Skew Cyclic Codes Of Arbitrary Length

Irfan Siap
Department of Mathematics, Adıyaman University,
Adıyaman, TURKEY,
isiap@adiyaman.edu.tr

Taher Abualrub
Department of Mathematics and Statistics,
American University of Sharjah, Sharjah, UAE.,
abualrub@aus.edu

Nuh Aydin
Department of Mathematics, Kenyon College,
Gambier, Ohio, U.S.A.
aydinn@kenyon.edu

Padmapani Seneviratne
Department of Mathematics and Statistics,
American University of Sharjah, Sharjah, UAE.,
pseneviratne@aus.edu

February 2, 2009

Abstract

In this paper we study a special type of linear codes, called skew cyclic codes, in the most general case. This set of codes is a generalization of cyclic codes but constructed using a non-commutative ring called the skew polynomial ring. In previous works these codes have been studied with certain restrictions on their length. This work examines their structure for an arbitrary length without any restriction. Our results show that these codes are equivalent to either cyclic

codes or quasi-cyclic codes, hence establish strong connections with well-known classes of codes.

1 Introduction

Cyclic codes have been investigated and studied by many researchers for the last fifty years. These classes of codes were first discussed by a series of papers and reports by E. Prange [9], and [10] published between 1957 and 1959. Their rich algebraic structure made this class of error-correcting-codes one of the most important classes in coding theory. Prange in [9], and [10], identified cyclic codes of length n over a finite field F with ideals in the ring $F[x]/(x^n - 1)$. This relationship between ideals and cyclic codes led to the construction of BCH codes and Reed-Solomon codes. In the seventies many mathematicians and engineers expanded the study of linear and cyclic codes from finite fields to finite rings. A remarkable paper by Hammons et al. [4] showed that certain binary nonlinear codes with good error correcting capabilities can be viewed through a Gray mapping as linear codes over Z_4. All of this work is restricted to codes that are defined in a commutative ring.

D. Boucher, W. Geiselmann and F. Ulmer in [2], and in [3], took another direction when they studied a more generalized class of linear and cyclic codes using a non-commutative ring. They studied what they called skew cyclic codes, where the generator polynomial of a skew cyclic code comes from a non-commutative ring $F[x;\theta]$, where F is a finite field and θ is a field automorphism of F. They gave some examples of skew cyclic codes with Hamming distances larger than the best known linear codes with the same parameters [2].

The skew cyclic codes constructed in [2] and skew QC constructed in [1] have the property that $|\langle\theta\rangle| = m$ must be a factor of the length n of the code. If $m \nmid n$ then the polynomial generated by $(x^n - 1)$ is not a two-sided ideal and hence the set $R_n = F[x;\theta]/(x^n - 1)$ fails to be a ring. Therefore, the usual identification of codes with ideals is no longer valid.

In this paper, we are interested in studying skew cyclic codes for an arbitrary length n without any restriction. Since the polynomial $(x^n - 1)$ does not always generate a two-sided ideal in the ring $F[x;\theta]$, the set $R_n = F[x;\theta]/(x^n - 1)$ fails to be a ring unless $m|n$. It follows that identification of skew cyclic codes with ideals in R_n is invalid in this case. We will show that the set R_n is always a left $F[x;\theta]$ submodule. Therefore, we identify

skew cyclic codes with left submodules of R_n. Our main results show that any skew cyclic code is equivalent to a cyclic or a quasi-cyclic (QC) code.

The rest of the paper is organized as follows. Section 2 includes a brief description of the skew polynomial ring $F[x;\theta]$ and the definition of skew cyclic codes. It also includes a description of the set $R_n = F[x;\theta]/(x^n - 1)$. We show that R_n fails to be a ring if $m \nmid n$. However, we show that R_n can be considered as a left $F[x;\theta]$ module. In Section 3, we discuss the structure of skew cyclic codes where we show that these types of codes are left $F[x;\theta]$ submodules of R_n. Moreover we show that skew cyclic codes are free modules. This identification will help in finding a basis and the dimension of these codes. In section 4 we focus on the relationship between skew cyclic codes and cyclic and QC codes. We show that if $(m,n) = 1$ then skew cyclic codes are the same as cyclic codes and if $(m,n) = d > 1$, then skew cyclic codes are equivalent to QC codes. Section 5 concludes the paper.

