Turk. J. Math. Comput. Sci.
15(1)(2023) 96–103
© MatDer
DOI : 10.47000/tjmcs.995569

Skew Cyclic Codes over $\mathbb{Z}_8 + u\mathbb{Z}_8 + v\mathbb{Z}_8$

Basri Çalışkan[1,*], Kemal Balıkçı[2]

[1]Department of Mathematics, Faculty of Arts and Science, Osmaniye Korkut Ata University, 80000, Osmaniye, Türkiye.
[2]Department of Electrical Engineering, Engineering Faculty, Osmaniye Korkut Ata University, 80000, Osmaniye, Türkiye.

Received: 14-09-2021 • Accepted: 14-05-2023

Abstract. In this paper, we study skew-cyclic codes over the ring $S = \mathbb{Z}_8 + u\mathbb{Z}_8 + v\mathbb{Z}_8$, where $u^2 = u$, $v^2 = v$, $uv = vu = 0$. We consider these codes as left $S[x, \theta]$-submodules and use Gray map on S to obtain their $\mathbb{Z}_8$-images. The generator and parity-check matrices of a free θ-cyclic code of even length over S are determined. Also, these codes are generalized to double skew-cyclic codes. We give some examples using Magma computational algebra system.

2010 AMS Classification: 94B05, 94B15, 11T71

Keywords: Double-cyclic codes, Gray map, linear codes, skew-cyclic codes.

1. Introduction

Since the beginning of the coding theory, a great deal of work has been done on cyclic codes, which is a class of linear codes in coding theory. Cyclic codes are defined over some algebraic structures such as finite fields, finite rings etc. and are invariant under a cyclic shift of coordinates. Also, these codes are described as ideals of $\mathbb{F}_q/\langle x^t - 1\rangle$. They are convenient to implement, they have nice algebraic structures, and they have various important generalizations [4–8, 10]. While initially mostly commutative and finite chain rings were used, in 2007, Boucher and Ulmer [3] gave a new direction to the study of cyclic codes by defining a generalization thereof in the non-commutative setting of skew polynomial rings. These codes are known as skew-cyclic codes. The authors studied linear codes using skew-polynomial rings with automorphism defined on the field $\mathbb{F}_q$. Skew polynomial ring is denoted by $\mathbb{F}_q[x, \theta]$, where the addition is defined as the usual one of polynomials and the multiplication is defined by the rule $xa = \theta(a)x, a \in \mathbb{F}_q$. Also, they found skew cyclic codes with greater minimum distances than previously well-known codes [2].

Then, the skew-cyclic codes over different rings were presented in [9, 11, 13, 15]. More recently, in [14] skew-cyclic codes over the ring $\mathbb{Z}_4 + u\mathbb{Z}_4$, where $u^2 = 1$ have been studied. Also, the authors in [12] studied skew-constacyclic codes over the ring $\mathbb{Z}_q(\mathbb{Z}_q + u\mathbb{Z}_q)$, where $q = p^s$ for a prime p and $u^2 = 0$. In [7], the structures of cyclic codes over the ring $S = \mathbb{Z}_8 + u\mathbb{Z}_8 + v\mathbb{Z}_8$, where $u^2 = u$, $v^2 = v$, $uv = vu = 0$ were determined.

The aim of this paper is to introduce and study skew-cyclic codes over the ring $S = \mathbb{Z}_8 + u\mathbb{Z}_8 + v\mathbb{Z}_8$, where $u^2 = u$, $v^2 = v$, $uv = vu = 0$. Some structural properties of the skew polynomial ring $S[x, \theta]$ are discussed, where θ is an automorphism of S. We determine the generator and parity-check matrices of these codes. Also, we investigate the Gray images of the codes and give some examples.

