POLYCYCLIC CODES AND SEQUENTIAL CODES

MANABU MATSUOKA

Abstract. In this paper we generalize the notion of cyclicity of codes, that is, polycyclic codes and sequential codes. We study the relation between polycyclic codes and sequential codes over finite commutative QF rings. Furthermore, we characterized the family of some constacyclic codes.

Key Words: finite rings, (θ, δ)-codes, skew polynomial rings.

2010 *Mathematics Subject Classification*: Primary 94B60; Secondary 94B15.

1. Introduction

Let R be a finite commutative ring. A linear code C of length n over R is a submodule of the R-module $R^n = \{(a_0, \cdots, a_{n-1}) | a_i \in R\}$. If C is a free R-module, C is said to be a free code. A linear code $C \subseteq R^n$ is called cyclic if $(a_0, a_1, \cdots, a_{n-1}) \in C$ implies $(a_{n-1}, a_0, a_1, \cdots, a_{n-2}) \in C$. The notion of cyclicity has been extended in various directions.

In [6], S. R. López-Permouth, B. R. Parra-Avila and S. Szabo studied the duality between polycyclic codes and sequential codes. By the way, J. A. Wood establish the extension theorem and MacWilliams identities over finite frobenius rings in [9]. M. Greferath and M. E. O'Sullivan study bounds for block codes on finite frobenius rings in [2]. In this paper, we generalize the result of [6] to codes with finite commutative QF rings.

In section 2 we define polycyclic codes over finite commutative rings. And we study the properties of polycyclic codes. In section 3 we define sequential codes and consider the properties of sequential codes. In section 4 we study the relation between polycyclic codes and sequential codes over finite commutative QF rings. And we characterized the family of some constacyclic codes.

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

2. Polycyclic codes

A linear $[n, k]$-code over a finite commutative ring R is a submodule $C \subseteq R^n$ of rank k. We define polycyclic codes over a finite commutative ring.

Definition 1. Let C be a linear code of length n over R. C is a polycyclic code induced by c if there exists a vector $c = (c_0, c_1, \cdots, c_{n-1}) \in R^n$ such that for every $(a_0, a_1, \cdots, a_{n-1}) \in C$, $(0, a_0, a_1, \cdots, a_{n-2}) + a_{n-1}(c_0, c_1, \cdots, c_{n-1}) \in C$. In this case we call c an associated vector of C.

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

As cyclic codes, polycyclic codes may be understood in terms of ideals in quotient rings of polynomial rings. Given $c = (c_0, c_1, \cdots, c_{n-1}) \in R^n$, if we let $f(X) = X^n - c(X)$, where $c(X) = c_{n-1}X^{n-1} + \cdots + c_1X + c_0$ then the R-module homomorphism $\rho : R^n \to R[X]/(f(X))$ sending the vector $a = (a_0, a_1, \cdots, a_{n-1})$ to the equivalence class of polynomial $\overline{a_{n-1}X^{n-1} + \cdots + a_1X + a_0}$, allows us to identify the polycyclic codes induced by c with the ideal of $R[X]/(f(X))$.

Definition 2. Let C be a polycyclic code in $R[X]/(f(X))$. If there exist monic polynomials g and h such that $\rho(C) = (g)/(f)$ and $f = hg$, then C is called a principal polycyclic code.

Proposition 3. *A code $C \subseteq R^n$ is a principal polycyclic code induced by some $c \in C$ if and only if C is a free R-module and has a $k \times n$ generator matrix of the form*

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

with an invertible g_{n-k}. In this case

$$\rho(C) = \left(\overline{g_{n-k}X^{n-k} + \cdots + g_1X + g_0}\right)$$

is the ideal of $R[X]/(f(X))$.

Definition 4. Let $C = (g)/(f) \subseteq R[X]/(f(X))$ be a principal polycyclic code. If the constant term of g is invertible, then C is called a principal polycyclic code with an invertible constant term.

For a $c = (c_0, c_1, \cdots, c_{n-1}) \in R^n$, let D_c be the following square matrix;

$$D_c = \begin{pmatrix} 0 & 1 & & 0 \\ & & \ddots & \\ 0 & & & 1 \\ c_0 & c_1 & \cdots & c_{n-1} \end{pmatrix}.$$

It follows that a code $C \subseteq R^n$ is polycyclic with an associated vector $c \in R^n$ if and only if it is invariant under right multiplication by D_c.

3. Sequential codes

Definition 5. Let C be a linear code of length n over R. C is a sequential code induced by c if there exists a vector $c = (c_0, c_1, \cdots, c_{n-1}) \in R^n$ such that for every $(a_0, a_1, \cdots, a_{n-1}) \in C$, $(a_1, a_2, \cdots, a_{n-1}, a_0c_0 + a_1c_1 + \cdots + a_{n-1}c_{n-1}) \in C$. In this case we call c an associated vector of C.

Let C be a sequential code with an associated vector $c = (c_0, c_1, \cdots, c_{n-1})$. Then C is invariant under right multiplication by the matrix

$$
{}^tD_c = \begin{pmatrix} 0 & & 0 & c_0 \\ 1 & & & c_1 \\ & \ddots & & \vdots \\ 0 & & 1 & c_{n-1} \end{pmatrix}
$$

On R^n define the standard inner product by

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

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 code C is defined by

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

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

Theorem 6. *For a code $C \subseteq R^n$, we have the following assertions:*
(1) *If C is polycyclic, then $C^\perp$ is sequential.*
(2) *If C is sequential, then $C^\perp$ is polycyclic.*

4. Codes over finite commutative QF rings

Let R be a (not necessarily commutative) ring. A left R-module P is projective if for every R-epimorphism $g : M \to N$ and every R-homomorphism $f : P \to N$, there exists a R-homomorphism $h : P \to M$ with $f = g \circ h$.

