International Journal of Algebra, Vol. 5, 2011, no. 2, 65 - 70

θ-Polycyclic Codes and θ-Sequential Codes over Finite Fields

Manabu Matsuoka[1]

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

Abstract. In this paper we generalize the notion of cyclicity of codes, that is, θ-polycyclic codes and θ-sequential codes. It is shown that for a code C, C is θ-polycyclic (θ-sequential) if and only if its dual $C^{\perp}$ is θ^{-1}-sequential (θ^{-1}-polycyclic). Furthermore, we study central θ-constacyclic codes.

Mathematics Subject Classification: Primary 94B60; Secondary 94B15, 16W20

Keywords: finite fields, θ-polycyclic codes, θ-sequential codes, skew polynomial rings

1. Introduction

Let $\mathbf{F}$ be a finite field. A linear code of length n over $\mathbf{F}$ is a subspace C of the vector space $\mathbf{F}^n = \{(a_0, \cdots, a_{n-1}) | a_i \in \mathbf{F}\}$. For a code $C \subseteq \mathbf{F}^n$, C is a polycyclic code induced by c if there exists a vector $c = (c_0, c_1, \cdots, c_{n-1}) \in \mathbf{F}^n$ such that for every $(a_0, a_1, \cdots, a_{n-1}) \in C$, $(0, a_0, a_1, \cdots, a_{n-2}) + a_{n-1}(c_0, c_1, \cdots, c_{n-1}) \in C$. And C is a sequential code induced by c if there exists a vector $c = (c_0, c_1, \cdots, c_{n-1}) \in \mathbf{F}^n$ such that for every $(a_0, a_1, \cdots, a_{n-1}) \in C$, $(a_1, a_2, \cdots, a_{n-1}, a_0c_0 + a_1c_1 + \cdots + a_{n-1}c_{n-1}) \in C$.

Xiang-dong Hou, S. R. López-Permouth and B. R. Parra-Avila introduced sequential codes in [6]. And S. R. López-Permouth, B. R. Parra-Avila and S. Szabo studied the duality between polycyclic codes and sequential codes in [7]. By the way, D. Boucher and P. Solé studied skew constacyclic codes in [4]. They considered skew polynomial rings over Galois rings. In this paper, we generalize the result of [7] to codes with skew polynomial rings of automorphism type.

[1]The author is a doctoral program student of the Joint Graduate School in Science of School Education, Hyogo University of Teacher Education, 942-1 Shimokume, Kato city, Hyogo 673-1494, Japan.

Throughout this paper, $\mathbf{F}$ represents a finite field with $1 \neq 0$, θ an automorphism of $\mathbf{F}$ and $\mathbf{F}[X;\theta]$ a skew polynomial ring of automorphism type, unless otherwise stated.

We shall use the following conventions:

$\theta(a) = (\theta(a_0), \theta(a_1), \cdots, \theta(a_{n-1}))$ where $a = (a_0, a_1, \cdots, a_{n-1})$.
$(g)_l$ is the left ideal generated by $g \in \mathbf{F}[X;\theta]$.
(g) is the two-sided ideal generated by $g \in \mathbf{F}[X;\theta]$.
$Z(\mathbf{F}[X;\theta])$ is the center of $\mathbf{F}[X;\theta]$.
$\mathbf{F}^\theta = \{r \in \mathbf{F} | \theta(r) = r\}$.

2. θ-polycyclic codes and θ-sequential codes

First we review the definition of skew polynomial rings. Complete treatment of this rings can be found in [5] and [8].

