Journal of Engineering Technology and Applied Sciences, 2022 *e-ISSN:* 2548-0391
Received 13 January 2022, Accepted 23 April 2022 *Vol. 7, No. 1, 51-60*
Published online 29 April 2022, Research Article *doi: 10.30931/jetas.1057395*

Citation: Koroglu, M. E, "Skew Cyclic Codes over the Non-Chain ring $\mathcal{R}_q = \mathbb{F}_q[v]/\langle v^2+1\rangle$ ". Journal of Engineering Technology and Applied Sciences 7 (1) 2022 : 51-60.

SKEW CYCLIC CODES OVER THE NON-CHAIN RING $\mathcal{R}_q = \mathbb{F}_q[v]/\langle v^2+1\rangle$ [1,2]

Mehmet Emin Köroğlu

Department of Mathematics Faculty of Arts and Sciences
Yildiz Technical University, Esenler 34220, Istanbul-Turkey
mkoroglu@yildiz.edu.tr

Abstract

In this paper, we investigate the algebraic structure of the non-local ring $\mathcal{R}_q = \mathbb{F}_q[v]/\langle v^2+1\rangle$ and identify the automorphisms of this ring to study the algebraic structure of the skew cyclic codes and their duals over it.

Keywords: Non-chain ring, linear codes, skew cyclic codes

1. Introduction

In recent three decades, codes over finite commutative chain rings were studied remarkably (see Refs. [1, 7-9, 13, 14, 16, 17]). In recent years, some specific non-chain rings have been used as the alphabets for codes (see Refs. [10-12, 15]). Cyclic codes form an important class of linear codes in the area of coding theory and have practical applications to other disciplines including classical and quantum communication systems as they can be encoded with shift registers since their algebraic structure. Since the factorization of the polynomials over non-commutative structures is not unique, they are potentially more convenient for the purpose of obtaining good code parameters than commutative structures. This fact makes the study of skew polynomial rings more conspicuous. The algebraic structure of the cyclic codes of length n over the standard polynomial rings is totally determined by the polynomial divisors

[1] This research is supported by Yildiz Technical University Scientific Research Projects Coordination Department with Project Number FKD-2022-4419.
[2] A preliminary version of this paper is presented in International E-Conference on Pure and Applied Mathematical Sciences (ICPAMS-2022).

of the binomial $x^n - 1$. In [2], Boucher, Geiselmann and Ulmer used skew polynomials to determine the algebraic structure of cyclic codes under a skew cyclic shift.

Here, we recall the algebraic structure of the non-local ring $\mathcal{R}_q = \mathbb{F}_q[v] \big/ \langle v^2 + 1 \rangle$ and determine the automorphisms of this ring to study the algebraic structure of the skew cyclic codes and their duals over it.

The rest of the paper is organized as follows. In Sect. 2, we recall some basic notations and results that are needed in the rest of the study. In Sect. 3, we introduce algebraic structure of the ring $\mathcal{R}_q$ and we give a decomposition of it. Then we determine automorphism group of the ring and define a Gray type map over it. Finally, we recall structure of the linear codes over the ring $\mathcal{R}_q$. In Sect. 4, we introduce basics of the skew cyclic codes over finite fields and extend this results to the ring $\mathcal{R}_q$.

2. Preliminaries

In this section, we will fix some notations for this paper and recall some basic notations and results that are needed in the rest of the study. Throughout this work, we will use the following notation unless otherwise noted.

- $q = p^k$ and $p = a^2 + b^2$ is a prime, where a and b positive integers
- $\mathbb{F}_q$ is the finite field of q elements
- $\mathbb{F}_q^* = \mathbb{F}_q - \{0\}$
- $\mathcal{R}_q = \mathbb{F}_q[v] / \langle v^2 + 1 \rangle$ such that $v^2 \equiv -1 (mod\ q)$
- $\mathcal{U}(\mathcal{R}_q)$ is the unit group of $\mathcal{R}_q$
- $Aut(\mathcal{R}_q)$ is the automorphism group of $\mathcal{R}_q$

A linear code of length n and dimension k over $\mathbb{F}_q$ is a vector subspace of the vector space $\mathbb{F}_q^n$. An element of a linear code is termed as a codeword. The minimum Hamming distance d of a linear code $\mathcal{C}$ is the minimum Hamming weight $w_H(\mathcal{C})$ of $\mathcal{C}$, where $w_H(\mathcal{C}) = \min\{w_H(c) | 0 \neq c \in \mathcal{C}\}$ and $w_H(c) = |\{i : c_i \neq 0, i \in \{0,1,\ldots,n-1\}\}|$. A linear code $\mathcal{C}$ over $\mathbb{F}_q$ of length n, dimension k and minimum distance d is denoted by the triple $[n,k,d]_q$ and this code can correct up to $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors. The (Euclidean) dual $\mathcal{C}^\perp$ of a linear code $\mathcal{C}$ over $\mathbb{F}_q$ is the set $\mathcal{C}^\perp = \left\{ y \in \mathbb{F}_q^n \middle| \sum_{i=0}^{n-1} x_i y_i = 0, \forall x \in \mathcal{C} \right\}$.

