Mathematical Aspects of \((\theta, \delta)-\)Codes
with Skew Polynomial Rings

Manabu Matsuoka

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 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.

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

Keywords: finite rings, \((\theta, \delta)-\)codes, skew polynomial rings

1. Introduction

Let \(F\) be a finite field. A linear \([n, k]-\)code over \(F\) is a \(k\)-dimensional subspace \(C\) of the vector space \(F^n = \{(a_0, \ldots, a_{n-1})|a_i \in F\}\). We use polynomial representation of the code \(C\), where we identify code words \((a_0, \ldots, a_{n-1}) \in C\) with coefficient tuples of polynomials \(a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in F[X]\). Those polynomials can also be seen as elements of a quotient ring \(F[X]/(f)\) 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 \((\theta, \delta)-\)type skew polynomial rings \(R[X; \theta, \delta]\). We study mathematical aspects of coding theory with skew polynomial rings over finite rings.
In section 2 we review the definition of skew polynomial rings. Complete treatment of this rings can be found in [6] and [7]. Next we define skew codes and generalize coding theory to the skew polynomial rings $R[X; \theta, \delta]$. In section 3 we study skew codes of endomorphism type $R[X; \theta]$ and derivation type $R[X; \delta]$. And we give some examples.

Let $R$ be a ring and $\theta$ be an endomorphism of $R$. A $\theta$-derivation of $R$ is an additive map $\delta : R \rightarrow R$ 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 $1 \neq 0$, $\theta$ an endomorphism of $R$ with $\theta(1) = 1$ and $\delta$ a $\theta$-derivation of $R$, unless otherwise stated.

We shall use the following conventions:

- $R[X; \theta, \delta]_{(c)} = \{ f \in R[X; \theta, \delta] | R[X; \theta, \delta]f = fR[X; \theta, \delta] \}$.
- $Z(R[X; \theta, \delta])$ 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 $g \in R[X; \theta, \delta]$.
- $R^\delta = \{ r \in R | \theta(r) = r \}$.
- $R^\delta = \{ r \in R | \delta(r) = 0 \}$, $Z^\delta = \{ r \in Z | \delta(r) = 0 \}$, where $Z$ is the center of $R$.

2. Skew $(\theta, \delta)$-codes over finite rings

In this section, we define $(\theta, \delta)$-codes and study some properties of them.

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

**Proposition 2.** 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. \qed

**Proposition 3.** Let $R$ be a ring, $\theta$ be an endomorphism of $R$, $\delta$ be a $\theta$-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. \qed
Definition 2. Let $R$ be a finite ring, $\theta$ be an endomorphism of $R$, $\delta$ be a $\theta$-derivation of $R$. Suppose $f \in R[X; \theta, \delta]$ is a nonzero polynomial with an invertible leading coefficient. Then, by Proposition 3, $R[X; \theta, \delta]/(f)$ is a finite ring and a left ideal of $R[X; \theta, \delta]/(f)$ is called a skew $(\theta, \delta)$-code.

A skew $(\theta, \delta)$-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 $(\theta, \delta)$-code corresponding to a left ideal of $R[X; \theta, \delta]/(f)$ a central $(\theta, \delta)$-code.

We shall consider skew codes under the condition $R[X; \theta, \delta]/(f)$ are principal, but in the following we will focus on those ideals.

Definition 3. A $(\theta, \delta)$-principal code is a skew $(\theta, \delta)$-code corresponding to a left ideal $(g)_i/(f)$ where $(g)_i$ is a left ideal generated by $g$ and $hg = f$ for some $h$. A $(\theta, \delta)$-cyclic code is a $(\theta, \delta)$-principal code corresponding to a left ideal $(g)_i/(X^n - 1)$.

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

Proposition 4. If $C$ is a $(\theta, \delta)$-cyclic code, then $(a_0, a_1, \ldots, a_{n-1}) \in C$ implies

$$(\theta(a_{n-1}) + \delta(a_0), \theta(a_0) + \delta(a_1), \theta(a_1) + \delta(a_2), \ldots, \theta(a_{n-2}) + \delta(a_{n-1})) \in C.$$

Proof. Straightforward. \hfill \Box

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 1. Let $C = (g)_i/(f)$ 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 $R[X; \theta, \delta]/(f)$ is a free left $R$-module and $\text{rank } C = \deg(f) - \deg(g)$.