Definition 1. *Let $\mathbf{F}$ be a finite field and θ be an automorphism of $\mathbf{F}$. Suppose S is a $\mathbf{F}$-vector space with a basis $\{1, X, X^2, \cdots\}$ and give a multiplication from the rules $X^iX^j = X^{i+j}$ and $Xr = \theta(r)X$ for all $r \in \mathbf{F}$. The ring S constructed in this way is denoted by $\mathbf{F}[X;\theta]$ and is called a skew polynomial ring.*

Proposition 1. *Let $\mathbf{F}$ be a finite field and θ be an automorphism of $\mathbf{F}$. For any $f, g \in \mathbf{F}[X;\theta]$, there exist polynomials q and r such that $g = qf + r$ where $\deg(r) < \deg(f)$.*

Proof. By the induction on deg(g), it is proved. □

Definition 2. *Let R be a ring. R is called a principal left ideal domain if it is a domain in which all left ideals are principal. A principal right ideal domains are defined analogously.*

Theorem 1. *$\mathbf{F}[X;\theta]$ is a principal left ideal domain and is also a principal right ideal domain.*

Proof. See [5, Theorem 1.11]. □

Now we define θ-polycyclic codes and study some properties of them.

Definition 3. *Let $C \subseteq \mathbf{F}^n$ be a linear code. C is a θ-polycyclic code induced by c if there exists a vector $c = (c_0, c_1, \cdots, c_{n-1}) \in \mathbf{F}^n$ such that for every $(a_0, a_1, \cdots, a_{n-1}) \in C$,*

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

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

As cyclic codes, θ-polycyclic codes may be understood in terms of ideals in quotient rings of skew polynomial rings.

Given $c = (c_0, c_1, \cdots, c_{n-1}) \in \mathbf{F}^n$, 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 $\mathbf{F}$-linear isomorphism $\rho : \mathbf{F}^n \to \mathbf{F}[X;\theta]/(f(X))$ sending the vector $a = (a_0, a_1, \cdots, a_{n-1})$ to the polynomial

$a_{n-1}X^{n-1}+\cdots+a_1X+a_0$, allows us to identify the θ-polycyclic codes induced by c with the left ideal of $\mathbf{F}[X;\theta]/(f(X))$.

Let D_c be the following square matrix;

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

where $c=(c_0,c_1,\cdots,c_{n-1})$. It follows that a code $C\subseteq\mathbf{F}^n$ is θ-polycyclic with an associated vector $c\in\mathbf{F}^n$ if and only if for any $a\in C$, $\theta(a)D_c\in C$.

For a θ-polycyclic code $C=(g)_l/(f)$, if f satisfies the condition $\mathbf{F}[X;\theta]f=f\mathbf{F}[X;\theta]$, we can determine the generator matrix of C via the generator polynomial g.

Proposition 2. *Let C be a θ-polycyclic code corresponding to the left ideal generated by g in $\mathbf{F}[X;\theta]/(f)$ where $f=hg\in\mathbf{F}[X;\theta]$ and $\mathbf{F}[X;\theta]f=f\mathbf{F}[X;\theta]$. If $deg(f)=n$ and $g(X)=g_{n-k}X^{n-k}+\cdots+g_1X+g_0$ with $g_{n-k}\neq 0$, then C has the $k\times n$ generator matrix given by*

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ 0 & \theta(g_0) & \theta(g_1) & \cdots & \theta(g_{n-k}) & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ \vdots & & & & & & \vdots \\ 0 & \cdots & 0 & \theta^{k-1}(g_0) & \theta^{k-1}(g_1) & \cdots & \theta^{k-1}(g_{n-k}) \end{pmatrix}.$$

Proof. In $\mathbf{F}[X;\theta]/(f)$, $\{\overline{X^{k-1}g(X)},\cdots,\overline{Xg(X)},\overline{g(X)}\}$ generates C.
Next, suppose $\sum_{i=0}^{k-1} r_i\overline{X^ig(X)}=0$ in $\mathbf{F}[X;\theta]/(f)$.
We get $(\sum_{i=0}^{k-1} r_iX^i)g(X)\in\mathbf{F}[X;\theta]f$ by the condition $\mathbf{F}[X;\theta]f=f\mathbf{F}[X;\theta]$. Then we have $(\sum_{i=0}^{k-1} r_iX^i)g(X)=0$. Thus we get $r_0=r_1=\cdots=r_{n-r-1}=0$. Hence $\{\overline{X^{k-1}g(X)},\cdots,\overline{Xg(X)},\overline{g(X)}\}$ is a basis of C. For $l=0,1,2,\cdots,k-1$, $X^lg(X)=\theta^l(g_{n-k})X^{l+n-k}+\cdots+\theta^l(g_1)X^{l+1}+\theta^l(g_0)X^l$. Therefore we get the result. □

