(θ, δ)-CODES WITH SKEW POLYNOMIAL RINGS

MANABU MATSUOKA

Abstract. In this paper we generalize coding theory of cyclic codes over finite fields to skew polynomial rings over finite rings. Codes that are principal ideals in quotient rings of skew polynomial rings by two sided ideals are studied. Next we consider skew codes of endomorphism type and derivation type. And we give some examples.

Key Words: Finite rings, (θ, δ)-codes, Skew polynomial rings.

2000 *Mathematics Subject Classification*: Primary 94B60; Secondary 94B15, 16D25.

1. Introduction

Let $\mathbf{F}$ be a finite field. A linear $[n, k]$-code over $\mathbf{F}$ is a k-dimensional subspace C of the vector space $\mathbf{F}^n = \{(a_0, \cdots, a_{n-1}) \mid a_i \in \mathbf{F}\}$. We use polynomial representation of the code C, where we identify code words $(a_0, \cdots, a_{n-1}) \in C$ with coefficient tuples of polynomials $a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbf{F}[X]$. Those polynomials can also be seen as elements of a quotient ring $\mathbf{F}[X]/(f)$ where f is a polynomial of degree n.

D. Boucher, W. Geiselmann and F. Ulmer [3] generalized the notion of codes to skew polynomial rings. In [4], D. Boucher and P. Solé studied skew constacyclic codes. They considered skew polynomial rings over Galois rings. In this paper, we generalize the result of [4] to codes with (θ, δ)-type skew polynomial rings $R[X; \theta, \delta]$. We study mathematical aspects of coding theory with skew polynomial rings over finite rings.

Let R be a ring and θ be an endomorphism of R. A θ-derivation of R is an additive map $\delta : R \to R$ such that $\delta(rs) = \theta(r)\delta(s) + \delta(r)s$ for all r, $s \in R$. Throughout this paper, R represents a finite ring with $1 \neq 0$, θ an endomorphism of R with $\theta(1) = 1$ and δ a θ-derivation of R, unless otherwise stated.

We shall use the following conventions:

$Z(R[X; \theta, \delta])$ is the center of $R[X; \theta, \delta]$.
$(g)_l$ is the left ideal generated by $g \in R[X; \theta, \delta]$.
(g) is the two-sided ideal generated by $g \in R[X; \theta, \delta]$.
$R^\theta = \{r \in R \mid \theta(r) = r\}$.
$R^\delta = \{r \in R \mid \delta(r) = 0\}$, $Z^\delta = \{r \in Z \mid \delta(r) = 0\}$, where Z is the center of R.

2. Skew (θ, δ)-codes over finite rings

In this section, we define (θ, δ)-codes and study some properties of them.

Definition 1. Let R be a ring, θ be an endomorphism of R, δ be a θ-derivation of R. Suppose S is a free left R-module with basis 1, X, X^2, $\cdots$ and give a multiplication from

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

the rules $X^iX^j = X^{i+j}$ and $Xr = \theta(r)X + \delta(r)$ for all $r \in R$. The ring S constructed in this way is denoted by $R[X;\theta,\delta]$ and is called a *skew polynomial ring*.

Proposition 2. *For any h, $g \in R[X;\theta,\delta]$, if the leading coefficients of g is invertible, then* $\deg(h{\cdot}g) = \deg(h) + \deg(g)$.

Proof. Straightforward. □

Proposition 3. *Let $h{\cdot}g \in Z(R[X;\theta,\delta])$. If the leading coefficient of g is invertible, then $h{\cdot}g = g{\cdot}h$ in $R[X;\theta,\delta]$.*

Proof. Straightforward. □

Proposition 4. *Let R be a ring, θ be an endomorphism of R, δ be a θ-derivation of R. For any f, $g \in R[X;\theta,\delta]$, if the leading coefficient of f is invertible, then 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 5. Let R be a finite ring, θ be an endomorphism of R, δ be a θ-derivation of R. Suppose $f \in R[X;\theta,\delta]$ is a nonzero polynomial with an invertible leading coefficient. Then, by Proposition 4, $R[X;\theta,\delta]/(f)$ is a finite ring and a left ideal of $R[X;\theta,\delta]/(f)$ is called a *skew (θ,δ)-code*.

A skew (θ,δ)-code is called an *$[n,k]$-code* if the degree of f and the rank of C as a free left R-module are n and k, respectively. If $f \in Z(R[X;\theta,\delta])$, then we call a skew (θ,δ)-code corresponding to a left ideal of $R[X;\theta,\delta]/(f)$ a *central (θ,δ)-code*.

We shall consider skew codes under the condition $R[X;\theta,\delta]f = fR[X;\theta,\delta]$, which is a weaker condition than $f \in Z(R[X;\theta,\delta])$.

Note that not all left ideals in $R[X;\theta,\delta]/(f)$ are principal, but in the following we will focus on those ideals.

