

2. Rings with the direct summand condition

For a ring R, we consider the following direct summand condition for free left modules:

$(\mathrm{DS})_{\mathrm{l}}$ Every finitely generated free submodule N of a finitely generated free left R-module M is a direct summand of M.

Similarly, we consider the direct summand condition for free right modules:

$(\mathrm{DS})_{\mathrm{r}}$ Every finitely generated free submodule N of a finitely generated free right R-module M is a direct summand of M.

If R satisfies the both conditions, it is said that it has the condition (DS).

For a semisimple ring, every module is semisimple, and every submodule of a semisimple module is a direct summand. Thus, a semisimple ring satisfies the condition (DS).

Definition 1. For a ring R, R is called a QF (quasi-Frobenius) ring if R is left artinian and left self-injective.

The detailed version of this paper will be submitted for publication elsewhere.

It is well-known that the definition of a QF ring is left-right symmetric.

Proposition 2. *Let R be a QF ring. Then R satisfies the condition* (DS).

For any left R-module ${}_RM$, $M^* = \mathrm{Hom}_R({}_RM, {}_RR)$ is a right R-module. In fact the right R-actions of M^* is defined by

$$(f{\cdot}r)(m) = f(m){\cdot}r$$

where $r \in R$, $m \in M$ and $f \in M^*$.

The natural homomorphism $\xi : M \to M^{**}$ is defined by

$$\xi(m)(f) = f(m)$$

where $m \in M$ and $f \in M^*$. A module M is called torsionless if the natural homomorphism $\xi : M \to M^{**}$ is injective. A torsionless module M is said to be reflexive if the natural injection $\xi : M \to M^{**}$ is an isomorphism.

Proposition 3. *Let R be a ring, and let ${}_RN$ be a left R-submodule of R^n. If ${}_RN$ is a direct summand of R^n, then ${}_RN$ is reflexive.*

For any submodule $A \subseteq M$, let $A^\circ = \{f \in M^* \mid f(A) = 0\}$, which is a submodule of M^*. And, for any submodule $I \subseteq M^*$, let $I^\diamond = \cap_{f\in I}\ker(f)$, which is a submodule of M.

Lemma 4. *Let R be a ring, and let ${}_RM$ be a reflexive left R-module. If I is a right R-submodule of M^*, then $I^\diamond \cong I^\circ$ as left R-modules.*

Lemma 5. *Let R be a ring, and let ${}_RM$ be a free left R-module. If A is a direct summand of M, then $A^{\circ\diamond} = A$.*

By Lemma 4 and Lemma 5, we get the following theorem.

Theorem 6. *Let R be a ring, and let ${}_RM$ be a reflexive free left R-module. If A is a direct summand of M, then $A^{\circ\circ} \cong A$ as left R-modules.*

Corollary 7. *Let R be a ring with the condition* (DS)*, and let ${}_RN$ be a finitely generated free left R-submodule of R^n. Then $N^{\circ\circ} \cong N$ as left R-modules.*

3. Codes over finite rings with the condition (DS)$_{\mathrm{l}}$

Let R be a finite ring. A linear left(right) code C of length n over R is a left(right) R-submodule of the left(right) R-module $R^n = \{(a_0, \cdots, a_{n-1}) \mid a_i \in R\}$. If C is a free R-module, C is said to be a free code.

On R^n define the standard inner product by

$$< x, y >= \textstyle\sum_{i=0}^{n-1} x_i y_i$$

for $x = (x_0, x_1, \cdots, x_{n-1})$, $y = (y_0, y_1, \cdots, y_{n-1}) \in R^n$.

The dual code $C^\perp$ of a linear left code C is defined by

$$C^\perp = \{a \in R^n \mid \ < c, a >= 0 \text{ for any } c \in C\}.$$

Clearly, $C^\perp$ is a linear right code over R.

Similarly, for a linear right code D, we can define the dual code

$$D^\perp = \{b \in R^n \mid \ < b, d >= 0 \text{ for any } d \in D\},$$

Then $D^\perp$ is a linear left code over R.

For a left(right) code $C \subseteq R^n$, C is called a self-dual code if $C = C^\perp$. In this case, C is a bi-module.