*Corresponding Author
Email addresses: bcaliskan@osmaniye.edu.tr (B. Çalışkan), kbalikci@osmaniye.edu.tr (K. Balıkçı)

2. Preliminaries

Consider the ring $S = \mathbb{Z}_8 + u\mathbb{Z}_8 + v\mathbb{Z}_8$, where $u^2 = u$, $v^2 = v$, $uv = vu = 0$. It can be also viewed as the quotient ring $\mathbb{Z}_8[u, v]/\left\langle u^2 - u, v^2 - v, uv - vu\right\rangle$. Let d be any element of S, which can be expressed uniquely as $d = a + ub + vc$, where $a, b, c \in \mathbb{Z}_8$ [6].

The ring S has the following properties:

- It has 512 elements.
- Its units are given by

$$U = \{a + ub + vc \mid a \in \{1, 3, 5, 7\}, b, c \in \{0, 2, 4, 6\}\}.$$

- It has a total of 64 ideals.

To know more about the ring S, we refer to [6]. Recall that a linear code C of length n over the ring S is an S-submodule of S^n. A codeword is denoted as $\mathbf{d} = (d_0, d_1, \ldots, d_{n-1})$ [6].

A cyclic shift operator is defined as:

$$\sigma(d_0, d_1, \ldots, d_{n-1}) = (d_{n-1}, d_0, \ldots, d_{n-2}).$$

Let C be a linear code of length n over S, then C is called cyclic if $\sigma(C) = C$.

It is known that the Lee weight w_L of any element a of $\mathbb{Z}_8$ is

$$w_L(a) = \min\{|a|, |8 - a|\}.$$

The Lee weight $w_L(w)$ of a vector, $w \in \mathbb{Z}_8^3$ is defined as the rational sum of the Lee weights of its coordinates. In [6] the Gray map was defined as follows

$$\begin{aligned} \phi : S &\to \mathbb{Z}_8^3 \\ a + ub + vc &\mapsto (a, a + b, a + c). \end{aligned}$$

For any element $d = a + ub + vc \in S$, the Gray weight $w_G(d)$ of d is defined as $w_G(d) = w_L(\phi(d))$. That is,

$$w_L(d) = w_L(a, a + b, a + c),$$

where $a, b, c \in \mathbb{Z}_8$ [6].

This map is extended componentwise to

$$\Phi : S^n \to \mathbb{Z}_8^{3n}$$

and the Gray weight $w_G(d)$ of $d \in \mathbb{Z}_8^{3n}$ is defined as the rational sum of Gray weights of its coordinates.

3. Skew Polynomial Ring over $\mathbb{Z}_8 + u\mathbb{Z}_8 + v\mathbb{Z}_8$

In this section we study the structure of the non-commutative ring $S[x, \theta]$.

Define a map

$$\begin{aligned} \theta &: S \to S \\ a + ub + vc &\mapsto a + uc + vb, \end{aligned}$$

where $a, b, c \in \mathbb{Z}_8$.

Let $d = a + ub + vc,\ d' = a' + ub' + vc' \in S$.

$$\begin{aligned} \theta(d + d') &= \theta((a + ub + vc) + (a' + ub' + vc')) \\ &= \theta(a + a' + u(b + b') + v(c + c')) \\ &= a + a' + u(c + c') + v(b + b') \\ &= a + uc + vb + a' + uc' + vb' \\ &= \theta(d) + \theta(d'), \end{aligned}$$

$$\begin{aligned} \theta(dd') &= \theta((a + ub + vc)(a' + ub' + vc')) \\ &= \theta(aa' + u(ab' + ba' + bb') + v(ac' + ca' + cc')) \\ &= aa' + u(ac' + ca' + cc') + v(ab' + ba' + bb'), \end{aligned}$$

$$\begin{aligned}\theta(d)\theta(d') &= \theta(a+ub+vc)\theta(a'+ub'+vc') \\ &= (a+uc+vb)(a'+uc'+vb') \\ &= aa'+u(ac'+ca'+cc')+v(ab'+ba'+bb').\end{aligned}$$

Above discussion shows that θ is a nontrivial automorphism of S. Moreover, since $\theta^2(d) = d$ for all $d \in S$, the order of θ is 2. Note that the automorphism θ fixes every element of $\mathbb{Z}_8$.

