JP Journal of Algebra, Number Theory and Applications
Volume 23, Number 1, 2011, Pages 77-85
Published Online: September 14, 2011
Available online at http://pphmj.com/journals/jpanta.htm

POLYCYCLIC CODES AND SEQUENTIAL CODES OVER FINITE COMMUTATIVE QF RINGS

MANABU MATSUOKA

Graduate School in Science of School Education
Hyogo University of Teacher Education
942-1 Shimokume, Kato city
Hyogo 673-1494
Japan
e-mail: e-white@hotmail.co.jp

Abstract

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

1. Introduction

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

In [6], López-Permouth et al. studied the duality between polycyclic codes and sequential codes. By the way, Wood established the extension theorem and MacWilliams identities over finite Frobenius rings in [9]. Greferath and O'Sullivan

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

Keywords and phrases: polycyclic codes, sequential codes, QF rings.

Received April 1, 2011

studied 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 characterize 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 $c = (c_0, c_1, ..., c_{n-1}) \in R^n$ such that for every

$$(a_0, a_1, ..., a_{n-1}) \in C, (0, a_0, a_1, ..., a_{n-2}) + a_{n-1}(c_0, c_1, ..., c_{n-1}) \in C.$$

In this case, we call c an *associated vector* of C.

As cyclic codes, polycyclic codes may be understood in terms of ideals in quotient rings of polynomial rings. Given $c = (c_0, c_1, ..., c_{n-1}) \in R^n$, 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 $a = (a_0, a_1, ..., a_{n-1})$ 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 1. *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,* $\rho(C) = (\overline{g_{n-k}X^{n-k} + \cdots + g_1X + g_0})$ *is the ideal of* $R[X]/(f(X))$.

Proof. If C is principal polycyclic, then we may assume that $\rho(C) = (g)/(f)$, where the leading coefficient of g is invertible. Then $\{\overline{X^{k-1}g(X)}, \ldots, \overline{Xg(X)}, \overline{g(X)}\}$ is a basis of $\rho(C)$. Hence, C is a free module and above G is a generator matrix of C.

Conversely, suppose G is a generator matrix of C and g_{n-k} is invertible. Put

$$g(X) = g_{n-k}X^{n-k} + g_{n-k-1}X^{n-k-1} + \cdots + g_1X + g_0.$$

Now let $h(X)$ be any polynomial whose leading coefficient is invertible and of degree k. Then $f(X) = h(X)g(X)$ is a polynomial whose leading coefficient is invertible and of degree n. Then $\rho(C) = (g)/(f)$ is an ideal of $R[X]/(f)$. Therefore, C is principal polycyclic. □

Definition 3. Let $C = (g)/(f)$ be a principal polycyclic code in $R[X]/(f(X))$. If the constant term of g is invertible, then C is called a *principal polycyclic code* with an invertible constant term.

For a $c = (c_0, c_1, \ldots, c_{n-1}) \in R^n$, 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 4. Let C be a linear code of length n over R. Then C is a sequential code induced by c if there exists a vector $c = (c_0, c_1, \ldots, c_{n-1}) \in R^n$ such that for every

$$(a_0, a_1, \ldots, a_{n-1}) \in C, (a_1, a_2, \ldots, a_{n-1}, a_0c_0 + a_1c_1 + \cdots + a_{n-1}c_{n-1}) \in C.$$

In this case, we call c an *associated vector* of C.

Let C be a sequential code with an associated vector $c = (c_0, c_1, \ldots, c_{n-1})$. 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

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

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

The orthogonal of a linear code C is defined by

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

Clearly, $C^{\perp}$ is a linear code. $C^{\perp}$ is called a *dual code* of C.

Theorem 1. *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.*

Proof. (1) If C is polycyclic, then we have $aD_c \in C$ for any $a \in C$. So,

$aD_c{}^t b = 0$ for any $b \in C^{\perp}$. By $a(D_c{}^t b) = 0$, we get $D_c{}^t b \in C^{\perp}$. Hence, $C^{\perp}$ is sequential.

(2) It is proved analogously to use ${}^t D_c$ instead of D_c. □

4. Codes over Finite Commutative QF Rings

Let R be a (not necessarily commutative) ring. Then 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 an 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 an 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, then R is said to be a *self-injective ring*.

A left R-module M is Artinian if M 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, then R is said to be an *Artinian ring*.

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

Definition 5. 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 2. *For a* (*not necessarily commutative*) *ring* R, *the following conditions are equivalent*:

(1) *R is a QF ring*.

(2) *For submodules* $M \subseteq R^n$, $M^{\circ\circ} = M$.