For any left R-submodule $C \subseteq R^n$, C° is defined by

$$C^\circ = \{\lambda \in \mathrm{Hom}_R({}_RR^n, {}_RR) \mid \lambda(C) = 0\}.$$

Then C° is a right R-submodule of a right R-module $Hom_R({}_RR^n, {}_RR)$.

For every $x \in R^n$, we define a right R-module homomorphism $\delta_x : R^n \to R$ as $\delta_x(y) =< y, x >$.

Let $e_1, \cdots, e_n$ be fundamental vectors. We define a natural right R-module homomorphism $\epsilon : ({}_RR^n)^* \to R^n_R$ as $\epsilon(f) = (f(e_1), \cdots, (e_n))$. Then ϵ is an isomorphism. In fact $\delta : R^n_R \to ({}_RR^n)^*$ with $\delta(x) = \delta_x$ is an inverse map.

Proposition 8. *Let R be a finite ring, and let $C \subseteq R^n$ be a linear left code. Then $C^\perp \cong C^\circ$ as right R-modules.*

Theorem 9. *Let R be a finite ring with the condition* (DS). *For a free left code $C \subseteq R^n$, $(C^\perp)^\perp = C$.*

Given any subset $T \subseteq R$, a left annihilator of T is a set

$$\text{l.ann}_R(T)= \{r \in R \mid rt = 0 \text{ for all } t \in T\}$$

which is a left ideal of R. A right annihilator $\text{r.ann}_R(T)$ is defined, similarly.

Then we can get the following corollary.

Corollary 10. *Let R be a finite ring with the condition* (DS). *For a free left submodule C of ${}_RR$, we have*

$$\text{l.ann}_R(\text{r.ann}_R C) = C.$$

Similarly, if R satisfies the direct summand condition for free modules, then we have $\text{r.ann}_R(\text{l.ann}_R D) = D$ for any free right submodule D of R_R.

Theorem 11. *Let R be a finite ring with the condition* $(\text{DS})_1$. *If $C \subseteq R^n$ is a free left code of finite rank, then $C^\perp$ is a free right code of finite rank and* $\text{rank}C^\perp = n - \text{rank}C$.

4. Cyclic codes

Let R be a finite ring. A linear left(right) code $C \subseteq R^n$ is called cyclic if

$$(a_0, a_1, \cdots, a_{n-1}) \in C \text{ implies } (a_{n-1}, a_0, a_1, \cdots, a_{n-2}) \in C.$$

Let E be the following square matrix;

$$E = \begin{pmatrix} 0 & 1 & & 0 \\ & & \ddots & \\ 0 & & & 1 \\ 1 & 0 & \cdots & 0 \end{pmatrix}.$$

It follows that a left code $C \subseteq R^n$ is cyclic if and only if it is invariant under right multiplication by E.

Proposition 12. *Let R be a finite ring, and let $C \subseteq R^n$ be a linear left code. If C is a cyclic left code, $C^\perp$ is a cyclic right code.*

By Theorem 9 and Proposition 12, we get the following corollary.

Corollary 13. *Let R be a finite ring with the condition* (DS)*, and let $C \subseteq R^n$ be a free left code. Then C is a cyclic left code if and only if $C^{\perp}$ is a cyclic right code.*

In what follows, we shall use the following conventions:
$(g)_l$ is the left ideal generated by $g \in R[X]$.
$(g)_r$ is the right ideal generated by $g \in R[X]$.
(g) is the two-sided ideal generated by $g \in R[X]$.

Cyclic codes are understood in terms of left ideals in quotient rings of polynomial rings. The left R-module isomorphism $\rho : R^n \to R[X]/(X^n - 1)$ sending the vector $a = (a_0, a_1, \cdots, a_{n-1})$ to the equivalence class of polynomial $a_{n-1}X^{n-1} + \cdots + a_1X + a_0$, allows us to identify the cyclic left code with the left ideal of $R[X]/(X^n - 1)$.

Notice that $X^n - 1$ is the central element of $R[X]$.

Theorem 14. *Let R be a finite ring. There is a one to one correspondence between cyclic left codes in R^n and left ideals of $R[X]/(X^n - 1)$.*

Definition 15. Let R be a finite ring, and let C be a cyclic left code in $R[X]/(X^n-1)$. If there exist monic polynomials g and h such that $\rho(C) = (g)_l/(X^n - 1)$ and $X^n - 1 = hg$, then C is called the principal cyclic left code. In this case, $g(X)$ is called the generator polynomial and $h(X)$ is called the parity check polynomial of C. Similarly, for a cyclic right code C, C is called the principal cyclic right code if $\rho(C) = (g)_r/(X^n - 1)$ and $X^n - 1 = gh$.