Definition 4. *Let $C\subseteq\mathbf{F}^n$ be a linear code. C is a θ-sequential code induced by c if there exists a vector $c=(c_0,c_1,\cdots,c_{n-1})\in\mathbf{F}^n$ such that for every $(a_0,a_1,\cdots,a_{n-1})\in C$,*

$$(\theta(a_1),\theta(a_2),\cdots,\theta(a_{n-1}),\theta(a_0)c_0+\theta(a_1)c_1+\cdots+\theta(a_{n-1})c_{n-1})\in C.$$

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

It follows that a code $C\subseteq\mathbf{F}^n$ is θ-sequential with an associated vector $c\in\mathbf{F}^n$ if and only if for any $a\in C$, ${D_c}^t\theta(a)\in C$.

Theorem 2. *For a code $C\subseteq\mathbf{F}^n$, we have the following assertions:*
(1) *If C is a θ-polycyclic code induced by c, then $C^\perp$ is a θ^{-1}-sequential code induced by $\theta^{-1}(c)$.*

(2) *If C is a θ-sequential code induced by c, then $C^{\perp}$ is a θ^{-1}-polycyclic code induced by $\theta^{-1}(c)$.*

Proof. (1) If C is a θ-polycyclic code induced by c, we have $\theta(a)D_c \in C$ for any $a \in C$. So, $\theta(a)D_c{}^t b = 0$ for any $b \in C^{\perp}$. By $\theta^{-1}(\theta(a)D_c{}^t b) = 0$, we have $aD_{\theta^{-1}(c)}{}^t\theta^{-1}(b) = 0$. Therefore $D_{\theta^{-1}(c)}{}^t\theta^{-1}(b) \in C^{\perp}$. Hence $C^{\perp}$ is a θ^{-1}-sequential code induced by $\theta^{-1}(c)$.
(2) It is proved analogously to use ${}^t D_c$ instead of D_c. □

3. Central θ-constacyclic codes

Let $C \subseteq \mathbf{F}^n$ be a θ-polycyclic code or a θ-sequential code induced by $c = (c_0, c_1, \cdots, c_{n-1})$. Then C is called a central code if $f(X) = X^n - c_{n-1}X^{n-1} - \cdots - c_1X - c_0 \in Z(\mathbf{F}[X;\theta])$.

A θ-polycyclic code is called a θ-constacyclic code if $C = (g)_l/(X^n - \alpha)$ for some $\alpha \neq 0$. A θ-constacyclic code is a θ-polycyclic code and is also a θ-sequential code.

Proposition 3. *For a code $C \subseteq \mathbf{F}^n$, C is a central θ-polycyclic code induced by c if and only if $C^{\perp}$ is a central θ^{-1}-sequential code induced by $\theta^{-1}(c)$.*

Proof. Suppose C is a central θ-polycyclic code induced by c. By $f(X) = X^n - c_{n-1}X^{n-1} - \cdots - c_1X - c_0 \in Z(\mathbf{F}[X;\theta])$, $X \cdot f(X) = f(X) \cdot X$ in $\mathbf{F}[X;\theta]$. Then we get $\theta(c_i) = c_i (0 \leq i \leq n-1)$. Thus we have $\theta^{-1}(c_i) = c_i$. Hence $C^{\perp}$ is a central θ^{-1}-sequential code induced by $\theta^{-1}(c)$.
Conversely if $C^{\perp}$ is a central θ^{-1}-sequential code, C is a central θ-polycyclic code, similarly. □