A cyclic code over the finite field $\mathbb{F}_q$ of length n is a linear code $\mathcal{C}$ satisfying that $(c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$ for each codeword $\mathbf{c} = (c_0, \ldots, c_{n-1}) \in \mathcal{C}$. By mapping a codeword

$\mathbf{c}=(c_0,\ldots,c_{n-1})$ to a polynomial $c_0+c_1x+\cdots+c_{n-1}x^{n-1}$, one gets that a cyclic code over $\mathbb{F}_q$ of length n corresponds to a principal ideal $\mathcal{C}=\langle g(x)\rangle$ in the quotient ring $\mathbb{F}_q[x]/\langle x^n-1\rangle$.

Note that a cyclic code $\mathcal{C}=\langle g(x)\rangle$ of length n is of $n-k$ dimension, where $k=deg(g(x))$.

3. Structure of the ring $\mathcal{R}_q$ and linear codes over $\mathcal{R}_q$

In this section, we introduce algebraic structure of the ring $\mathcal{R}_q$ and we give a decomposition of it. Then we determine automorphism group of the ring and define a Gray type map over it. Finally, we recall structural properties of the linear codes over the ring $\mathcal{R}_q$.

An automorphism of the finite field $\mathbb{F}_q$ is a bijection from the field onto itself. The distinct automorphisms of $\mathbb{F}_q$ over $\mathbb{F}_p$ are exactly the mappings $\theta_0,\theta_1,\ldots,\theta_{k-1}$, defined by $\theta_j(\beta)=\beta^{p^j}$ for $\beta\in\mathbb{F}_q$ and $0\leqslant j\leqslant k-1$.

The ring $\mathcal{R}_q=\mathbb{F}_q[v]/\langle v^2+1\rangle$ such that $v^2\equiv -1(mod\ q)$ is a non-chain principal ideal ring with two maximal ideals $\langle\alpha\rangle$ and $\langle\alpha^*\rangle$, where $\alpha=a+bv$ is an element of $\mathcal{R}_q$ and $\alpha^*=a-bv$, which is called as the conjugate of the element α. The ideal lattice of $\mathcal{R}_q$ is given in the Figure 1.

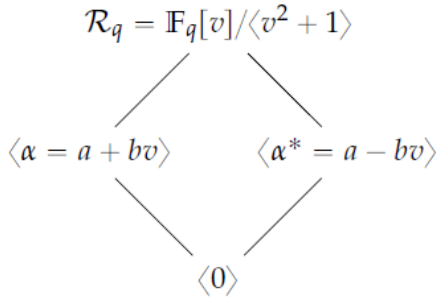

Figure 1. The ideal lattice of the ring $\mathcal{R}_q=\mathbb{F}_q[v]/\langle v^2+1\rangle$

An element $\pi\in\mathcal{R}_q$ is called an idempotent if $\pi^2=\pi$ and two idempotents π_1,π_2 are said to be orthogonal if $\pi_1\pi_2=0$. An idempotent of $\mathcal{R}_q$ is said to be primitive if it is non-zero and it cannot be written as a sum of orthogonal idempotents. A collection $\{\pi_0,\pi_1,\ldots,\pi_{s-1}\}$ of idempotents of $\mathcal{R}_q$ is complete if $\pi_0+\pi_1+\ldots+\pi_{s-1}=1$. Any complete collection of idempotents in $\mathcal{R}_q$ is a basis of the $\mathbb{F}_q$-vector space $\mathcal{R}_q$. Hence, any element $r\in\mathcal{R}_q$ can be uniquely expressed as $r=r_0\pi_0+r_1\pi_1+\ldots+r_{s-1}\pi_{s-1}$, where $r_i\in\mathcal{R}_q$.

Let $\pi_0 = \frac{1}{2a}\alpha$ and $\pi_1 = \frac{1}{2a}\alpha^*$ be two elements in $\mathcal{R}_q$. It is easy to see that the set $\{\pi_0, \pi_1\}$ is a complete set of idempotents in $\mathcal{R}_q$. Therefore, any element $r \in \mathcal{R}_q$ can be uniquely represented as $r = r_0\pi_0 + r_1\pi_1$, where $r_0, r_1 \in \mathbb{F}_q$. From the Figure 1, we can easily see that an element $x\pi_0 + y\pi_1 \in \mathcal{R}_q$ is a unit if and only if both x and y are nonzero. Then the unit group of $\mathcal{R}_q$ is described as

$$\mathcal{U}(\mathcal{R}_q) = \{x\pi_0 + y\pi_1 \mid x, y \in \mathbb{F}_q \textbf{ such that } x \neq 0 \textbf{ and } y \neq 0\}.$$

Because of the choice of x and y, the number of unit elements of $\mathcal{R}_q$, i.e., the cardinality of the set $\mathcal{U}(\mathcal{R}_q)$, $|\mathcal{U}(\mathcal{R}_q)|$ is equal to $(q-1)(q-1)$.