Proof. Put $n = \deg(f)$ and $r = \deg(g)$. Let leading coefficients of $g$ and $h$ are $b$ and $c$, respectively. Since $b$ is invertible, we get $\theta(b) \neq 0$ and $c^\theta \delta^g(b)(b) \neq 0$. Since the leading coefficient of $f$ is invertible and $R$ is Dedekind-finite, $c$ is invertible and $\deg(h) = n - r$. This implies $\{X^{n-r-1}g(X), \ldots, Xg(X), g(X)\}$ generates $C$ by Proposition 3. Suppose $\sum_{i=0}^{n-r-1} r_i X^i g(X) = 0$ in $R[X; \theta, \delta]/(f)$. We get $(\sum_{i=0}^{n-r-1} r_i X^i)g(X) \in R[X; \theta, \delta]/(f)$ by $f \in R[X; \theta, \delta]$. Then we have $(\sum_{i=0}^{n-r-1} r_i X^i)g(X) = 0$. Since the leading coefficient of $g$ is invertible, we get $r_0 = r_1 = \cdots = r_{n-r-1} = 0$. Hence $\{X^{n-r-1}g(X), \ldots, Xg(X), g(X)\}$ is a basis of $C$. \hfill \Box
Example 1. Let $C$ be a $(\theta, \delta)$-code corresponding to a left ideal generated by $g$ in $R[X; \theta, \delta]/(f)$ and $R[X; \theta, \delta]f = fR[X; \theta, \delta]$. Denote $\deg(f) = 4$ and $g(X) = g_1X + g_0$. Then the generator matrix $G$ of $C$ is given by

$$
\left(\begin{array}{ccc}
g_0 & g_1 & 0 \\
\delta(g_0) & \theta(g_0 + \delta(g_1)) & \theta(g_1) \\
\delta^2(g_0) & (\theta \delta + \delta \theta)(g_0) + \delta^2(g_1) & \theta^2(g_0) + (\theta \delta + \delta \theta)(g_1)
\end{array}\right).
$$

Definition 4. An element $P \in R[X; \theta, \delta]$ is bounded if the left ideal $(P)_l$ contains a two-sided ideal $(P^*)$. In this case $P^*$ is called a bound for $P$.

For a given $P \in R[X; \theta, \delta]$, if there exist polynomials $P^*, Q$ such that $P^* = QP$ and $R[X; \theta, \delta]P^* = P^*R[X; \theta, \delta]$, then $P^*$ is a bound for $P$.

Proposition 5. A ring extension $R$ of $R^\theta$ is of degree $l$ and $R^\theta[x^m] \subseteq R[X; \theta, \delta]_{(c)}$. If $P \in R[X; \theta, \delta]$ is of degree $n$ with an invertible leading coefficient, then there exists a bound $P^*$ for $P$ of degree at most $l \cdot n \cdot m$.

Proof. The elements in $R[X; \theta, \delta]$ of degree less than $n$ form a free $R$-module of rank $n$ and therefore a free $R^\theta$-module of rank $ln$. Considering the remainders of the division

$$X^{im} = Q_i \cdot P + R_i, \quad (i = 0, 1, \cdots, ln)$$

with degree $\deg(R_i) < n$, there exists a non-trivial linear combination $\sum_{i=0}^{ln} c_i R_i = 0$ where $c_i \in R^\theta$. This shows that

$$\sum_{i=0}^{ln} c_i X^{im} = (\sum_{i=0}^{ln} c_i Q_i) \cdot P$$

By the condition $R^\theta[x^m] \subseteq R[X; \theta, \delta]_{(c)}$, the polynomial $\sum_{i=0}^{ln} c_i X^{im}$ is a bound for $P$. \hfill \Box

Lemma 1. Let $C = (g)/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 $\overline{ah} = 0$ in $R[X; \theta, \delta]/(f)$.

Proof. If $a \in C$, then $a = \varphi g$ in $R[X; \theta, \delta]/(f)$. Therefore we get $ah = \varphi gh = \varphi f = 0$ in $R[X; \theta, \delta]/(f)$. Conversely, if $ah = 0$ in $R[X; \theta, \delta]/(f)$, then $ah = \psi f = \psi hg = \psi gh$ in $R[X; \theta, \delta]$. By the leading coefficient of $h$ is invertible, $h$ is a right cancellator. Hence we obtain $a = \psi g$, showing that $a \in C$. \hfill \Box

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

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

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 1. Let \( C = (g)/(f) \) be a skew code in \( \overline{R} = R[X;\theta]/(f) \) and \( f = hg = gh \). Suppose that the leading coefficient of \( h \) is invertible and \( R[X;\theta]/(f) = f R[X;\theta] \). Then we have \( C = \text{ann}_{\overline{R}}(\overline{h}(X)) \).

3. **Skew codes of endomorphism type and derivation type**

First we study skew codes of endomorphism type \( R[X;\theta] \).

**Proposition 6.** Let \( C = (g)/(f) \) be a skew code in \( R[X;\theta]/(f) \) and \( f = hg \). Suppose that the leading coefficients of \( f \) and \( g \) are invertible and \( R[X;\theta]/(f) = f R[X;\theta] \). If \( \deg(f) = n \) and \( g(X) = g_{n-k} X^{n-k} + g_{n-k-1} X^{n-k-1} + \cdots + g_1 X + g_0 \), then \( C \) is a free \( R \)-module and has the \( k \times n \) generator matrix \( G \) given by

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

**Proof.** For \( l = 0, 1, 2, \cdots, k-1 \), \( X^l g(X) = \theta^l(g_{n-k}) X^{l+n-k} + \cdots + \theta^l(g_1) X^{l+1} + \theta^l(g_0) X^l \). Therefore we get the result.