Proposition 16. *Let R be a finite ring, and let $C \subseteq R^n$ be a principal cyclic left code with the generator polynomial $g(X)$ of degree $n - k$. Then C is a free left code of rank k.*

Let $C \subseteq R^n$ be a free left(right) code. If a basis of C is used as rows of a matrix G, the matrix G is called a generator matrix of C. If G is a $k \times n$ generator matrix of a free left code C, then, for any $c \in C$, we have $c = aG$ for some $a \in R^k$. If G is a $k \times n$ generator matrix of a free right code D, then, for any $d \in D$, we have ${}^t d = {}^t G {}^t b$ for some $b \in R^k$. A generator matrix of $C^{\perp}$ is called a parity check matrix of C.

Proposition 17. *Let R be a finite ring, and let $C \subseteq R^n$ be a principal cyclic left code with the generator polynomial*

$$g(X) = g_{n-k}X^{n-k} + \cdots + g_1X + g_0$$

with $g_{n-k} = 1$. Then C has the $k \times n$ generator matrix G of the form

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k} & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ \vdots & & & & & & \vdots \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_{n-k} \end{pmatrix}.$$

The generator matrix of the principal cyclic right code $\rho(C) = (g)_r/(X^n-1)$ with $X^n-1 = gh$ is the same form.

Next, we determine the parity check matrix of a principal cyclic left code.

Proposition 18. *Let R be a finite ring with the condition* $(\mathrm{DS})_{\mathrm{l}}$*, and let $C \subseteq R^n$ be a principal cyclic left code with the generator polynomial $g(X)$ of degree $n-k$ and the parity check polynomial*

$$h(X) = h_k X^k + \cdots + h_1 X + h_0$$

with $h_k = 1$. Suppose $X^n - 1 = hg = gh \in R[X]$. Then C has the $(n-k) \times n$ parity check matrix H of the form

$$H = \begin{pmatrix} h_k & \cdots & h_1 & h_0 & 0 & \cdots & 0 \\ 0 & h_k & \cdots & h_1 & h_0 & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ \vdots & & & & & & \vdots \\ 0 & \cdots & 0 & h_k & \cdots & h_1 & h_0 \end{pmatrix}.$$

Corollary 19. *Let R be a finite ring with the condition* $(\mathrm{DS})_{\mathrm{l}}$*, and let $C \subseteq R^n$ be a principal cyclic left code with the generator polynomial $g(X)$ of degree $n-k$ and the parity check polynomial*

$$h(X) = h_k X^k + \cdots + h_1 X + h_0$$

with $h_k = 1$. Suppose $X^n - 1 = hg = gh \in R[X]$. Then $C^{\perp}$ is the principal cyclic right code, and we have

$$\rho(C^{\perp}) = (h^{\perp})_r / (X^n - 1),$$

where $h^{\perp}(X) = (h_0 X^k + \cdots + h_{k-1} X + h_k) h_0{}^{-1}$.

Proposition 20. *Let R be a finite ring, and let $C \subseteq R^n$ be a principal cyclic left code with the generator polynomial $g(X)$ and the parity check polynomial $h(X)$. Suppose $X^n - 1 = hg = gh \in R[X]$. Then $a \in C$ if and only if $\rho(a)\overline{h} = 0$ in $R[X]/(X^n - 1)$.*

Then we get the following corollary.

Corollary 21. *Let R be a finite ring, and let $C \subseteq R^n$ be a principal cyclic left code with the generator polynomial $g(X)$ and the parity check polynomial $h(X)$. Suppose $X^n - 1 = hg = gh \in R[X]$. Set $\overline{R} = R[X]/(X^n - 1)$. Then we have*

$$\rho(C) = (g)_l / (X^n - 1) = \mathrm{l.ann}_{\overline{R}} \left(\overline{h}\right).$$

By Corollary 19 and Proposition 20, we get the following corollary.