Theorem 3.1. Let θ be an automorphism of $\mathbb{F}_q$ and σ be a permutation of the set $\{0,1\}$. Then the map $\Theta_{\theta,\sigma} : \mathcal{R}_q \longrightarrow \mathcal{R}_q$, $\Theta_{\theta,\sigma}(r_0\pi_0 + r_1\pi_1) \mapsto \theta(r_0)\pi_{\sigma(0)} + \theta(r_1)\pi_{\sigma(1)}$ is an automorphism of the ring $\mathcal{R}_q$. Further, the cardinality $|Aut(\mathcal{R}_q)|$ of the automorphism group of $\mathcal{R}_q$ $Aut(\mathcal{R}_q) = \{\Theta_{\theta,\sigma} \mid \theta \in Aut(\mathbb{F}_q) \textbf{ and } \sigma \in S_2\}$, where S_2 is the permutation group of the set $\{0,1\}$, is $2k$.

Proof. It is easy to check that $\Theta_{\theta,\sigma}$ is an automorphism of the ring $\mathcal{R}_q$. Hence, $\{\Theta_{\theta,\sigma} \mid \theta \in Aut(\mathbb{F}_q) \textbf{ and } \sigma \in S_2\} \subset Aut(\mathcal{R}_q)$. On the other hand, if $\Theta \in Aut(\mathcal{R}_q)$, then the restriction of Θ over $\mathbb{F}_q$ is θ. Thus, for any $r = r_0\pi_0 + r_1\pi_1 \in \mathcal{R}_q$, we have $\Theta(r) = \theta(r_0)\Theta(\pi_0) + \theta(r_1)\Theta(\pi_1)$. Now the set $\{\Theta(\pi_0), \Theta(\pi_1)\}$ is another complete set of primitive pairwise orthogonal idempotents in $\mathcal{R}_q$. By the idempotent decomposition of the ring $\mathcal{R}_q = \pi_0\mathcal{R}_q \oplus \pi_1\mathcal{R}_q$, it follows that there exists a permutation of the set $\{0,1\}$ such that $\Theta(\pi_i) = \pi_{\sigma(i)}$. Therefore, $\Theta(r) = \theta(r_0)\pi_{\sigma(0)} + \theta(r_1)\pi_{\sigma(1)}$ and $Aut(\mathcal{R}_q) = \{\Theta_{\theta,\sigma} \mid \theta \in Aut(\mathbb{F}_q) \textbf{ and } \sigma \in S_2\}$. In conclusion, $\Theta_{\theta,\sigma} \circ \Theta_{\theta',\sigma'} = \Theta_{\theta\circ\theta',\sigma\circ\sigma'}$ and hence $|Aut(\mathcal{R}_q)| = 2k$.

The map $\varphi : \mathcal{R}_q \longrightarrow \mathbb{F}_q^2$ such that $\varphi(r_0\pi_0 + r_1\pi_1) = (r_0, r_1)$ is a ring epimorphism and can be extended to $\mathcal{R}_q^n$ as

$$\Phi : \mathcal{R}_q^n \longrightarrow \mathbb{F}_q^{2n},\ \Phi(r_{0,0}\pi_0 + r_{0,1}\pi_1, \ldots, r_{n-1,0}\pi_0 + r_{n-1,1}\pi_1) \mapsto (r_{0,0}, \ldots, r_{n-1,0}, r_{0,1}, \ldots, r_{n-1,1}) = (\Phi_0 \mid \Phi_1).$$

This Gray type map is an isomorphism of vector spaces over $\mathbb{F}_q$. The Gray weight of any element $\mathbf{r} \in \mathcal{R}_q^n$ is defined as $w_G(\mathbf{r}) = w_H(\Phi(\mathbf{r}))$. It is apparent that the linear Gray type map Φ is a weight preserving map from $\mathcal{R}_q^n$ to $\mathbb{F}_q^{2n}$. A linear code $\mathcal{C}$ of length n is an $\mathcal{R}_q$-submodule of $\mathcal{R}_q^n$. The Euclidean dual of a linear code $\mathcal{C}$ over $\mathcal{R}_q$ is defined by

$\mathcal{C}^{\perp} = \left\{ \mathbf{s} \in \mathcal{R}_q^n \,\middle|\, \sum_{i=0}^{n-1} r_i s_i = 0, \forall \mathbf{r} \in \mathcal{C} \right\}$. Note that the Euclidean dual of a linear code over $\mathcal{R}_q$ is also a linear code over $\mathcal{R}_q$.