Proof. See [9, Theorem 7.2]. □

Theorem 3. *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*.

Proof. See [5, Theorem 15.9]. □

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

Proposition 2. *The homomorphism* $\delta : C^{\perp} \to C^{\circ}$ *sending* x *to* δ_x *is an isomorphism of R-modules*.

Proof. Straightforward. □

Theorem 4. *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* $rank C^{\perp} = n - rank C$.

Proof. Let $k = rank C$. Since C is a free R-module, it is a projective R-module. Then C is an injective R-module. Hence, C is a direct summand of R^n. And there exists some submodule K such that $R^n = C \oplus K$. Then K is a free R-module of rank $n - k$. Therefore, we can get the following:

$$C^{\perp} \cong C^{\circ} \cong Hom_R(K, R) \cong Hom_R(R^{n-k}, R) \cong R^{n-k}.$$ □

Corollary 1. *Let R be a finite commutative QF ring. For a submodule* $C \subseteq R^n$, $(C^{\perp})^{\perp}. = C$.

Proof. By Theorem 4, $rank C = rank(C^{\perp})^{\perp}$ and $C \subseteq (C^{\perp})^{\perp}$. Since the orders of C and $(C^{\perp})^{\perp}$ are finite, we get $C = (C^{\perp})^{\perp}$. □

By Theorem 1 and Corollary 1, we can get the following Corollary 2.

Corollary 2. *Let R be a finite commutative QF ring. Then C is a polycyclic code if and only if* $C^{\perp}$ *is a sequential code*.

We determine the parity check matrix of a constacyclic code.

Proposition 3. *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*

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

Proof. For any $a \in C$, it holds $ah = 0$ in $R[X]/(X^n - \alpha)$. Now $\deg(ah) < n + k$ and we deduce the coefficients of the monomials $X^k, X^{k+1}, \ldots, X^{n-1}$ in this product ah must be zero. Since R is commutative and $\sum_{j=0}^{k} a_{l-j} h_j = 0$ $(l = k, k+1, \ldots, n-1)$, we get $Ha = 0$. As the leading coefficient of h is invertible, the rank of above matrix is $n - k$. Hence, we get the result. □

Definition 6. 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.

Theorem 5. *Let R be a finite commutative QF ring. Suppose C is a free code 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.

Proof. The equivalence of first four statements is from Corollary 2.

(1) $\Rightarrow$ (5) If C and $C^{\perp}$ have generator matrices of the forms

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

and

$$H = \begin{pmatrix} h_k & h_{k-1} & \cdots & h_0 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & h_k & h_{k-1} & \cdots & h_0 \end{pmatrix},$$

respectively, then as $G^t H = 0$, we get $g(X)h(X) = g_{n-k}h_k X^n + g_0 h_0$, where $g(X) = \sum g_i X^i$ and $h(X) = \sum h_j X^j$. Since g_{n-k}, g_0, h_k and h_0 are invertible, C is constacyclic.

(5) $\Rightarrow$ (1) Clearly, C is a principal polycyclic code with an invertible constant term. Next let $R[X, X^{-1}]$ be a Laurent polynomial ring. Then we can define a map $\varphi : R[X] \to R[X, X^{-1}]$ such that $\sum_{i=0}^{n} a_i X^i \mapsto \sum_{i=0}^{n} a_i X^{-i}$. For $\xi, \eta \in R[X]$, we get $\varphi(\xi + \eta) = \varphi(\xi) + \varphi(\eta)$ and $\varphi(\xi\eta) = \varphi(\xi)\varphi(\eta)$. If $X^n - \alpha = h \cdot g$, then we have $X^k \cdot \varphi(h) \cdot \varphi(g) \cdot X^{n-k} = X^k \cdot \varphi(X^n - \alpha) \cdot X^{n-k} = 1 - \alpha X^n$. By $X^k \cdot \varphi(h) = h_k + h_{k-1}X + \cdots + h_0 X^k$ and Proposition 3, $C^{\perp}$ is a constacyclic code with the generator matrix $X^k \cdot \varphi(h)$. That is, $C^{\perp}$ is a principal polycyclic code with an invertible constant term.

Since C and $C^{\perp}$ are symmetric, we can get (1) $\Rightarrow$ (6), similarly. □

Acknowledgement

The author wishes to thank Professor 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, Adv. Math. Commun. 2(3) (2008), 273-292.

[2] M. Greferath and 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, Adv. Math. Commun. 3(3) (2009), 227-234.

[7] M. Matsuoka, θ-polycyclic codes and θ-sequential codes over finite fields, Internat. J. Algebra 5(2) (2011), 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.