The ring $S[x,\theta] = \left\{a_0 + a_1x + \ldots + a_{n-1}x^{n-1} : a_i \in S, n \in \mathbb{N}\right\}$ is called skew polynomial ring and an element in $S[x,\theta]$ is called a skew polynomial. The addition is defined as the ordinary addition of polynomials and the multiplication is defined by the rule

$$xd = \theta(d)x$$

for any $d \in S$. The multiplication is extended to all elements in $S[x,\theta]$ by associativity and distributivity.

Example 3.1. Let $p = ux + 5$ and $p' = x + u$ be in $S[x,\theta]$. Then,

$$\begin{aligned}pp' &= (ux+5)(x+u) \\ &= ux^2 + u(\theta(u)x) + 5x + 5u \\ &= ux^2 + 5x + 5u\end{aligned}$$

and

$$\begin{aligned}p'p &= (x+u)(ux+5) \\ &= (\theta(u)x)x + 5x + u^2x + 5u \\ &= vx^2 + (u+5)x + 5u.\end{aligned}$$

It is clear that the coefficients of the terms x^2 and x are different. Therefore, $pp' \neq p'p$. Thus, $S[x,\theta]$ is a non-commutative ring.

Lemma 3.2. *Let $d \in S$ be a unit in S. Then, $\theta(d)$ is a unit in S.*

Proof. Let $d = a + ub + vc$ be a unit in S such that $a \in \{1,3,5,7\}$, $b, c \in \{0,2,4,6\}$. Then, from the definition of θ, we have

$$\theta(d) = a + cu + bv.$$

So, it is clear that $\theta(d)$ is a unit in S. □

Lemma 3.3. *Let $S^\theta = \{\alpha + u\beta + v\gamma | \alpha, \beta, \gamma \in \mathbb{Z}_8,\ \beta = \gamma\}$. Then, S^θ is a subring of S fixed by θ.*

Proof. Let $\alpha + u\beta + v\gamma$ be an element in $\in S^\theta$. Then,

$$\theta(\alpha + u\beta + c\gamma) = \alpha + \gamma u + \beta v$$

and the element $\alpha + u\beta + v\gamma$ is fixed by θ if and only if $\beta = \gamma$. It is clear that S^θ is a subring of S. □

Definition 3.4. A polynomial $p(x) \in S[x,\theta]$ is said to be a central polynomial if

$$p(x)r(x) = r(x)p(x)$$

for all $r(x) \in S[x,\theta]$ [14]. From now on, the center of $S[x,\theta]$ will be denoted by $Z(S[x,\theta])$.

Theorem 3.5. $Z(S[x,\theta]) = \left\{\sum_{i=0}^{l} d_i x^{2i} | d_i \in S^\theta\right\}$.

Proof. Let $D = \left\{\sum_{i=0}^{l} d_i x^{2i} | d_i \in S^\theta\right\}$ and $p = \sum_{i=0}^{l} d_i x^{2i} \in D$. Since the order of θ is 2, for any non-negative integer i, we have

$$x^{2i}d_i = \left(\theta^2\right)^i (d_i)x^{2i} = d_i x^{2i}$$

for all $d_i \in S^\theta$. This implies $x^{2i} \in Z(S[x,\theta])$, and hence all polynomials of the form

$$p = d_0 + d_1x^2 + d_2x^4 + \cdots + d_lx^{2l}$$

with $d_i \in S^\theta$ are in the $Z(S[x,\theta])$. Therefore, $D \subseteq Z(S[x,\theta])$.

Conversely, let $p = p_0 + p_1 x + p_2 x^2 + \cdots + p_k x^k \in Z(S[x,\theta])$. We have $px = xp$ which gives that all p_i are fixed by θ, so that $p_i \in S^{\theta}$. Next, choose $d \in S$ such that $\theta(d) \neq d$. Now it follows from the relation $dp(x) = p(x)d$ that $p_i = 0$ for all indices i not dividing 2. Thus,

$$p(x) = d_0 + d_1 x^2 + d_2 x^4 + \cdots + d_\ell x^{2\ell} \in D.$$

So, $Z(S[x,\theta]) \subseteq D$, and completes the proof. □

Corollary 3.6. *Let $p(x) = x^m - 1$. Then, $p(x) \in Z(S[x,\theta])$ if and only if $2|m$.*

The Corollary 3.6 shows that if m is even, then the quotient space $S[x,\theta]/\langle x^m - 1\rangle$ is a ring and the polynomial $(x^m - 1)$ is in the $Z(S[x,\theta])$ of the ring $S[x,\theta]$, hence generates a two-sided ideal if and only if $2 \mid m$. Otherwise, it is just an S-module.