Proposition 3.2. Let $\mathcal{C}$ be a linear code of length n over $\mathcal{R}_q$. Then, $\Phi\left(\mathcal{C}^{\perp}\right) = \left(\Phi\left(\mathcal{C}\right)\right)^{\perp}$. Further, $\mathcal{C}$ is a self-dual code iff $\Phi\left(\mathcal{C}\right)$ is a self-dual code of length $2n$.

Proof. It is enough to show that the map Φ preserves the orthogonality, that is, $\left\langle \Phi\left(\mathbf{c}_0\right), \Phi\left(\mathbf{c}_1\right) \right\rangle = 0$ when $\left\langle \mathbf{c}_0, \mathbf{c}_1 \right\rangle = 0$. By the linearity of Φ, let $\mathbf{r} = r_0\pi_0 + r_1\pi_1, \mathbf{s} = s_0\pi_0 + s_1\pi_1 \in \mathcal{R}_q$ such that $\left\langle \mathbf{r}, \mathbf{s} \right\rangle = 0$. Then, we get $\left\langle \mathbf{r}, \mathbf{s} \right\rangle = r_0 s_0 \pi_0 + r_1 s_1 \pi_1 = \frac{r_0 s_0 + r_1 s_1}{2} + \frac{\left(r_0 s_0 - r_1 s_1\right) b}{2a} v = 0$ and so $r_0 s_0 + r_1 s_1 = 0$. In this case, it follows that $\left\langle \Phi\left(\mathbf{r}\right), \Phi\left(\mathbf{s}\right) \right\rangle = r_0 s_0 + r_1 s_1 = 0,$ which completes the proof.

Since $\mathcal{R}_q = \pi_0 \mathcal{R}_q \oplus \pi_1 \mathcal{R}_q$ it follows that $\mathcal{R}_q^n = \pi_0 \mathcal{R}_q^n \oplus \pi_1 \mathcal{R}_q^n$. Let $\mathcal{C}$ be a linear code of length n over $\mathcal{R}_q$ and $\mathbf{r} = \left(\mathbf{r}_0, \mathbf{r}_1, \ldots, \mathbf{r}_{n-1}\right) \in \mathcal{C}$. Then $\mathbf{r}_i = r_{i,0}\pi_0 + r_{i,1}\pi_1$, where $r_{i,0}$, $r_{i,1} \in \mathbb{F}_q$ and $\mathbf{r} = \left(r_{0,0}, r_{1,0}, \ldots, r_{n-1,0}\right)\pi_0 + \left(r_{0,1}, r_{1,1}, \ldots, r_{n-1,1}\right)\pi_1$. Let $\mathcal{C}_i = \Phi_i\left(\mathcal{C}\right)$ for $i = 0,1$. It is obvious that $\mathcal{C}_0$ and $\mathcal{C}_1$ are linear codes of length n over $\mathbb{F}_q$ and $\mathcal{C} = \pi 0 \mathcal{C}_0 \oplus \pi_1 \mathcal{C}_1$. This implies that for any linear code $\mathcal{C}$ over $\mathcal{R}_q$ of length n there exist linear codes $\mathcal{C}_0$ and $\mathcal{C}_1$ over $\mathbb{F}_q$ such that $\mathcal{C} = \pi_0 \mathcal{C}_0 \oplus \pi_1 \mathcal{C}_1$. The following determines the dual of linear codes over $\mathcal{R}_q$.

Proposition 3.3. Let $\mathcal{C} = \pi_0 \mathcal{C}_0 \oplus \pi_1 \mathcal{C}_1$ be a linear code of length n over $\mathcal{R}_q$. Then $\mathcal{C}^{\perp} = \pi_0 \mathcal{C}_0^{\perp} \oplus \pi_1 \mathcal{C}_1^{\perp}$. Further, $\mathcal{C}$ is a self-dual code iff both $\mathcal{C}_0$ and $\mathcal{C}_1$ are self-dual.

4. Skew cyclic codes over the ring $\mathcal{R}_q$

In this section, we will introduce basics of the skew cyclic codes over finite fields, which are important for the determining the algebraic structure of the skew cyclic codes over the non-chain ring $\mathcal{R}_q$.

For a given automorphism θ of $\mathbb{F}_q$, the set $\mathbb{F}_q[x;\theta] = \{a_0 + a_1 x + \ldots + a_1 x^n \mid a_i \in \mathbb{F}_q \text{ and } n \in N\}$ of formal polynomials forms a ring under the usual addition of polynomials and the polynomial multiplication with the restriction $xb = \theta(b)x$. The multiplication is extended to all the elements of $\mathbb{F}_q[x;\theta]$ via distributivity and associativity. This ring is called the *skew polynomial ring* over $\mathbb{F}_q$.

Definition 4.1. For a given automorphism θ of $\mathbb{F}_q$, a θ-skew cyclic code over the finite field $\mathbb{F}_q$ of length n is a linear code $\mathcal{C}$ satisfying that $\left(\theta\left(c_{n-1}\right), \theta\left(c_0\right), \ldots, \theta\left(c_{n-2}\right)\right) \in \mathcal{C}$ for each codeword $\mathbf{c} = \left(c_0, \ldots, c_{n-1}\right) \in \mathcal{C}$.