A left R-module Q is injective if for every R-monomorphism $g : N \to M$ and every R-homomorphism $f : N \to Q$, there exists a R-homomorphism $h : M \to Q$ with $f = h \circ g$.

The ring R is said to be left (resp. right) self-injective if R itself is injective as left (resp. right) R-module. If both conditions hold, R is said to be a self-injective ring.

A left R-module M is Artinian if M is satisfies the descending chain condition on submodules. A ring R is left (resp. right) Artinian if R itself is Artinian as left (resp. right) R-module. If both conditions hold, R is said to be an Artinian ring.

It is clear that a finite ring is an Artinian ring.

Definition 7. For a (not necessarily commutative) ring R, R is called a QF (quasi-Frobenius) ring if R is left Artinian and left self-injective.

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

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

$$C^\circ = \{\lambda \in Hom_R(R^n, R) | \lambda(C) = 0\}.$$

Theorem 8. *For a (not necessarily commutative) ring R, the following conditions are equivalent:*
(1) *R is a QF ring.*
(2) *For submodules $M \subseteq R^n$, $M^{\circ\circ} = M$.*

Theorem 9. *For a (not necessarily commutative) ring R, the following are equivalent:*
(1) *R is a QF ring.*
(2) *A left module is projective if and only if it is injective.*

We define an R-module homomorphism $\delta_x : R^n \to R$ as $\delta_x(y) =< y, x >$ for any $x \in R^n$.

Proposition 10. *The homomorphism $\delta : C^{\perp} \to C^{\circ}$ sending x to δ_x is an isomorphism of R-modules.*

Theorem 11. *Let R be a finite commutative QF ring. For a submodule $C \subseteq R^n$, $(C^{\perp})^{\perp} = C$.*

By Theorem 1 and Theorem 4, we can get the following corollary.

Corollary 12. *Let R be a finite commutative QF ring. Then C is a polycyclic code if and only if $C^{\perp}$ is a sequential code.*

Theorem 13. *Let R be a finite commutative QF ring. If $C \subseteq R^n$ is a free R-module of finite rank, then $C^{\perp}$ is a free R-module of* $\mathrm{rank} C^{\perp} = n - \mathrm{rank} C$.

We determine the parity check matrix of a constacyclic code.

Proposition 14. *Let R be a finite commutative QF ring and $f = X^n - \alpha \in R[X]$. Suppose $f = hg \in R[X]$ where g and h are polynomials of degree $n-k$ and k, respectively. Let C be the linear $[n,k]$-code corresponding to the ideal generated by g in $R[X]/(X^n - \alpha)$ and $h(X) = h_k X^k + h_{k-1}X^{k-1} + \cdots + h_1 X + h_0$. Then C has the $(n-k) \times n$ parity check matrix H given by*

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

Definition 15. Let R be a finite commutative QF ring. For a sequential code $C \subseteq R^n$, C is called a principal sequential code if $C^{\perp}$ is a principal polycyclic code. And C is called a principal sequential code with an invertible constant term if $C^{\perp}$ is a principal polycyclic code with an invertible constant term.

Now we can get the main theorem.

Theorem 16. *Let R be a finite commutative QF ring. Suppose C is a free codes of R^n. Then the following conditions are equivalent:*
(1) *Both C and $C^{\perp}$ are principal polycyclic codes with invertible constant terms.*
(2) *Both C and $C^{\perp}$ are principal sequential codes with invertible constant terms.*
(3) *C is a principal polycyclic and sequential code with an invertible constant term.*
(4) *$C^{\perp}$ is a principal polycyclic and sequential code with an invertible constant term.*
(5) *$C = (g)/(X^n - \alpha)$ is a constacyclic code with an invertible α.*
(6) *$C^{\perp} = (q)/(X^n - \beta)$ is a constacyclic code with an invertible β.*

Acknowledgement. The author wishes to thank Prof. Y. Hirano, Naruto University of Education, for his helpful suggestions and valuable comments.

References

[1] D. Boucher and P. Solé, *Skew constacyclic codes over Galois rings*, Advances in Mathematics of Communications, Volume **2**, No. **3** (2008), 273–292.

[2] M. Greferath, M. E. O'Sullivan, *On bounds for codes over Frobenius rings under homogeneous weights*, Discrete Math, **289** (2004), 11–24.

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

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

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

[6] S. R. López-Permouth, B. R. Parra-Avila and S. Szabo, *Dual generalizations of the concept of cyclicity of codes*, Advances in Mathematics of Communications, Volume **3**, No. **3** (2009), 227–234.

[7] M. Matsuoka, *θ-polycyclic codes and θ-sequential codes over finite fields*, International Journal of Algebra, Vol. **5** (2011), no. **2**, 65–70.

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

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

Kuwanakita-Highscool
2527 Shimofukayabe Kuwana Mie 511-0808 Japan
E-mail address: e-white@hotmail.co.jp