2 The Definition of Skew Cyclic Codes

2.1 The Skew Polynomial Ring $F[x;\theta]$ and Skew Cyclic Codes

This section represents the construction of a non-commutative ring $R = F[x;\theta]$. The structure of this noncommutative ring depends on the elements of a finite field F and an automorphism θ of F.

Let F be any finite field of characteristic p. Let θ be an automorphism of F with $|\langle\theta\rangle| = m$. Let K be a subfield of F fixed under $\langle\theta\rangle$. Then, $[F:K] = m$ and $K = GF(p^t)$ where $F = GF(q)$ and $q = p^{tm}$. Moreover since K is fixed under θ, we have $\theta(a) = a^{p^t}$ for all $a \in F$.

Example 1 *Consider the finite field* $GF(4) = \{0, 1, \alpha, \alpha^2\}$ *where* $\alpha^2+\alpha+1 = 0$. *Define an automorphism*

$$\begin{aligned} \theta &: GF(4) \to GF(4) \text{ by} \\ \theta(a) &= a^2. \end{aligned}$$

Then $\theta(0) = 0,\ \theta(1) = 1,\ \theta(\alpha) = \alpha^2$ *and* $\theta(\alpha^2) = \alpha$. *Hence the fixed field* K *is just the binary field* $GF(2)$.

Definition 2 *Following the above notation, we define the skew polynomial set* $F[x;\theta]$ *as*

$$F[x;\theta] = \left\{ \begin{array}{c} f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n | \ \ where \\ a_i \in \ F \ for \ all \ i = 0, 1, \ldots, n \end{array} \right\}$$

where addition of these polynomials is defined in the standard manner while multiplication, which we will denote by *, is defined using the distributive law and the rule

$$(ax^i) * (bx^j) = a\theta^i(b)x^{i+j}.$$

Example 3 *Using the same automorphism from Example1 we get*

$$\begin{array}{rcl} (\alpha x) * (\alpha^2 x) & = & \alpha\theta(\alpha^2)x^2 \\ & = & (\alpha)(\alpha)x^2 = \alpha^2x^2. \end{array}$$

On the other hand we have,

$$\begin{array}{rcl} (\alpha^2 x) * (\alpha x) & = & \alpha^2\theta(\alpha)x^2 \\ & = & \alpha^2(\alpha^2)x^2 = \alpha x^2. \end{array}$$

This shows that $(\alpha x) * (\alpha^2 x) \neq (\alpha^2 x) * (\alpha x)$.

Theorem 4 *[7] The set* $F[x;\theta]$ *with respect to addition and multiplication defined above forms a non-commutative ring called the skew polynomial ring.*

The following facts are straightforward for the ring $F[x;\theta]$:

1. It has no nonzero zero-divisors.
2. The units of $F[x;\theta]$ are the units of F.
3. $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$.
4. $\deg(f * g) = \deg(f) + \deg(g)$.

The skew polynomial ring $F[x;\theta]$ was introduced by Ore [8] in 1933, and a complete treatment of this ring can be found in [6] and in [7].

Theorem 5 *[7] (The Right Division Algorithm) For any polynomials* f *and* g *in* $F[x;\theta]$ *with* $f \neq 0$ *there exist unique polynomials* q *and* r *such that*

$$g = q * f + r \ \ where \ \ \deg(r) < \deg(f).$$

The above result is called division on the right by f. A similar result can be proved regarding division on left by f. Applying the division algorithm above one can easily prove the following theorem:

Theorem 6 *[6] $F[x;\theta]$ is a non-commutative principal left (right) ideal ring. Moreover any two sided ideal must be generated by*

$$f(x) = \left(a_0 + a_1 x^m + a_2 x^{2m} + \ldots + a_r x^{rm}\right) * x^t,$$

where $|\langle\theta\rangle| = m$.

A version of the following lemma appears in [1] where only one direction of the implication is stated. We include a full statement and proof for the sake of completeness.