Definition 6. A *(θ,δ)-principal code* is a skew (θ,δ)-code corresponding to a left ideal $(g)_l/(f)$ where $(g)_l$ is a left ideal generated by g and $hg = f$ for some h. A *(θ,δ)-cyclic code* is a (θ,δ)-principal code corresponding to a left ideal $(g)_l/(X^n - 1)$.

In what follows, for a code $C = (g)_l/(f)$, we assume that $n = \deg(f) \geq 2$.

Proposition 7. *If C is a (θ,δ)-cyclic code, then $(a_0, a_1, \cdots, a_{n-1}) \in C$ implies $(\theta(a_{n-1}) + \delta(a_0), \theta(a_0) + \delta(a_1), \theta(a_1) + \delta(a_2), \cdots, \theta(a_{n-2}) + \delta(a_{n-1})) \in C$.*

Proof. Straightforward. □

A ring R is said to be *Dedekind finite* if $ab = 1$ implies $ba = 1$ (a, $b \in R$). It is well-known that a finite ring is Dedekind finite.

Theorem 8. *Let $C = (g)_l/(f)$ be a skew code in $R[X;\theta,\delta]/(f)$ and $f = hg$. Suppose that the leading coefficients of f and g are invertible. If f satisfies the condition $R[X;\theta,\delta]f = fR[X;\theta,\delta]$, then C is a free left R-module and* $\operatorname{rank} C = \deg(f) - \deg(g)$.

Example 9. Let C be a (θ,δ)-code corresponding to a left ideal generated by g in $R[X;\theta,\delta]/(f)$ and $R[X;\theta,\delta]f = fR[X;\theta,\delta]$. Suppose that $\deg(f) = 4$ and $g = g_1X + g_0$. Then the generator matrix of C is given by

$$\begin{pmatrix} g_0 & g_1 & 0 & 0 \\ \delta(g_0) & \theta(g_0)+\delta(g_1) & \theta(g_1) & 0 \\ \delta^2(g_0) & (\theta\delta+\delta\theta)(g_0)+\delta^2(g_1) & \theta^2(g_0)+(\theta\delta+\delta\theta)(g_1) & \theta^2(g_1) \end{pmatrix}.$$

Lemma 10. *Let $C=(g)_l/(f)$ be a skew code in $R[X;\theta,\delta]/(f)$ and $f=hg=gh$. Suppose that the leading coefficient of h is invertible and $R[X;\theta,\delta]f=fR[X;\theta,\delta]$. Then $\overline{a}\in C$ if and only if $\overline{a}\,\overline{h}=0$ in $R[X;\theta,\delta]/(f)$.*

For any subset $T\subseteq R$, the left annihilator of T is the set

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

which is a left ideal of R. The right annihilator $r.ann_R(T)$ is defined, similarly.

Then we can get the following corollary.

Corollary 11. *Let $C=(g)_l/(f)$ be a skew code in $\overline{R}=R[X;\theta,\delta]/(f)$ and $f=hg=gh$. Suppose that the leading coefficient of h is invertible and $R[X;\theta,\delta]f=fR[X;\theta,\delta]$. Then we have $C=l.ann_{\overline{R}}\left(\overline{h}\right)$.*

3. Skew codes of endomorphism type and derivation type

First we study skew codes of endomorphism type, i.e., skew $(\theta,0)$-codes.

Proposition 12. *Let $C=(g)_l/(f)$ be a skew code in $R[X;\theta]/(f)$ and $f=hg$. Suppose that the leading coefficients of f and g are invertible and $R[X;\theta]f=fR[X;\theta]$. If $\deg(f)=n$ and $g=g_{n-k}X^{n-k}+g_{n-k-1}X^{n-k-1}+\cdots+g_1X+g_0$, then C is a free R-module and has the $k\times n$ generator matrix given by*

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

We study constacyclic codes and determine their parity check matrix.

Proposition 13. *Suppose that R is a finite commutative ring, $X^n-\alpha=f=h\cdot g\in Z(R[X;\theta])$ and the leading coefficient of g is invertible. Let C denote the $(\theta,0)$-code corresponding to the left ideal generated by g in $R[X;\theta]/(X^n-\alpha)$. Denote by $h=h_kX^k+h_{k-1}X^{k-1}+\cdots+h_1X+h_0$. If the dual code $C^\perp$ is a free R-module and $\operatorname{rank}C^\perp=n-k$, then C has the following $(n-k)\times n$ parity check matrix given by*

$$\begin{pmatrix} h_k & \cdots & \theta^{k-1}(h_1) & \theta^k(h_0) & 0 & \cdots & 0 \\ 0 & \theta(h_k) & \cdots & \theta^k(h_1) & \theta^{k+1}(h_0) & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ \vdots & & & & & & \vdots \\ 0 & \cdots & 0 & \theta^{n-k-1}(h_k) & \cdots & \theta^{n-2}(h_1) & \theta^{n-1}(h_0) \end{pmatrix}.$$