Example 3.7. Let $p(x) = (1 + 7u + 7v)x^2 + 5$, $q(x) = (1 + 7u + 7v)x$. Then,

$$\begin{aligned} p(x) &= xq(x) + 5 \\ p(x) &= (1 + 7u + 7v)xq(x) + 5 \end{aligned}$$

It is clear that $x \neq (1 + 7u + 7v)x$ and $deg(5) < deg((1 + 7u + 7v)x)$.

So $S[x,\theta]$ is not Euclidean. Therefore, division algorithm does not hold in it. But division algorithm can be applied on some particular elements of $S[x,\theta]$.

Theorem 3.8. *[14] Let $f(x), g(x) \in S[x,\theta]$ be such that the leading coefficient of $g(x)$ is a unit. Then, there exist $q(x), r(x) \in S[x,\theta]$ such that*

$$f(x) = q(x)g(x) + r(x),$$

where $r(x) = 0$ or $deg(r(x)) < deg(g(x))$.

4. Skew Cyclic Codes over $\mathbb{Z}_8 + u\mathbb{Z}_8 + v\mathbb{Z}_8$

In this section we are interested in studying skew-cyclic codes over S, also called θ-cyclic codes.

A code of length n over S is a nonempty subset of S^n. A code C is said to be linear if it is a submodule of the S-module of S^n.

Definition 4.1. Let θ be an automorphism in S. A code C is said to be θ-cyclic if C is closed under the θ-cyclic shift:

$$\sigma_\theta : S^n \longrightarrow S^n$$

defined by

$$\sigma_\theta(z_0, z_1, \ldots, z_{n-1}) = (\theta(z_{n-1}), \theta(z_0), \ldots, \theta(z_{n-2})).$$

Let $\frac{S[x,\theta]}{\langle p(x)\rangle}$, where $p(x)$ is an arbitrary polynomial of degree n over S. In polynomial representation, we can associate a word $z = (z_0, z_1, \ldots, z_{n-1})$ to the corresponding polynomial

$$z(x) = z_0 + z_1 x + \ldots + z_{n-1} x^{n-1}.$$

Moreover $\frac{S[x,\theta]}{\langle p(x)\rangle}$ is a left $S[x,\theta]$-module with respect to the multiplication $r(x)(z(x) + \langle p(x)\rangle) = r(x)z(x) + \langle p(x)\rangle$.

Theorem 4.2. *A code C of length n over S is a θ-cyclic code if and only if C is a left $S[x,\theta]$-submodule of the left $S[x,\theta]$-module of $S_n = \frac{S[x,\theta]}{\langle x^n - 1\rangle}$.*

Proof. Assume that, C is a θ-cyclic of length n over S and $z, z' \in C$. Let $z(x) = z_0 + z_1 x + \ldots + z_{n-1} x^{n-1}$ and $z'(x) = z'_0 + z'_1 x + \ldots + z'_{n-1} x^{n-1}$. Since C is a linear code, $z + z' \in C$. Also, all $x^i z(x)$ belong to C for all $i \in \mathbb{N}$, because C is cyclic. This means that $p(x)z(x) \in C$ for all $p(x) \in S_n$. So C is a submodule. Now suppose that C is a submodule of S_n and $z, z' \in C$. Then, by definition of submodule we have $z + z' \in C$ and $x^i z(x) \in C$. So C is a θ-cyclic code over S. □

Corollary 4.3. *If C is a θ-cyclic of even length n over S, then C is an ideal of $S_n = \frac{S[x,\theta]}{\langle x^n - 1\rangle}$.*