Lemma 7 *$(x^n - 1) \in Z\left(F[x;\theta]\right)$ if and only if $m|n$ where $Z\left(F[x;\theta]\right)$ is the center of $F[x;\theta]$.*

Proof. Assume $m|n$ and let $f(x) \in F[x;\theta]$, say

$$f(x) = a_0 + a_1 x + \cdots + a_r x^r.$$

Since $m|n$, $\theta^n(a) = a$ for any any $a \in F$. Hence,

$$\begin{aligned}
(x^n - 1) * f(x) &= (x^n - 1) * (a_0 + a_1 x + \cdots + a_r x^r) \\
&= x^n * a_0 + x^n * a_1 x + \cdots + x^n * a_r x^r - f(x) \\
&= \theta^n(a_0)x^n + \theta^n(a_1)x^n \cdot x + \cdots + \theta^n(a_r)x^n \cdot x^r - f(x) \\
&= a_0 x^n + a_1 x^n \cdot x + \cdots + a_r x^n \cdot x^r - f(x) \\
&= a_0 * x^n + a_1 x * x^n + \cdots + a_r x^r * x^n - f(x) \\
&= (a_0 + a_1 x + \cdots + a_r) * x^n - f(x) \\
&= f(x) * (x^n - 1)\,.
\end{aligned}$$

Hence, $(x^n - 1) \in Z\left(F[x;\theta]\right)$.

Conversely, suppose $(x^n - 1) \in Z\left(F[x;\theta]\right)$. Then, $x^n - 1$ commutes with every element of $F[x;\theta]$. In particular, $(x^n - 1) * ax^m = ax^m * (x^n - 1)$, for any $a \in F$. Now, $(x^n - 1) * ax^m = \theta^n(a)x^{n+m} - ax^m$, and $ax^m * (x^n - 1) = ax^{n+m} - ax^m$. This implies that $\theta^n(a) = a$ for all $a \in F$, hence $|\langle\theta\rangle|\,|n$. ■

The skew polynomial ring is important in the study the structure of skew cyclic codes which are defined as follows.

Definition 8 *Let F be any finite field of characteristic p and let θ be an automorphism of F with $|\langle\theta\rangle| = m$. A subset C of F^n is called a skew cyclic code of length n if*

1. *C is a subspace of F^n.*
2. *If*
$$c = (c_0, c_1, \ldots, c_{n-1}) \in C$$
then
$$\theta(c) = (\theta(c_{n-1}), \theta(c_0), \ldots, \theta(c_{n-2})) \in C.$$

It is shown in [2, 3] that under the usual identification of vectors with polynomials, the skew cyclic shift (the second condition in the definition above) corresponds to skew multiplication by x in $F[x;\theta]$, and skew cyclic codes are ideals in $F[x;\theta]/(x^n - 1)$ when $m|n$.

2.2 Algebraic Structure Of $R_n = F[x;\theta]/(x^n - 1)$

As a result of Theorem 6, the ideal generated by the polynomial $x^n - 1$ is a two sided ideal if and only if $m|n$. Moreover by Lemma 7, $(x^n - 1)$ commutes with the elements of $F[x;\theta]$ if and only if $m|n$. This result has a big impact on the structure of elements in the set $R_n = (F[x;\theta]/(x^n - 1)$. If $m|n$ then the set R_n is a well-defined ring where multiplication of elements in R_n is defined by

$$\begin{aligned}(f_1(x) + (x^n - 1)) * (f_2(x) + (x^n - 1)) \qquad (1)\\ = f_1(x) * f_2(x) + f_1(x) * (x^n - 1) + (x^n - 1) * f_2(x) + (x^n - 1)\end{aligned}$$

Now since $m|n$, by Lemma 7, $(x^n - 1) \in Z(F[x,\theta])$. Hence

$$(x^n - 1) * f_2(x) = f_2(x) * (x^n - 1). \qquad (2)$$

This implies that

$$\begin{aligned}&(f_1(x) + (x^n - 1)) * (f_2(x) + (x^n - 1))\\ &\quad = f_1(x) * f_2(x) + (f_1(x) + f_2(x)) * (x^n - 1) + (x^n - 1)\\ &\quad = f_1(x) * f_2(x) + (x^n - 1).\end{aligned}$$