Proposition 4. *Let $C \subseteq \mathbf{F}^n$ be a θ-polycyclic code with a generator polynomial $g(X) = g_{n-k}X^{n-k} + \cdots + g_1X + g_0$. If C is a φ-sequential code for some automorphism φ, then $g_0 \neq 0$.*

Proof. Suppose $g_0 = 0$. Let $1 \leq i \leq n-k$ be the first i such that $g_i \neq 0$. Then we have $(0, \cdots, 0, g_i, \cdots, g_{n-k}, 0, \cdots, 0) \in C$. Since C is φ-sequential, we get $(g_i, \cdots, g_{n-k}, \cdots) \in C$. Then $g_i = 0$. This is a contradiction. □

Proposition 5. *If $h \cdot g \in Z(\mathbf{F}[X;\theta])$, then $h \cdot g = g \cdot h$ in $\mathbf{F}[X;\theta]$.*

Proof. Since $h \cdot g$ is a central element, we have $g \cdot (h \cdot g) = (h \cdot g) \cdot g$. Therefore $(g \cdot h - h \cdot g) \cdot g = 0$. Then we get $h \cdot g = g \cdot h$ in $\mathbf{F}[X;\theta]$. □

Theorem 3. *If $C = (g)_l/(X^n - \alpha)$ is a central θ-constacyclic code with $\alpha \neq 0$, then $C^{\perp}$ is also a central θ-constacyclic code.*

Proof. Let $\mathbf{F}[X, X^{-1};\theta]$ be a skew Laurent ring. Then we can define a map $\varphi : \mathbf{F}[X;\theta] \to \mathbf{F}[X, X^{-1};\theta]$ such that $\sum_{i=0}^{n} a_iX^i \mapsto \sum_{i=0}^{n} X^{-i}a_i$. For any $\xi, \eta \in \mathbf{F}[X;\theta]$, we get $\varphi(\xi + \eta) = \varphi(\xi) + \varphi(\eta)$ and $\varphi(\xi\eta) = \varphi(\eta)\varphi(\xi)$. Since $C = (g)_l/(X^n - \alpha)$ is central, we get $X^n - \alpha = h \cdot g = g \cdot h$ and $\theta(\alpha) = \alpha$. Therefore we have $X^k \cdot \varphi(h) \cdot \varphi(g) \cdot X^{n-k} = X^k \cdot \varphi(X^n - \alpha) \cdot X^{n-k} = 1 - \alpha X^n = (-\alpha) \cdot (X^n -$

α^{-1}). Then $X^k \cdot \varphi(h) = h_k + \theta(h_{k-1})X + \cdots + \theta^k(h_0)X^k$. Moreover $X^n - \alpha^{-1} \in Z(\mathbf{F}[X;\theta])$ and $g_0 \neq 0$. By Proposition 5, $\varphi(g) \cdot X^{n-k}(-\alpha^{-1}) \cdot X^k \cdot \varphi(h) = X^n - \alpha^{-1}$. Then we have $C^\perp = (g^\perp)_l/(X^n - \alpha^{-1})$ where $g^\perp = h_k + \theta(h_{k-1})X + \cdots + \theta^k(h_0)X^k$. Hence $C^\perp$ is θ-constacyclic. □

It is clear from Theorem 3 that, for a central θ-constacyclic code C, both C and $C^\perp$ are central θ-polycyclic codes.

Question 1. *Is C a central θ-constacyclic code if C and $C^\perp$ are central θ-polycyclic codes?*

We shall consider the condition in which the answer is affirmative.

