SUT Journal of Mathematics
Vol. 48, No. 1 (2012), 47–53

Polynomial realization of sequential codes over finite fields

Manabu Matsuoka

(Received April 5, 2011; Revised January 24, 2012)

Abstract. In this paper we study the relation between polycyclic codes and sequential codes over finite fields. It is shown that, for a sequential code $C \subseteq \mathbf{F}^n$, C is realized as an ideal in the quotient ring of the polynomial ring. Furthermore, we characterize the dual codes of polycyclic codes.

AMS 2010 *Mathematics Subject Classification.* Primary 94B60; Secondary 94B15, 16D25.

Key words and phrases. Polycyclic codes, sequential codes, finite fields.

§1. Introduction

In coding theory, a linear code of length n over a finite field $\mathbf{F}$ is a subspace C of the vector space $\mathbf{F}^n = \{(a_0, \cdots, a_{n-1}) | a_i \in \mathbf{F}\}$. A linear code $C \subseteq \mathbf{F}^n$ 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 generalized in several ways.

For a code $C \subseteq \mathbf{F}^n$, 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 $(a_0, a_1, \cdots, a_{n-1}) \in C$, $(a_1, a_2, \cdots, a_{n-1}, a_0c_0 + a_1c_1 + \cdots + a_{n-1}c_{n-1}) \in C$. S. R. López-Permouth, B. R. Parra-Avila and S. Szabo studied the duality between polycyclic codes and sequential codes in [2]. Polycyclic codes and sequential codes are generalized using skew polynomial rings. That is, θ-polycyclic codes and θ-sequential codes. The properties of them were considered in [3].

By the way, Y. Hirano characterized finite frobenius rings in [1]. And J. A. Wood establish the extension theorem and MacWilliams identities over finite frobenius rings in [5]. Polycyclic codes and sequential codes over finite commutative QF rings were considered in [4].

In this paper, we study the relation between polycyclic codes and sequential codes. And we realize sequential codes as ideals in quotient rings of polynomial rings. In section 2 we review properties of polycyclic codes and sequential codes over finite field. In section 3 we prove that, for a polycyclic code C, its dual $C^\perp$ is realized as an ideal in the quotient ring of the polynomial ring.

Throughout this paper, $\mathbf{F}$ denotes a finite field with $1 \neq 0$, n denotes a natural number with $n \geq 2$, (g) denotes an ideal generated by $g \in \mathbf{F}[X]$, unless otherwise stated.

§2. Polycyclic codes and sequential codes

A linear $[n,k]$-code over a finite field $\mathbf{F}$ is a k-dimensional subspace $C \subseteq \mathbf{F}^n$. We define polycyclic codes over a finite field.

Definition 1. *Let C be a linear code of length n over $\mathbf{F}$. C is a (right) 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 $(a_0, a_1, \cdots, a_{n-1}) \in C$,*

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

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 $c = (c_0, c_1, \cdots, c_{n-1}) \in \mathbf{F}^n$, 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 $\rho : \mathbf{F}^n \to \mathbf{F}[X]/(f(X))$ 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 polycyclic codes induced by c with the left ideal of $\mathbf{F}[X]/(f(X))$.

Let C be a polycyclic code in $\mathbf{F}[X]/(f(X))$. Then there exists monic polynomials g and h such that $C = (g)/(f)$ and $f = hg$.

Proposition 1. *A code $C \subseteq \mathbf{F}^n$ is a polycyclic code induced by some $c \in C$ if and only if it 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 $g_{n-k} \neq 0$. In this case $\rho(C) = \left(\overline{g_{n-k}X^{n-k} + \cdots + g_1X + g_0}\right)$ is an ideal of $\mathbf{F}[X]/(f(X))$.

Proof. See [2, Theorem 2.3]. □

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

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

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

Next we define a sequential code.

Definition 2. *Let C be a linear code of length n over $\mathbf{F}$. C is a (right) 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 $(a_0, a_1, \cdots, a_{n-1}) \in C$,*

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

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

Let $c = (c_0, c_1, \cdots, c_{n-1}) \in \mathbf{F}^n$. Then, a code $C \subseteq \mathbf{F}^n$ is sequential with an associated vector $c \in \mathbf{F}^n$ if and only if it is invariant under right multiplication by the matrix

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

On $\mathbf{F}^n$ define the standard inner product by

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

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

The orthogonal of a linear code C is defined by

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

It is well-known that $dim C^{\perp} = n - dim C$.

Proposition 2. *Let C be a linear code of length n. Then C is a polycyclic (sequential) code if and only if $C^{\perp}$ is a sequential (polycyclic) code.*

Proof. See [2, Theorem 3.2]. □

§3. Polynomial realization of sequential codes

We define $\mathbf{F}$-linear isomorphism $\tau : \mathbf{F}^n \to \mathbf{F}[X]/(X^n - c_{n-1}X^{n-1} - \cdots - c_0)$ sending $(a_0, a_1, \cdots, a_{n-1})$ to $\overline{b_{n-1}X^{n-1} + \cdots + b_1X + b_0}$ where $b_i = a_{n-i-1} - a_{n-i-2}c_{n-1} - a_{n-i-3}c_{n-2} - \cdots - a_0c_{i+1}$, $(i = 0, 1, \cdots, n-2)$ and $b_{n-1} = a_0$.