So multiplication is well-defined in R_n and hence R_n is a ring. If $m \nmid n$ then $(x^n - 1) \notin Z(F[x, \theta])$ and hence Equation 2 is not valid anymore. This implies that

$$\begin{aligned}(f_1(x) + (x^n - 1)) * (f_2(x) + (x^n - 1)) \\ &= f_1(x) * f_2(x) + f_1(x) * (x^n - 1) + (x^n - 1) * f_2(x) + (x^n - 1) \\ &\neq f_1(x) * f_2(x) + (x^n - 1). \end{aligned} \quad (3)$$

Equation 3 implies that multiplication is not well-defined in the set R_n and hence R_n is not a ring anymore. Since R_n is not a ring, we can not discuss the structure of ideals in this set. In all of the literature on skew cyclic codes, the condition $m|n$ is assumed, hence the one-to-one correspondence between the skew cyclic codes and the ideals in R_n is used. Because R_n fails to be a ring for other values of n, we are faced with two possible scenarios regarding the structure of skew cyclic codes

- Scenario I: Restrict the study of skew cyclic codes to the case $m|n$ **only:** In this case there is a a one-to-one correspondence between skew cyclic codes and ideals in R_n. This is the reason that the work in [2, 3] was restricted to the case where $m|n$.

- Scenario II: No restriction on the length n : In this case the traditional relationship between ideals and cyclic codes is no longer valid. Another approach is needed to handle the case of arbitrary code length n.

In this paper we are interested in studying the structure of skew cyclic codes for any length n (Scenario II). Although the set R_n is not a ring anymore for $m \nmid n$, it still has a useful structure that makes it possible to handle this case.

Let $(f(x) + (x^n - 1))$ be an element in the set R_n, and let $r(x) \in F[x; \theta]$. Define multiplication from left as:

$$r(x) * (f(x) + (x^n - 1)) = r(x) * f(x) + (x^n - 1) \text{ for any } r(x) \in F[x; \theta]. \quad (4)$$

This is a well-defined multiplication of the elements of R_n by the elements of $F[x; \theta]$. Under this definition we have the following theorem:

Theorem 9 *R_n is a left $F[x; \theta]$-module where multiplications is defined as in Equation 4.*

Proof. Using the definition in Equation 4, it is straightforward to show that all the conditions of a left module are satisfied. ■

3 The Structure of Skew Cyclic Codes

The set R_n can be described as

$$R_n = F[x;\theta]/\left(x^n-1\right) = \left\{ \begin{array}{c} f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1}x^{n-1} | \text{ where} \\ a_i \in F \text{ for all } i = 0, 1, \ldots, n-1 \text{ and } x^n = 1 \end{array} \right\}.$$

It is worth noting that the set R_n can be considered as a left F-module, and from Theorem 9 as a left $F[x;\theta]$-module.

Under this representation of R_n and due to Theorem 6, we can identify each codeword

$$(a_o, a_1, \ldots, a_{n-1})$$

by a polynomial

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1}x^{n-1} \text{ in } R_n$$

as in the traditional study of cyclic codes. The following theorem gives a well-defined definition of skew cyclic codes for any length n.

Theorem 10 *A code C in R_n is a skew cyclic code if and only if C is a left $F[x;\theta]$-submodule of the left $F[x;\theta]$-module R_n.*

Proof. Suppose C is a skew cyclic code in R_n. Let

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1}x^{n-1}$$

be any codeword in C. Since C is a skew cyclic code, $(a_0, a_1, \ldots, a_{n-1})$ and all its skew cyclic shifts are in C. Note that