By the definition of a θ-skew cyclic code $\mathcal{C}$ over $\mathbb{F}_q$, each codeword $\mathbf{c}=(c_0,\ldots,c_{n-1})\in\mathcal{C}$ can be considered as a skew polynomial $c(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}$ in the skew quotient ring $\mathbb{F}_q[x,\theta]\big/\langle x^n-1\rangle$.

For the purpose of characterization of skew cyclic codes over $\mathcal{R}_q$, we recollect some well-known results about skew-cyclic codes over finite fields (see Refs. [2-6, 10, 17]).

The skew reciprocal polynomial of a polynomial $g(x)=\sum_{i=0}^{n-k}g_ix^i\in\mathbb{F}_q[x,\theta]$ of degree $n-k$ denoted by $g^*(x)$ is defined as $g^*(x)=\sum_{i=0}^{n-k}x^{n-k-i}g_i=\sum_{i=0}^{n-k}\theta^i(g_{n-k-i})x^i$.

If $g_0\neq 0$, the left monic skew reciprocal polynomial of $g(x)$ is $g^{\natural}(x):=\frac{1}{\theta^{n-k}(g_0)}g^*(x)$ (see Definition 3 of [4]).

From the reference [2], we have the following two results.

Proposition 4.2. Let $\mathcal{C}$ be a θ-skew cyclic code of length n over $\mathbb{F}_q$. Then there exists a monic polynomial $g(x)$ of minimal degree in $\mathcal{C}$ such that $g(x)$ is a right divisor of x^n-1 and $\mathcal{C}=\langle g(x)\rangle$.

Let $g(x)=x^m+g_{m-1}x^{m-1}+\cdots+g_0$ be a generator of a θ-skew cyclic code of length n over $\mathbb{F}_q$. It follows from $x^n-1=h(x)g(x)$ for some $h(x)\in\mathbb{F}_q[x,\theta]$ that the constant term g_0 of $g(x)$ cannot be zero in $\mathbb{F}_q$. From [2], we have the following result on the dual of θ-skew cyclic codes over $\mathbb{F}_q$.

Proposition 4.3. Let $\mathcal{C}$ be a θ-skew cyclic code of length n over $\mathbb{F}_q$ generated by a monic polynomial $g(x)$ of degree $n-k$ with $g(x)=x^{n-k}+\sum_{i=0}^{n-k-1}g_ix^i$. Then $\mathcal{C}^{\perp}$ is a θ-skew cyclic code of length n over $\mathbb{F}_q$ such that $\mathcal{C}^{\perp}=\langle h^*(x)\rangle$ where $h(x)$ is a monic polynomial of degree k such that $x^n-1=g(x)h(x)$. Moreover $h^*(x)$ is a right divisor of x^n-1.

Definition 4.4. Let $\mathcal{C}$ be a linear code of length $2n$ over $\mathbb{F}_q$ and $(\theta,\sigma)\in Aut(\mathbb{F}_q)\times S_2$. The code $\mathcal{C}$ is called double twisted with respect to (θ,σ) if for all $\mathbf{c}=(\mathbf{c}_0,\mathbf{c}_1)\in\mathcal{C}$, where $\mathbf{c}_0=(c_{0,0},c_{1,0},\ldots,c_{n-1,0})$ and $\mathbf{c}_1=(c_{0,1},c_{1,1},\ldots,c_{n-1,1})$, the word $\left(\theta\left(c_{n-1,\sigma^{-1}(0)}\right),\theta\left(c_{0,\sigma^{-1}(0)}\right),\ldots,\theta\left(c_{n-2,\sigma^{-1}(0)}\right),\theta\left(c_{n-1,\sigma^{-1}(1)}\right),\theta\left(c_{0,\sigma^{-1}(1)}\right),\ldots,\theta\left(c_{n-2,\sigma^{-1}(1)}\right)\right)\in\mathcal{C}$, where σ^{-1} is the inverse of the permutation σ.

Now, we are ready to give the definition of skew cyclic codes over $\mathcal{R}_q$.

Definition 4.5. Let $\Theta_{\theta,\sigma} \in Aut\left(\mathcal{R}_q\right)$. A linear code $\mathcal{C}$ of length n over $\mathcal{R}_q$ is said to be a $\Theta_{\theta,\sigma}$-skew cyclic code of length n over $\mathcal{R}_q$ if $\left(c_0, c_1, \ldots, c_{n-1}\right) \in \mathcal{C}$, then $\left(\Theta_{\theta,\sigma}\left(c_{n-1}\right), \Theta_{\theta,\sigma}\left(c_0\right), \ldots, \Theta_{\theta,\sigma}\left(c_{n-2}\right)\right) \in \mathcal{C}$.