We study constacyclic codes and determine their parity check matrix.

**Proposition 7.** 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 \( h(X) = h_k X^k + h_{k-1} X^{k-1} + \cdots + h_1 X + h_0 \). If the dual code \( C^\perp \) is a free \( R \)-module and \( \text{rank} C^\perp = n - k \), then \( C \) has the following \((n-k) \times n\) parity check matrix \( H \) given by

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

**Proof.** Since the leading coefficient of \( g \) is invertible and \( f \) is central, we get \( gh = hg \). By Lemma 1, \( ah = 0 \) in \( R[X;\theta]/(X^n - \alpha) \) for any \( a \in C \). Now \( \deg(ah) < n + k \) and we deduce the coefficients of the monomials \( X^k, X^{k+1}, \cdots, X^{n-1} \) in this product \( ah \) must be zero. Since \( R \) is commutative and \( \sum_{j=0}^k a_{l-j} \theta^{l-j}(h_j) = 0, (l = k, k+1, \cdots, n-1) \), 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 5. Let $R$ be a ring, $\theta$ be an automorphism of $R$. Let $S$ be a free left $R$-module with basis $1, X, X^{-1}, X^2, X^{-2}, \ldots$ and give a multiplication from the rules $Xr = \theta(r)X$ for all $r \in R$. The ring $S$ constructed in this way is denoted by $R[X, X^{-1}; \theta]$ and $S$ is called a skew Laurent ring.

Theorem 2. Suppose that $R$ is a finite commutative ring, $\theta$ 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 $h(X) = h_kX^k + h_{k-1}X^{k-1} + \cdots + h_1X + h_0$. If the dual code $C^\perp$ is a free left $R$-module and rank$C^\perp = n - k$, then the dual of the $\theta$-constacyclic code $(g)/(X^n - \alpha)$ is the $\theta$-constacyclic code $(g^\perp)/(X^n - \alpha)$ where

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

Proof. Let $R[X, X^{-1}; \theta]$ be a skew Laurent ring. Then we can define a map $\varphi : R[X; \theta] \rightarrow R[X, X^{-1}; \theta]$ such that $\sum_{i=0}^{n} a_iX^i \mapsto \sum_{i=0}^{n} X^{-i}a_i$. For $\xi, \eta \in R[X; \theta]$, we get $\varphi(\xi + \eta) = \varphi(\xi) + \varphi(\eta)$ and $\varphi(\xi\eta) = \varphi(\eta)\varphi(\xi)$. By Proposition 2, we get $X^n - \alpha = h \cdot g = g \cdot h$. Therefore we have $X^k \cdot \varphi(h) \cdot \varphi(g) \cdot X^{n-k} = X^k \cdot \varphi(X^n - \alpha) \cdot X^{n-k} = 1 - \alpha X^n = (X^n - \alpha) \cdot (-\alpha)$ Then $X^k \cdot \varphi(h) = h_k + \theta(h_{k-1})X + \cdots + \theta^k(h_0)X^k = g^\perp$. Hence we get the result.

Next we consider skew codes of derivation type $R[X; \delta]$ and give some examples.

Lemma 2. 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 3. 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 $R[X; \delta] f = f R[X; \delta]$ 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 $X^i r = \sum_{l=0}^{i} \binom{i}{l} \delta^{l-i}(r) X^i$ for $r \in R$. So we can calculate a generator matrix for a given polynomial $g(X) = g_{n-k}X^{n-k} + g_{n-k-1}X^{n-k-1} + \cdots + g_1X + g_0$.

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
Mathematical aspects of \((\theta, \delta)\)-codes

\[ R_p = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in M_2(\mathbb{Z}_p) \mid a, b \in \mathbb{Z}_p \right\}. \]

Then \(R_p\) is a finite commutative local ring with the unique maximal ideal

\[ M = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{Z}_p) \mid b \in \mathbb{Z}_p \right\}. \]

Now we can define a derivation \(\delta : R_p \rightarrow R_p\) 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 2.** We consider the skew polynomial ring of derivation type \(R(3)[X; \delta]\).

Let \(f = X^3 + 2X\). By Lemma 3, \(f\) 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 \((g)/(f)\) is a \([3, 2]\) skew \(\delta\)-code.

Let \(S_p = M_2(R_p)\) and define a derivation \(\Delta : M_2(R_p) \rightarrow M_2(R_p)\) 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 3.** We consider the skew polynomial ring of the derivation type \(S(3)[Y; \Delta]\). Let \(f = Y^3 + 2Y\). By Lemma 3, \(f\) 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 \((g)/(f)\) is a \([3, 2]\) skew \(\Delta\)-code. So the factorizations of \(R(3)[X; \delta]\) is lifted to \(S(3)[Y; \Delta]\).

**References**


Received: July, 2010