$$\begin{array}{rcl} x * f(x) & = & \theta(a_{n-1}) + \theta(a_0)x + \ldots + \theta(a_{n-2})x^{n-1} \\ & = & (\theta(a_{n-1}), \theta(a_0), \theta(a_1), \ldots, \theta(a_{n-2})), \\ \vdots & & \\ x^i * f(x) & = & \theta^i\left(a_{n-i}\right) + \theta^i\left(a_{n-i+1}\right)x + \ldots + \theta^i\left(a_{n-i-1}\right)x^{n-1} \\ & = & \left(\theta^i\left(a_{n-i}\right), \theta^i\left(a_{n-i+1}\right), \ldots, \theta^i\left(a_{n-i-1}\right)\right) \end{array}$$

are all elements in C, where all the indices are taken $\mod n$. Since C is a linear code, it follows that $r(x) * f(x) \in C$ for any $r(x) \in F[x;\theta]$. Therefore C is an $F[x;\theta]$-submodule of R_n.

Now suppose C is a left $F[x;\theta]$-submodule of the left $F[x;\theta]$-module R_n, then for any $f(x) \in C$ we have $x * f(x) \in C$. Therefore C is a skew cyclic code. ■

In the sequel the structure of skew cyclic codes will be identified with the structure of the left $F[x;\theta]$-submodules of R_n.

Lemma 11 *Let C be a left submodule of R_n. Then C is a cyclic submodule generated by a monic polynomial of minimal degree in C.*

Proof. Let $f(x) \in C$ be a monic polynomial of minimal degree among non-zero polynomials in C. Note that $f(x)$ is unique (otherwise if $l(x) \in C$ is monic of the same degree then $f(x) - l(x) \in C$ would be of degree less than the degree of $f(x)$). Let $c(x)$ be any element in C. By the right division algorithm there are two unique polynomials q and r such that

$$c = q * f + r \text{ where } r = 0 \text{ or } \deg(r) < \deg(f).$$

Since C is a left submodule, $r = c - qf \in C$. This is a contradiction unless $r = 0$, since $f(x)$ is of minimal degree in C. Therefore, we have $c = q * f$ and hence C is a cyclic submodule generated by $f(x)$. We write this as $C = (f)$. ■

Theorem 12 *Let $C = (f)$ be a left submodule of R_n. Then $f(x)$ is a right divisor of $x^n - 1$.*

Proof. Let $f(x)$ be a polynomial of minimal degree in C. Again as in Lemma 11 above there are two unique polynomials q and r such that

$$x^n - 1 = q * f + r \text{ where } \deg(r) < \deg(f).$$

Since $f(x)$ and $x^n - 1 = 0$ are in C, we conclude that $r(x) \in C$. But $f(x)$ is of minimal degree in C. Therefore $r(x) = 0$ and hence $f(x)$ is a right divisor of $x^n - 1$. ■

Before we state the next results it is important to note that C can be considered both as left $F[x;\theta]$ and F submodules.

Theorem 13 *Let $C = (g)$ be a left submodule of R_n where $g(x)$ is a right divisor of $x^n - 1$ of degree r, and $x^n - 1 = h(x) * g(x)$. Then C is a free left F-submodule with basis*

$$\begin{aligned} \beta &= \left\{g(x),\ x * g(x), \ldots, x^{n-r-1} * g(x)\right\}, \text{ and} \\ \dim C &= n - r. \end{aligned}$$

Proof. Let $C = (g(x))$ be a left submodule of R_n where $g(x)$ is a right divisor of $x^n - 1$ of degree r. Let $c(x) \in C$. Then there is an element $l(x) \in F[x; \theta]$ such that

$$c(x) = l(x) * g(x).$$

If $\deg l(x) \leq n - r - 1$ then β is a spanning set of C. Otherwise by the right division algorithm there are two polynomials $q(x)$ and $r(x)$ such that

$$l(x) = q(x) * h(x) + r(x)$$

with $r(x0 = 0$ or $\deg r(x) \leq n - r - 1$. Multiplying by $g(x)$ on the right and noting that $h(x) * g(x) = 0$ we get

$$l(x) * g(x) = r(x) * g(x).$$

Therefore, β spans C. To show that β is linearly independent suppose that

$$c_0 g(x) + c_1 x * g(x) + \ldots + c_{n-r-1} x^{n-r-1} * g(x) = 0.$$

Comparing coefficients yields the fact that $c_i = 0$ for all $i = 0, 1, \ldots, n-r-1$. Hence β is linearly independent and therefore it is a basis for C with $\dim C = n - r$. ■

4 Relationship between skew cyclic codes and cyclic and QC-codes

Before we prove our main results in this section, we will recall the definition of cyclic codes and quasi cyclic codes.