We investigate the Φ-Gray images of $\Theta_{\theta,\sigma}$-skew cyclic codes over $\mathcal{R}_q$.

Proposition 4.6. Let $\Theta_{\theta,\sigma} \in Aut\left(\mathcal{R}_q\right)$. Suppose that $\mathcal{C} = \pi_0\mathcal{C}_0 \oplus \pi_1\mathcal{C}_1$ be a $\Theta_{\theta,\sigma}$-skew cyclic code of length n over $\mathcal{R}_q$. Then $\Phi\left(\mathcal{C}\right) = \left\{\Phi\left(\mathbf{c}\right) : \forall \mathbf{c} \in \mathcal{C}\right\}$ is a double twisted code of length $2n$ over $\mathbb{F}_q$ with respect to $\left(\theta, \sigma\right)$.

Proof. Let $\mathbf{c} = \left(\mathbf{c}_0, \mathbf{c}_1\right) \in \Phi\left(\mathcal{C}\right)$ where $\mathbf{c}_i = \left(c_{0,i}, c_{1,i}, \ldots, c_{n-1,i}\right) \in \mathbb{F}_q^n$. Then, $\pi_0\mathbf{c}_0 + \pi_1\mathbf{c}_1 \in \mathcal{C}$. Since $\mathcal{C}$ is a $\Theta_{\theta,\sigma}$-skew cyclic code over $\mathcal{R}_q$, we get

$$\left(\sum_{i=0}^{1}\pi_{\sigma(i)}\theta\left(c_{0,i}\right), \sum_{i=0}^{1}\pi_{\sigma(i)}\theta\left(c_{1,i}\right), \ldots, \sum_{i=0}^{1}\pi_{\sigma(i)}\theta\left(c_{n-1,i}\right)\right)$$
$$= \left(\sum_{i=0}^{1}\pi_i\theta\left(c_{0,\sigma^{-1}(i)}\right), \sum_{i=0}^{1}\pi_i\theta\left(c_{1,\sigma^{-1}(i)}\right), \ldots, \sum_{i=0}^{1}\pi_i\theta\left(c_{n-1,\sigma^{-1}(i)}\right)\right)$$
$$= \left(\theta\left(c_{0,\sigma^{-1}(0)}\right), \theta\left(c_{1,\sigma^{-1}(0)}\right), \ldots, \theta\left(c_{n-1,\sigma^{-1}(0)}\right)\right)\pi_0 + \left(\theta\left(c_{0,\sigma^{-1}(1)}\right), \theta\left(c_{1,\sigma^{-1}(1)}\right), \ldots, \theta\left(c_{n-1,\sigma^{-1}(1)}\right)\right)\pi_1 \in \mathcal{R}_q.$$

Therefore, we have

$$\left(\theta\left(c_{n-1,\sigma^{-1}(0)}\right), \theta\left(c_{0,\sigma^{-1}(0)}\right), \ldots, \theta\left(c_{n-2,\sigma^{-1}(0)}\right), \theta\left(c_{n-1,\sigma^{-1}(1)}\right), \theta\left(c_{0,\sigma^{-1}(1)}\right), \ldots, \theta\left(c_{n-2,\sigma^{-1}(1)}\right)\right) \in \Phi(\mathcal{C}),$$

which completes the proof.

As an immediate result of Proposition 4.6, letting $\sigma = id$ and $\Theta_{\theta,id} = \Theta_\theta$ we deduce the following theorem.

Theorem 4.7. Let $\Theta_\theta \in Aut\left(\mathcal{R}_q\right)$. Suppose that $\mathcal{C} = \pi_0\mathcal{C}_0 \oplus \pi_1\mathcal{C}_1$ be a linear code of length n over $\mathcal{R}_q$. Then $\mathcal{C}$ is a Θ_θ-skew cyclic code over $\mathcal{R}_q$ of length n if and only if $\mathcal{C}_i$ is a θ-skew cyclic code over $\mathbb{F}_q$ of length n.

Proof. It follows from the proof of Proposition 4.6 by taking $\sigma = id$.

Hereafter, we only consider the automorphism $\Theta_\theta = \Theta_{\theta,id}$ defined by $\Theta_\theta : \mathcal{R}_q \longrightarrow \mathcal{R}_q$, $\Theta_\theta\left(r_0\pi_0 + r_1\pi_1\right) \mapsto \theta\left(r_0\right)\pi_0 + \theta\left(r_1\right)\pi_1$, where $\theta \in Aut\left(\mathbb{F}_q\right)$.

Now, we give a generator of a Θ_θ-skew cyclic code over $\mathcal{R}_q$.