Corollary 22. *Let R be a finite ring with the condition* $(\mathrm{DS})_{\mathrm{l}}$*, and let $C \subseteq R^n$ be a principal cyclic left code with the generator polynomial*

$$g(X) = g_{n-k} X^{n-k} + \cdots + g_1 X + g_0$$

with $g_{n-k} = 1$ and the parity check polynomial $h(X)$. Suppose $X^n - 1 = hg = gh \in R[X]$. Set $\overline{R} = R[X]/(X^n - 1)$. Then we have

$$\rho(C^{\perp}) = (h^{\perp})_r / (X^n - 1) = \mathrm{r.ann}_{\overline{R}} \left(\overline{g^{\perp}}\right),$$

where $g^{\perp}(X) = g_0^{-1}(g_0 X^{n-k} + \cdots + g_{n-k-1} X + g_{n-k})$.

Now we give a basic example.

Example 23. Let $\mathbf{Z}_2$ be a finite field of two elements, and $M_2(\mathbf{Z}_2)$ be a set of 2×2 matrices over $\mathbf{Z}_2$. Let $R = D_2(\mathbf{Z}_2)$, where

$$D_2(\mathbf{Z}_2) = \left\{ \left(\begin{array}{cc} a & b \\ 0 & a \end{array} \right) \in M_2(\mathbf{Z}_2) \,\middle|\, a, b \in \mathbf{Z}_2 \right\}.$$

R is a finite commutative local ring with the unique maximal ideal

$$M = \left\{ \left(\begin{array}{cc} 0 & b \\ 0 & 0 \end{array} \right) \in M_2(\mathbf{Z}_2) \,\middle|\, b \in \mathbf{Z}_2 \right\}.$$

Then R satisfies the condition (DS).

Now set $i = \left(\begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array} \right)$. Then we have

$$R = \{ \ 0, \ 1, \ i, \ 1+i \ \}$$

with $i^2 = 1$. Thus we get $D_2(\mathbf{Z}_2) = \mathbf{Z}_2[\ i\ ]$.

Now we get the following factorizations:

$$X^4 - 1 = (X^2 + (1+i)X + i)(X^2 + (1+i)X + i).$$

Set $\rho(C) = (X^2 + (1+i)X + i)/(X^4 - 1)$. Then C is a principal cyclic code of rank 2. And we get $\rho(C^{\perp}) = (X^2 + (1+i)X + i)/(X^4 - 1)$. Hence this is a self-dual code.

References

[1] A. A. Andrade and Palazzo Jr., *Linear Codes over Finite Rings*, TEMA Tend. Mat. Apl. Comput. **6**, No. **2** (2005), 207–217.

[2] M. Greferath, *Note cyclic codes over finite rings*, Discrete Math, **177** (1997), 273–277.

[3] Y. Hirano, *On admissible rings*, Indag. Math. **8** (1997), 55–59.

[4] Y. Hirano, *Rings in which every free submodule of a free module is a direct summand* (preprint).

[5] S. Ikehata, *On separable polynomials and Frobenius polynomials in skew polynomial rings*, Math. J. Okayama. Univ. **22** (1980), 115–129.

[6] T. Y. Lam, *Lectures on Modules and Rings*, Graduate Texts in Mathematics, Vol.189, Springer-Verlag, New York, 1999.

[7] M. Matsuoka, *Polycyclic codes and sequential codes over finite commutative QF rings*, JP Journal of Algebra, Number Theory and Applications, Volume **23**, Number **1** (2011), 77–85.

[8] B. R. McDonald, *Finite Rings With Identity*, Pure and Applied Mathematics, Vol. 28, Marcel Dekker, Inc., New York, 1974.

[9] K. Shiromoto and L. Storme, *A Griesner bound for linear codes over finite quasi-Frobenius rings*, Discrete Applied Mathematics **128** (2003), 263–274.

[10] T. Sumiyama, *Note on maximal Galois subrings of finite local rings*, Math. J. Okayama. Univ. **21** (1979), No. **1**, 31–32.

[11] J. A. Wood, *Duality for modules over finite rings and applications to coding theory*, Amer. J. Math, **121** (1999), 555–575.

Faculty of Child Sciences
Osaka Shoin Women's University
958 Sekiya Kashiba-City Nara 639-0298, JAPAN
E-mail address: matsuoka.manabu@osaka-shoin.ac.jp