Definition 14 *Let F be any finite field of characteristic p. A subset C of F^n is called a cyclic code of length n if*

1. *C is a subspace of F^n.*
2. *If*
$$c = (c_0, c_1, \ldots, c_{n-1}) \in C$$
then
$$c = (c_{n-1}, c_0, \ldots, c_{n-2}) \in C.$$

Definition 15 *Let F be a finite field. A subset C of F^n is called a quasi-cyclic code of length n where $n = sl$, and index l if*

1. *C is a subspace of F^n.*
2. *If*

$$c = \begin{pmatrix} c_{0,0}, c_{0,1}, \ldots, c_{0,l-1}, c_{1,0}, c_{1,1}, \ldots, c_{1,l-1}, \ldots, \\ c_{s-1,0}, c_{s-1,1}, \ldots, c_{s-1,l-1} \end{pmatrix} \in C$$

then

$$T_{\theta,s,l}(c) = \begin{pmatrix} c_{s-1,0}, c_{s-1,1}, \ldots, c_{s-1,l-1}, c_{0,0}, \\ \ldots, c_{0,l-1}, \ldots, c_{s-2,0}, \ldots, c_{s-2,l-1} \end{pmatrix} \in C.$$

In the proofs of the following theorems, we will use the following fact from elementary number theory. Let d be the greatest common divisors of the integers a and b (denoted by $(a, b) = d$). Then there exist integers x and y such that

$$ax + by = d.$$

This representation is not unique. In fact, if we let let $x_0 = x + k\dfrac{b}{(a,b)}$, and $y_0 = y - k\dfrac{a}{(a,b)}$ for some integer k, then

$$\begin{aligned} ax_0 + by_0 &= ax + k\frac{ab}{(a,b)} + by - k\frac{ab}{(a,b)} \\ &= ax + by = d. \end{aligned} \tag{5}$$

Theorem 16 *Let C be a skew cyclic code of length n and let θ be an automorphism of F with $|\langle\theta\rangle| = m$. If $(m, n) = 1$ then C is a cyclic code of length n.*

Proof. Let $C = (g(x))$ be a skew cyclic code of length n such that $(m, n) = 1$. We know that there exist integers α_1, α_2 such that

$$1 = \alpha_1 m + \alpha_2 n \Rightarrow \alpha_1 m = 1 - \alpha_2 n.$$

By Equation 5 we may assume that α_2 is a negative integer, so we can write $\alpha_1 m = 1 + Dn$, where $D > 0$. Let $c(x) = c_0 + c_1 x + \ldots + c_{n-1} n - 1 x^{n-1} \in C$.

To show that C is a cyclic code it is suffices to show that $c_{n-1} + c_0 x + c_1 x^2 + \ldots + c_{n-2} x^{n-2} \in C$. Consider

$$\begin{aligned} & x^{\alpha_1 m} * c(x) \\ & \quad = x^{1+Dn} * \left(c_0 + c_1 x + \ldots + c_{n-1} x^{n-1}\right) \\ & \quad = \theta^{1+Dn}(c_0) x^{1+Dn} + \cdots + \theta^{1+Dn}(c_{n-2}) x^{1+Dn+n-2} + \theta^{1+Dn}(c_{n-1}) x^{1+Dn+n-1} \\ & \quad = \theta^{\alpha_1 m}(c_0) x^{1+Dn} + \ldots + \theta^{\alpha_1 m}\left(c_{n-2}\right) x^{Dn+n-1} + \theta^{\alpha_1 m}\left(c_{n-1}\right) x^{n+Dn} \in C. \end{aligned}$$

Note that in the ring $R_n = F[x;\theta]/(x^n - 1)$, we have $x^n = 1$ and $\theta^m(a) = a$ for any $a \in F$. This implies that

$$x^{\alpha_1 m} * c(x) = c_{n-1} + c_0 x + c_1 x^2 + \ldots + c_{n-2} x^{n-1} \in C.$$

Thus, C is a cyclic code of length n. ■

This theorem yields the following corollary.