Theorem 1. *If C is a sequential code induced by c, then $\tau(C)$ is an ideal of $\mathbf{F}[X]/(X^n - c_{n-1}X^{n-1} - \cdots - c_0)$.*

Proof. For any $a \in C$, we can get
$X\tau(a) = \overline{b_{n-1}X^n + b_{n-2}X^{n-1} + \cdots + b_1X^2 + b_0X}$
$= \overline{(b_{n-2} + b_{n-1}c_{n-1})X^{n-1} + \cdots + (b_1 + b_{n-1}c_2)X^2 + (b_0 + b_{n-1}c_1)X + b_{n-1}c_0}$
$= \tau(a^tD) \in \tau(C)$,
directly. So $\tau(C)$ is an ideal of $\mathbf{F}[X]/(X^n - c_{n-1}X^{n-1} - \cdots - c_0)$. □

By Theorem 1, we get the following corollary.

Corollary 1. *For a sequential code $C \subseteq \mathbf{F}^n$, there exists monic polynomials g and h in $\mathbf{F}[X]$ such that $\tau(C) = (g)/(f)$ and $f = hg$.*

Example 1. *For $n = 5$, let $f(X) = X^5 - c_4X^4 - c_3X^3 - c_2X^2 - c_1X - c_0$. $\tau : \mathbf{F}^5 \to \mathbf{F}[X]/(f(X))$ sending $(a_0, a_1, a_2, a_3, a_4)$ to $b_4X^4 + b_3X^3 + b_2X^2 + b_1X + b_0$, where*
$b_4 = a_0,$
$b_3 = a_1 - a_0c_4,$
$b_2 = a_2 - a_1c_4 - a_0c_3,$
$b_1 = a_3 - a_2c_4 - a_1c_3 - a_0c_2,$
$b_0 = a_4 - a_3c_4 - a_2c_3 - a_1c_2 - a_0c_1.$
For a sequential code $C \subseteq \mathbf{F}^5$, $\tau(C)$ is an ideal of $\mathbf{F}[X]/(f(X))$.

Lemma 3. *For given $c_1, \cdots, c_{n-1} \in \mathbf{F}$,*
Put $d_k = \sum_{m=1}^{k} \sum_{l_1+\cdots+l_m=k} c_{n-l_1}c_{n-l_2}\cdots c_{n-l_m}$, $(1 \le k \le n-1)$.
Then $d_k = c_{n-k} + c_{n-k+1}d_1 + c_{n-k+2}d_2 + \cdots + c_{n-1}d_{k-1}$, $(2 \le k \le n-1)$.

Proof.
$$\begin{aligned} d_k &= \sum_{m=1}^{k} \sum_{l_1+\cdots+l_m=k} c_{n-l_1}c_{n-l_2}\cdots c_{n-l_m} \\ &= c_{n-k} + c_{n-k+1}\sum_{l_1=1} c_{n-l_1} + c_{n-k+2}\sum_{m=1}^{2} \sum_{l_1+\cdots+l_m=2} (c_{n-l_1}\cdots c_{n-l_m}) + \cdots \\ &\quad \cdots + c_{n-1}\sum_{m=1}^{k-1} \sum_{l_1+\cdots+l_m=k-1} (c_{n-l_1}\cdots c_{n-l_m}) \\ &= c_{n-k} + c_{n-k+1}d_1 + c_{n-k+2}d_2 + \cdots + c_{n-1}d_{k-1}, \ (2 \le k \le n-1). \end{aligned}$$
□

Example 2. *For given* $c_1, \cdots, c_{n-1} \in \mathbf{F}$,
$d_1 = c_{n-1}$,
$d_2 = c_{n-2} + c_{n-1}^2$,
$d_3 = c_{n-3} + c_{n-2}c_{n-1} + c_{n-1}c_{n-2} + c_{n-1}^3$
$\quad = c_{n-3} + 2c_{n-2}c_{n-1} + c_{n-1}^3$,
$d_4 = c_{n-4} + c_{n-3}c_{n-1} + c_{n-2}c_{n-2} + c_{n-1}c_{n-3} + c_{n-2}c_{n-1}^2 + c_{n-1}c_{n-2}c_{n-1}$
$\quad + c_{n-1}^2 c_{n-2} + c_{n-1}^4$
$\quad = c_{n-4} + 2c_{n-3}c_{n-1} + c_{n-2}^2 + 3c_{n-2}c_{n-1}^2 + c_{n-1}^4$.