Theorem 14. *Suppose that R is a finite commutative ring, θ is an automorphism and $X^n-\alpha=h\cdot g\in Z(R[X;\theta])$ with $\alpha\in R^\theta$ and $\alpha^2=1$. Let C denote the central $(\theta,0)$-code corresponding to the left ideal generated by g in $R[X;\theta]/(X^n-\alpha)$ where the leading*

coefficient of g is invertible. Denote by $h = h_kX^k + h_{k-1}X^{k-1} + \cdots + h_1X + h_0$. If the dual code $C^\perp$ is a free left R-module and $\operatorname{rank} C^\perp = n - k$*, then the dual of the θ-constacyclic code $(g)/(X^n - \alpha)$ is the θ-constacyclic code $(g^\perp)/(X^n - \alpha)$ where*

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

Next we consider skew codes of derivation type, i.e., skew $(1, \delta)$-codes, and give some examples.

Lemma 15. *Let f be in $R[X; \delta]$. Then the following conditions are equivalent:*
(1) *f satisfies the condition $R[X; \delta]f = fR[X; \delta]$.*
(2) *f is central, that is, $f \in Z(R[X; \delta])$.*

Proof. See the proof of [1, Lemma 1.6]. □

Lemma 16. *Assume that R is a finite ring of prime characteristic p and Z is the center of R. Let $f = X^p + aX + b$ be in $R[X; \delta]$. Then f satisfies the condition $R[X; \delta]f = fR[X; \delta]$ if and only if*
(a) *$a \in Z^\delta$ and $b \in R^\delta$,*
(b) *$\delta^p(r) + a\delta(r) = rb - br$ for any $r \in R$.*

Proof. See [2, Lemma 2.1]. □

In $R[X; \delta]$, we have $X^l r = \sum_{i=0}^{l} \binom{l}{i} \delta^{l-i}(r)X^i$ for $r \in R$. So we can calculate a generator matrix for a given polynomial $g = g_{n-k}X^{n-k} + g_{n-k-1}X^{n-k-1} + \cdots + g_1X + g_0$.

Now we give some examples of skew codes of derivation type $R[X; \delta]$. Let $Z_p = Z/pZ$ be a finite field of p elements and let

$$R_{(p)} = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in M_2(Z_p) \;\middle|\; a, b \in Z_p \right\}.$$

Then $R_{(p)}$ is a finite commutative local ring with the unique maximal ideal

$$M = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \in M_2(Z_p) \;\middle|\; b \in Z_p \right\}.$$

Now we can define a derivation $\delta : R_{(p)} \to R_{(p)}$ by $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mapsto \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$. Therefore we can consider a skew polynomial ring of derivation type $R_{(p)}[X; \delta]$.

Example 17. We consider the skew polynomial ring of derivation type $R_{(3)}[X; \delta]$. Let $f = X^3 + 2X$. By Lemma 16, f satisfies the condition $R_{(3)}[X; \delta]f = fR_{(3)}[X; \delta]$. Put $g = X + 2\beta$ and $h = X^2 + \beta X + \alpha$, where $\alpha = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $\beta = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. We get the following factorizations:

$$X^3 + 2X = (X + 2\beta)(X^2 + \beta X + \alpha) = (X^2 + \beta X + \alpha)(X + 2\beta).$$

Then $(g)_l/(f)$ is a $[3, 2]$ skew δ-code.

Let $S_{(p)} = M_2(R_{(p)})$ and define a derivation $\Delta : M_2(R_{(p)}) \to M_2(R_{(p)})$ by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} \delta(a) & \delta(b) \\ \delta(c) & \delta(d) \end{pmatrix}$. Then we can consider a skew polynomial ring of derivation type $S_{(p)}[Y; \Delta]$.

Example 18. We consider the skew polynomial ring of derivation type $S_{(3)}[Y;\Delta]$. Let $f = Y^3 + 2Y$. By Lemma 16, f satisfies the condition $S_{(3)}[Y;\Delta]f = fS_{(3)}[Y;\Delta]$. Put $g = Y + 2\beta$ and $h = Y^2 + \beta Y + \alpha$. We get the following factorizations:

$$Y^3 + 2Y = (Y + 2\beta)(Y^2 + \beta Y + \alpha) = (Y^2 + \beta Y + \alpha)(Y + 2\beta).$$

Then $(g)_l/(f)$ is a $[3, 2]$ skew Δ-code. So the factorizations of $R_{(3)}[X;\delta]$ is lifted to $S_{(3)}[Y;\Delta]$.

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**(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 **2**(3) (2008), 273–292.

[5] D. Boucher and F. Ulmer, *Codes as modules over skew polynomial rings*, Proceedings of the 12th IMA conference on Cryptography and Coding, Cirencester, Lecture Notes in Computer Science 5921, pp. 38–55, 2009.

[6] K. R. Goodearl and R. B. Warfield, Jr., *An Introduction to Noncommutative Noetherian Rings*, Cambridge University Press, Cambridge, 1989.

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

Yokkaichi-Highscool
4-1-43 Tomida Yokkaichi Mie 510-8510 Japan
E-mail address: e-white@hotmail.co.jp