Corollary 17 *For $(m,n) = 1$, if $f(x)$ is a factor of $x^n - 1$ in $F[x,\theta]$, then $f(x)$ is also a factor of $x^n - 1$ in the usual polynomial ring $F[x]$.*

Theorem 18 *Let $C = (g(x))$ be a skew cyclic code of length n and let θ be an automorphism of F with $|\langle\theta\rangle| = m$. If $(m,n) = d$ then C is equivalent to a QC code of length n and index d.*

Proof. Let $n = ds$ and $c = \begin{pmatrix} c_{0,0}, c_{0,1}, \ldots, c_{0,d-1}, c_{1,0}, c_{1,1}, \ldots, c_{1,d-1}, \ldots, \\ c_{s-1,0}, c_{s-1,1}, \ldots, c_{s-1,d-1} \end{pmatrix} \in C$. Since $(m,n) = d$, we may write $\alpha_1 m = d + Jn$ for some nonnegative integer J. Consider

$$\begin{aligned} \theta^{d+Jn} \quad & \begin{pmatrix} c_{0,0}, c_{0,1}, \ldots, c_{0,d-1}, c_{1,0}, c_{1,1}, \ldots, c_{1,d-1}, \ldots, \\ c_{s-1,0}, c_{s-1,1}, \ldots, c_{s-1,d-1} \end{pmatrix} \\ = \quad & \begin{pmatrix} \theta^{d+Jn}\left(c_{s-1,0}\right), \theta^{d+Jn}\left(c_{s-1,1}\right), \ldots, \theta^{d+Jn}\left(c_{s-1,d-1}\right), \theta^{d+Jn}\left(c_{0,0}\right), \ldots, \\ \theta^{d+Jn}\left(c_{0,d-1}\right), \ldots, \theta^{d+Jn}\left(c_{s-2,0}\right), \theta^{d+Jn}\left(c_{s-2,1}\right), \ldots, \theta^{d+Jn}\left(c_{s-2,d-1}\right) \end{pmatrix}. \end{aligned}$$

$\theta^{d+Jn}(a) = \theta^{\alpha_1 m}(a) = a$ for any $a \in F$. This implies that

$$\begin{aligned} & \theta^{d+Jn} \begin{pmatrix} c_{0,0}, c_{0,1}, \ldots, c_{0,d-1}, c_{1,0}, c_{1,1}, \ldots, c_{1,d-1}, \ldots, \\ c_{s-1,0}, c_{s-1,1}, \ldots, c_{s-1,d-1} \end{pmatrix} \\ = \quad & \begin{pmatrix} c_{s-1,0}, c_{s-1,1}, \ldots, c_{s-1,d-1}, c_{0,0}, \ldots, \\ c_{0,d-1}, \ldots, c_{s-2,0}, c_{s-2,1}, \ldots, c_{s-2,d-1} \end{pmatrix} \in C. \end{aligned}$$

Therefore, C is equivalent to a QC code of length n and index d. ■

Remark 19 *Theorem 16 can be obtained as a corollary to Theorem 18, where $d = 1$. However, it is such an important special case that it is worthy of being stated by itself. Moreover, this is the order in which we observed and proved these results.*

Example 20 *Let us consider the skew cyclic code of length 40 generated by the polynomial $p(x) = a^2 + ax^2 + a^2x^4 + ax^5 + a^2x^6 + x^7 + x^8 + x^9 + a^2x^{10} + ax^{11} + x^{13} + x^{14} + x^{15} + ax^{17} + ax^{18} + ax^{19} + a^2x^{20} + x^{21} + x^{22} + ax^{23} + x^{24}$ over $GF(4)$. This polynomial generates a skew cyclic code with parameters $[40, 16, 15]$ [2], which is the best known code for these parameters. In this case $m = 2$, and $d = 2$. According to Theorem 18 this code should be equivalent to a QC code of index 2. In fact, it is equivalent to the 1-generator QC code generated by the polynomials $g_1(x) = x^{19} + x^{18} + x^{17} + x^{16} + x^5$ and $g_2(x) = a^2x^{19} + x^{18} + a^2x^{17} + x^{16} + a^2x^{15} + a^2x^{14} + ax^{13} + ax^{12} + a^2x^{10} + x^9 + x^8 + ax^7 + a^2x^5 + a^2x^3 + ax^2 + a$ [5].*