For given $c_1, \cdots, c_{n-1} \in \mathbf{F}$, let M be the following square matrix

$$M = \begin{pmatrix} -c_1 & -c_2 & -c_3 & \cdots & -c_{n-1} & 1 \\ -c_2 & -c_3 & & & 1 & 0 \\ -c_3 & & & \cdots & & \vdots \\ \vdots & & \cdots & & & \vdots \\ -c_{n-1} & 1 & 0 & \cdots & & \vdots \\ 1 & 0 & \cdots & \cdots & \cdots & 0 \end{pmatrix}.$$

Lemma 4. *For any* $c_1, \cdots, c_{n-1} \in \mathbf{F}$, M^{-1} *is given by the following matrix*

$$M^{-1} = \begin{pmatrix} 0 & \cdots & \cdots & \cdots & 0 & 1 \\ \vdots & & & 0 & 1 & d_1 \\ \vdots & & \cdots & 1 & d_1 & d_2 \\ \vdots & & \cdots & \cdots & & \vdots \\ 0 & 1 & d_1 & & & \vdots \\ 1 & d_1 & d_2 & \cdots & \cdots & d_{n-1} \end{pmatrix}$$

where $d_k = \sum_{m=1}^{k} \sum_{l_1+\cdots+l_m=k} c_{n-l_1}c_{n-l_2}\cdots c_{n-l_m}$, $(1 \leq k \leq n-1)$.

Proof. Put

$$\begin{pmatrix} -c_1 & -c_2 & \cdots & -c_{n-1} & 1 \\ -c_2 & -c_3 & & 1 & 0 \\ -c_3 & & \cdots & & \vdots \\ \vdots & \cdots & & & \vdots \\ -c_{n-1} & 1 & \cdots & & \vdots \\ 1 & 0 & \cdots & \cdots & 0 \end{pmatrix} \begin{pmatrix} 0 & \cdots & \cdots & 0 & 1 \\ \vdots & & \cdots & 1 & d_1 \\ \vdots & \cdots & \cdots & d_1 & d_2 \\ \vdots & \cdots & \cdots & & \vdots \\ 0 & 1 & & & \vdots \\ 1 & d_1 & \cdots & \cdots & d_{n-1} \end{pmatrix} = (m_{ij}).$$

It is clear that $m_{11} = \cdots = m_{nn} = 1$ and $m_{ij} = 0$, $(i > j)$. By Lemma 3, $m_{ij} = -c_{n-j+i} - c_{n-j+i+1}d_1 - c_{n-j+i+2}d_2 - \cdots - c_{n-1}d_{j-i-1} + d_{j-i} = 0, (i < j)$. □

Finally, we characterize the dual code $C^{\perp}$ of a polycyclic code C.

Theorem 2. *Let $C \subseteq \mathbf{F}^n$ be a polycyclic code corresponding to $(g)/(f) \subseteq \mathbf{F}[X]/(f(X))$ via ρ where $f = hg$. Then $C^{\perp}$ is a sequential code such that $\tau(C^{\perp}) = (h)/(f)$.*

Proof. Put $f(X) = X^n - c_{n-1}X^{n-1} - \cdots - c_1X - c_0$, $h(X) = h_kX^k + \cdots + h_1X + h_0$ and $g(X) = g_{n-k}X^{n-k} + \cdots + g_1X + g_0$, where $g_{n-k} \neq 0$ and $h_k \neq 0$. Let E be a linear subspace generated by $\{\overline{h}, \overline{Xh}, \cdots, \overline{X_{n-k-1}h}\}$ in $\mathbf{F}[X]/(f(X))$. Suppose $\tau(a_0, \cdots, a_{n-1}) = \overline{b_{n-1}X^{n-1} + \cdots + b_1X + b_0}$. Then $(b_0, \cdots, b_{n-1}) = M(a_0, \cdots, a_{n-1})$. By $c_u = \sum_{s+t=u} g_sh_t$, we have

$$< \rho^{-1}(X^ig), \tau^{-1}(X^jh) >$$
$$=< X^ig, M^{-1}(X^jh) >$$
$$= -c_{n-i-j-1} - c_{n-i-j}d_1 - c_{n-i-j+1}d_2 - \cdots - c_{n-1}d_{i+j} + d_{i+j+1}.$$

Then we get $< \rho^{-1}(X^ig), \tau^{-1}(X^jh) >= 0$ by Lemma 3. Therefore $E \subseteq C^{\perp}$. Since E and $C^{\perp}$ are the same dimension $n - k$ and $\mathbf{F}$ is a finite field, we get $E = C^{\perp}$. □

By Theorem 2, for a polycyclic code C, $C^{\perp}$ is represented by $C^{\perp} = \tau^{-1}((h)/(f))$.

In coding theory, the Hamming distance is very important. Thus we have the following problem.

Problem 1. *Study the relation of the Hamming distance between C and $\tau(C)$ for a sequential code C.*

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

References

[1] Y. Hirano, *On admissible rings*, Indagationes Mathematicae, Volume 8, Issue 1 (1997), 55-59.

[2] 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, Number 3 (2009), 227-234.

[3] M. Matsuoka, *θ-polycyclic codes and θ-sequential codes over finite fields*, International Journal of Algebra, Volume 5, Number 2 (2011), 65-70.

[4] 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.

[5] J. A. Wood, *Duality for modules over finite rings and applications to coding theory*, American Journal of Mathematics, Volume 121 (1999), 555-575.

Manabu Matsuoka
Kuwanakita-Highschool
2527 Shimofukayabe Kuwana Mie 511-0808, JAPAN
E-mail: e-white@hotmail.co.jp