Proposition 4.8. Let $\Theta_\theta \in Aut\left(\mathcal{R}_q\right)$. Suppose that $\mathcal{C} = \pi_0\mathcal{C}_0 \oplus \pi_1\mathcal{C}_1$ be a Θ_θ-skew cyclic code of length n over $\mathcal{R}_q$. Then there exists polynomials $g_0(x)$ and $g_1(x) \in \mathbb{F}_q\left[x,\theta\right]$ such that $\mathcal{C} = \left\langle \pi_0 g_0(x), \pi_1 g_1(x) \right\rangle$ with $\mathcal{C}_i = \left\langle g_i \right\rangle \subseteq {\mathbb{F}_q\left[x,\theta\right]}\Big/{\left\langle x^n - 1\right\rangle}$.

Proof. Let $\mathcal{E} = \left\langle \pi_0 g_0(x), \pi_1 g_1(x) \right\rangle$ and let $\mathbf{c}\left(x\right) = \mathbf{c}_0\left(x\right)\pi_0 + \mathbf{c}_1\left(x\right)\pi_1 \in \mathcal{C}$ such that $\mathbf{c}_i\left(x\right) \in \mathcal{C}_i$. Since $\mathcal{C}_i = \left\langle g_i \right\rangle$ is a left submodule of the skew ring ${\mathbb{F}_q\left[x,\theta\right]}\Big/{\left\langle x^n - 1\right\rangle}$, there exist l_0 and $l_1 \in \mathbb{F}_q\left[x,\theta\right]$ such that $\mathbf{c}\left(x\right) = l_0\left(x\right)\mathbf{c}_0\left(x\right)\pi_0 + l_1\left(x\right)\mathbf{c}_1\left(x\right)\pi_1 \in \mathcal{E}$ and hence $\mathcal{C} \subset \mathcal{E}$.

On the other hand, let $\mathbf{e} \in \mathcal{E}$, then there exist k_0 and $k_1 \in {\mathbb{F}_q\left[x,\theta\right]}\Big/{\left\langle x^n - 1\right\rangle}$ such that $\mathbf{e}\left(x\right) = k_0\left(x\right)g_0\left(x\right)\pi_0 + k_1\left(x\right)g_1\left(x\right)\pi_1$. Then there exist b_0 and $b_1 \in \mathbb{F}_q\left[x,\theta\right]$ such that $\pi_i b_i\left(x\right) = \pi_i k_i\left(x\right)$, thus $\mathbf{e}\left(x\right) = b_0\left(x\right)g_0\left(x\right)\pi_0 + b_1\left(x\right)g_1\left(x\right)\pi_1 \in \mathcal{C}$. This shows that $\mathcal{E} \subset \mathcal{C}$ and hence completes the proof.

We give the exact characterization of Θ_θ-skew cyclic codes over $\mathcal{R}_q$ as a consequence of Proposition 4.8.

Theorem 4.9. Let $\Theta_\theta \in Aut\left(\mathcal{R}_q\right)$. Suppose that $\mathcal{C} = \pi_0\mathcal{C}_0 \oplus \pi_1\mathcal{C}_1$ be a Θ_θ-skew cyclic code of length n over $\mathcal{R}_q$. Then $\mathcal{C}$ is principally generated with $\mathcal{C} = \left\langle g\left(x\right)\right\rangle$, where $g\left(x\right) = g_0\left(x\right)\pi_0 + g_1\left(x\right)\pi_1$ and $g\left(x\right)$ is a right divisor of $x^n - 1$ in $\mathcal{R}_q\left[x,\Theta_\theta\right]$.

Proof. It is apparent that $\left\langle g\left(x\right)\right\rangle \subset \mathcal{C}$. Since $\pi_0 g\left(x\right) = \pi_0 g_0\left(x\right)$ and $\pi_1 g\left(x\right) = \pi_1 g_1\left(x\right)$, we have $\mathcal{C} \subset \left\langle g\left(x\right)\right\rangle$. This implies that $\mathcal{C} = \left\langle g\left(x\right)\right\rangle$. Since $g_i\left(x\right)$ is a right divisor of $x^n - 1$, there exists $h_i\left(x\right) \in \mathbb{F}_q\left[x,\theta\right]$ such that $x^n - 1 = h_i\left(x\right)g_i\left(x\right)$. Seeing that $\pi_i\left(x^n - 1\right) = \pi_i\left(x^n - 1\right)$, hence

$$\begin{aligned}\left(\pi_0 h_0\left(x\right) + \pi_1 h_1\left(x\right)\right)\left(\pi_0 g_0\left(x\right) + \pi_1 g_1\left(x\right)\right) &= \pi_0 h_0\left(x\right)g_0\left(x\right) + \pi_1 h_1\left(x\right)g_1\left(x\right)\\ &= \pi_0\left(x^n - 1\right) + \pi_1\left(x^n - 1\right)\\ &= \pi_0\left(x^n - 1\right) + \pi_1\left(x^n - 1\right)\\ &= \left(\pi_0 + \pi_1\right)\left(x^n - 1\right) = x^n - 1.\end{aligned}$$

This shows that $\pi_0 h_0\left(x\right) + \pi_1 h_1\left(x\right)$ is a right divisor of $x^n - 1$.