Example 21 *Let us consider the skew cyclic code of length 30 generated by the polynomial $p(x) = a^2 + ax + a^2x^2 + a^2x^4 + ax^5 + x^6 + ax^7 + x^8 + x^9 + x^{10}ax^{11} + x^{13} + x^{14}$ over $GF(4)$. This polynomial generates a skew cyclic code with parameters $[30, 16, 9]$ [2], and it is the best known code for these parameters. This code is also equivalent to a QC code of index 2. This is a 2-generator QC code generated by the polynomials $g_1(x) = x^{10}$, $g_2(x) = a^2x^{12} + x^{11} + x^9 + x^8 + ax^7 + ax^6 + a^2x^3 + ax^2 + x$, $g_3(x) = 0$, and $g_4(x) = x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ [5].*

Example 22 *We have $x^6 - 1 = (x^3 + a^{10}x^2 + a^5x + a^5) * (x^3 + a^5x^2 + a^5x + a^{10})$ in $F[x, \theta]$ where $F = GF(16) = \mathbb{Z}_2(a)$, a is a root of $x^4 + x + 1$, and $\theta(z) = z^2$. The polynomial $g = x^3 + a^{10}x^2 + a^5x + a^5$ generates a skew cyclic code over $GF(16)$ with parameters $[6, 3, 3]$. In this example, $m = 4, n = 2$, and $d = 2$. As predicted by Theorem 18, this code is equivalent to the 2-QC code generated by $g_1(x) = a^{10}x + a^5$, and $g_2(x) = x + a^5$.*

5 Conclusion

In this paper, we investigated the structure of skew cyclic codes of an arbitrary length n, where the generator polynomial of a skew cyclic code comes from the non-commutative ring $F[x; \theta]$ where θ is an automorphism of F with

$|\langle\theta\rangle| = m$. We have shown that if $m \nmid n$ then the polynomial generated by $(x^n - 1)$ is not a two-sided ideal and hence the set $R_n = F[x;\theta]/(x^n - 1)$ fails to be a ring. Under this condition skew cyclic codes can not be identified with ideals in R_n. Considering R_n as a left $F[x;\theta]$-module, we have shown that a skew cyclic code is either equivalent to a usual cyclic code (the case $(m, n) = 1$), or a quasi-cyclic code of index d (case $(m, n) = d$).

References

[1] T. Abualrub, A. Ghrayeb, N. Aydin,I. Siap, On the construction of skew quasi-cyclic codes, Preprint.

[2] D. Boucher, W. Geiselmann, F. Ulmer, Skew cyclic codes Appl Algebr Eng Comm. 18 (2007) 379-389.

[3] D. Boucher, W. Geiselmann, F. Ulmer, Coding with skew polynomial ring,Preprint.

[4] A.R. Hammons Jr., P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, P. Sole, The Z_4-linearity of Kerdock, Preparata, Goethals and Related Codes, IEEE Trans. Inform. Theory, 40 (1994) 301-319.

[5] M. Grassl, Table of bounds on linear codes, Available at: http://www.codetables.de.

[6] N. Jacobson, The Theory of Rings, Amer. Math. Soc., New York, 1943.

[7] B. R. McDonald, Finite Rings With Identity, Marcel Dekker Inc., New York, 1974.

[8] O. Ore, Theory of non-commutative polynomials, Annals of Math. 34 (1933) 480-508.

[9] E. Prange, Cyclic error-correcting codes in two symbols, Air Force Cambridge Research Center-TN-57-103, Cambridge, MA, 1957.

[10] E. Prange, Some cyclic error-correcting codes with simple decoding algorithm, Air Force Cambridge Research Center-TN-58-156, Cambridge, MA, 1958.