Theorem 4. *For a central θ-polycyclic code $C \subseteq \mathbf{F}^n$ with a generator polynomial $g(X) = g_{n-k}X^{n-k} + \cdots + g_1X + g_0 (g_{n-k} \neq 0)$, if $C^\perp$ is also a central θ-polycyclic code with a generator polynomial $h(X) = h_kX^k + \cdots + h_1X + h_0 (h_k \neq 0)$ and satisfies the condition $g_0 g_{n-k}^{-1} \theta^{n-k}(h_0^{-1}) \theta^{n-k}(h_k) \in \mathbf{F}^\theta$, then $C = (g)_l/(X^n - \alpha)$ is a central θ-constacyclic code for some $\alpha \neq 0$.*

Proof. C and $C^\perp$ have generator matrices of the forms

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ 0 & \theta(g_0) & \theta(g_1) & \cdots & \theta(g_{n-k}) & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \theta^{k-1}(g_0) & \theta^{k-1}(g_1) & \cdots & \theta^{k-1}(g_{n-k}) \end{pmatrix}$$

and

$$H = \begin{pmatrix} h_0 & h_1 & \cdots & h_k & 0 & \cdots & 0 \\ 0 & \theta(h_0) & \theta(h_1) & \cdots & \theta(h_k) & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \theta^{n-k-1}(h_0) & \theta^{n-k-1}(h_1) & \cdots & \theta^{n-k-1}(h_k) \end{pmatrix}$$

respectively. Then, as $G^tH = 0$, we get $g(X)h(X) = g_{n-k}\theta^{n-k}(h_0)X^n + g_0\theta^{-k}(h_k)$ where $g(X) = \sum_{i=0}^{n-k} g_iX^i$ and $h(X) = \sum_{j=0}^{k} \theta^{-j}(h_j)X^{k-j}$. Since C is θ^{-1}-sequential, we get $g_0 \neq 0$ from Proposition 4. Similarly, $h_0 \neq 0$. Now let $c = (c_0, c_1, \cdots, c_{n-1})$ be an associated vector of C. By $f(X) = X^n - c_{n-1}X^{n-1} - \cdots - c_1X - c_0 \in Z(\mathbf{F}[X;\theta])$, $af(X) = f(X)a$ for any $a \in \mathbf{F}$. Thus θ^n is a identity map and $\theta^{-k} = \theta^{n-k}$. Therefore we have

$$g(X)h(X) = \{X^n + g_0\theta^{-k}(h_k)(\theta^{n-k}(h_0))^{-1}g_{n-k}^{-1}\}g_{n-k}\theta^{n-k}(h_0).$$

By $(\theta^{n-k}(h_0))^{-1} = \theta^{n-k}(h_0^{-1})$, $X^n + g_0\theta^{-k}(h_k)(\theta^{n-k}(h_0))^{-1}g_{n-k}^{-1}$ is central. Hence C is a central θ-constacyclic code. □

References

[1] S. Ikehata, On separable polynomials and Frobenius polynomials in skew polynomial rings, Math. J. Okayama. Univ. 22 (1980), 115-129.
[2] S. Ikehata, On H-separable and Galois polynomials of degree p in skew polynomial rings, International Mathematical Forum, 3, no. 32 (2008), 1581-1586.
[3] D. Boucher, W. Geiselmann and F. Ulmer, Skew cyclic codes, Applied Algebra in Engineering, Communication and Computing 18 (2007), 379-389.
[4] D. Boucher and P. Solé, Skew constacyclic codes over Galois rings, Advances in Mathematics of Communications, Volume 2, No.3 (2008), 273-292.
[5] K. R. Goodearl and R. B. Warfield, Jr., An Introduction to Noncommutative Noetherian Rings, Cambridge University Press, Cambridge, 1989.
[6] Xiang-dong Hou, S. R. López-Permouth and B. R. Parra-Avila, Rational power series, sequential codes and periodicity of sequences, J. Pure Appl. Algebra, 213 (2009), 1157-1169.
[7] 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.
[8] B. R. McDonald, Finite Rings with Identity, Pure and Applied Mathematics, Vol. 28, Marcel Dekker, Inc., New York, 1974.

Received: August, 2010