Proposition 3.3, Proposition 4.2, Theorem 4.7 and Theorem 4.9 together imply the following result:

Theorem 4.10. Let $\Theta_\theta \in Aut(\mathcal{R}_q)$. If $\mathcal{C} = \pi_0\mathcal{C}_0 \oplus \pi_1\mathcal{C}_1$ is a Θ_θ-skew cyclic code of length n over $\mathcal{R}_q$ with $\mathcal{C}_i = \langle g_i(x) \rangle$, $g_i(x) = x^{n-k_i} + \sum_{j=0}^{n-k_i-1} g_{ij}x^j$, then $C^\perp = \langle h^*(x) \rangle$ is a Θ_θ-skew cyclic code of length n over $\mathcal{R}_q$, where $h^*(x) = \sum_{i=0}^{1} \pi_i h_i^*(x)$.

Proof. Recall that $\mathcal{C}^\perp = \pi_0\mathcal{C}_0^\perp + \pi_1\mathcal{C}_1^\perp$ by Proposition 4.2 and $\mathcal{C}_i = \langle h_i^* \rangle$ is a Θ_θ-skew cyclic code over $\mathbb{F}_q$ by Proposition 4.3. Then, by Theorem 4.7, $\mathcal{C}^\perp$ is a Θ_θ-skew cyclic code over $\mathcal{R}_q$. Finally, Theorem 4.9 gives the generator polynomial $h^*(x)$ of $\mathcal{C}^\perp$.

5. Conclusion and future remarks

In this paper, by determining the automorphism group of the ring $\mathcal{R}_q$ we define and study the skew cyclic codes over $\mathcal{R}_q$. We characterize the algebraic structure of skew cyclic codes and their duals over $\mathcal{R}_q$. We also investigate the Φ-images of skew cyclic codes over $\mathcal{R}_q$. As a future direction, we will consider the structure of skew constacyclic codes and their duals over $\mathcal{R}_q$.

References

[1] Amarra, M. C. V., Nemenzo, F. R., "On $(1-u)$-cyclic codes over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$", Applied Mathematics Letters 21(11) (2008) : 1129-1133.

[2] Boucher, D., Geiselmann, W., Ulmer, F., "Skew-cyclic codes", Applicable Algebra in Engineering, Communication and Computing 18(4) (2007) : 379-389.

[3] Boucher, D., Solé, P., Ulmer, F., "Skew constacyclic codes over Galois rings", Advances in mathematics of communications 2(3) (2008) : 273.

[4] Boucher, D. and Ulmer, F., "Codes as modules over skew polynomial rings", In IMA International Conference on Cryptography and Coding (2009) : 38-55.

[5] Boucher, D. and Ulmer, F., "Coding with skew polynomial rings", Journal of Symbolic Computation 44(12) (2009) : 1644-1656.

[6] Boucher, D., Ulmer, F., "Self-dual skew codes and factorization of skew polynomials", Journal of Symbolic Computation 60 (2014) : 47-61.

[7] Bonnecaze, A., Udaya, P., "Cyclic codes and self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$", IEEE Transactions on Information Theory 45(4) (1999) : 1250-1255.

[8] Dinh, H. Q., López-Permouth, S. R., "Cyclic and negacyclic codes over finite chain rings", IEEE Transactions on Information Theory 50(8) (2004) : 1728-1744.

[9] Dinh, H. Q., "Constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$", Journal of Algebra 324(5) (2010) : 940-950.

[10] Gao, J., Ma, F., Fu, F., "Skew constacyclic codes over the ring $\mathbb{F}_q + v\mathbb{F}_q$", Applied and Computational Mathematics 6(3) (2017) : 286-295.
[11] Gao, J., "Skew cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q$", Journal of Applied Mathematics and Informatics 31(3-4) (2013) : 337-342.
[12] Gursoy, F., Siap, I., Yildiz, B., "Construction of skew cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q$", Advances in Mathematics of Communications 8(3) (2014) : 313-322.
[13] Jitman, S., Ling, S., Udomkavanich, P., "Skew constacyclic codes over finite chain rings", Advances in Mathematics of Communications 6(1) (2012) : 39-63.
[14] Martìnez-Moro, E., Rùa, I. F., "Multivariable codes over finite chain rings: serial codes", SIAM Journal on Discrete Mathematics 20(4) (2006) : 947-959.
[15] Shi, M., Yao, T., Solè, P., "Skew cyclic codes over a non-chain ring", Chin. J. Electron. 26(3) (2017) : 544-547.
[16] Norton, G. H., Sâlâgean, A., "Strong Gröbner bases and cyclic codes over a finite-chain ring", Electron. Notes Discrete Math. 6(2001) : 240-250.
[17] Siap, I., Abualrub, T., Aydin, N., Seneviratne, P., "Skew Cyclic codes of arbitrary length", Int. J. Information and Coding Theory 2(1) (2011) : 10-20.