Proof. Let n be an even integer. Then, $\langle x^n - 1\rangle$ is a two sided ideal and so the quotient space $S_n = \frac{S[x,\theta]}{\langle x^n - 1\rangle}$ is a ring. □

Theorem 4.4. *Let C be a cyclic code of length n over S such that C contains a minimum degree polynomial $g(x)$ whose leading coefficient is a unit. Then $C = \langle g(x)\rangle$. Moreover $g(x)|(x^n - 1)$ and the set*

$$\left\{g(x), xg(x), \ldots, xg(x)^{n-deg(g(x))-1}g(x)\right\}$$

forms a basis for C.

Proof. The proof is similar to the proof of Theorem 14 [14]. □

4.1. **Generator Matrix.** In this subsection we find a set of generators for a free θ-cyclic code of length n over S.

Let $C = \langle g(x)\rangle$ be a cyclic code of length n over S generated by a right divisor $g(x)$ of $x^n - 1$. Then, a generator matrix of C is the $(n-k)\times n$ matrix

$$\begin{bmatrix} g(x) \\ xg(x) \\ x^2g(x) \\ \vdots \\ x^{n-k-1}g(x) \end{bmatrix}_{(n-k)\times n},$$

where $g(x) = g_0 + g_1x + g_2x^2 + \cdots + g_kx^k$. More precisely,

$$G = \begin{bmatrix} g_0 & g_1 & \cdots & g_k & 0 & \cdots & 0 \\ 0 & \theta(g_1) & \cdots & \theta(g_{k-1}) & \theta(g_k) & \cdots & 0 \\ 0 & 0 & \cdots & g_{k-2} & g_{k-2} & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \\ 0 & 0 & \cdots & \theta(g_0) & \theta(g_1) & \cdots & \theta(g_k) \end{bmatrix}_{(n-k)\times n}.$$

Example 4.5. Let C be a θ-cyclic code of length 6 over S generated by the right divisor $g(x) = (1+2u+2v)x^3 + (6+6u+6v)x^2 + (2+2u+2v)x + 1 + 4u + 4v$ of $x^6 - 1$. Then, the set

$$\begin{aligned} \left\{g(x), xg(x), x^2g(x)\right\} = & \left\{(1+2u+2v)x^3 + (6+6u+6v)x^2 + (2+2u+2v)x + 1 + 4u + 4v,\right. \\ & (1+2u+2v)x^4 + (6+6u+6v)x^3 + (2+2u+2v)x^2 + (1+4u+4v)x, \\ & \left.(1+2u+2v)x^5 + (6+6u+6v)x^4 + (2+2u+2v)x^3 + (1+4u+4v)x^2\right\} \end{aligned}$$

forms a basis for C. Therefore, C has cardinality 8^9. The generator matrix of C can be given as

$$\begin{bmatrix} 1+4u+4v & 2+2u+2v & 6+6u+6v & 1+2u+2v & 0 & 0 \\ 0 & 1+4u+4v & 2+2u+2v & 6+6u+6v & 1+2u+2v & 0 \\ 0 & 0 & 1+4u+4v & 2+2u+2v & 6+6u+6v & 1+2u+2v \end{bmatrix}.$$

Also the Gray image of the generator matrix of C is,

$$\begin{bmatrix} 155 & 244 & 644 & 133 & 000 & 000 \\ 000 & 155 & 244 & 644 & 133 & 000 \\ 000 & 000 & 155 & 211 & 644 & 133 \end{bmatrix}.$$

Using the computational algebra system Magma [1] for computations, we obtain $\Phi(C)$ has parameters $(18, 8^9, 2)$.

5. Duals of θ-Cyclic Codes over S

In this section, we present the structure of the dual of a free θ-cyclic code of even length n over S.

Definition 5.1. Let C be θ-cyclic code of length n over S. Then, the dual of C is defined as

$$C^\perp = \{\mathbf{w} \mid \mathbf{w}\cdot\mathbf{z} = 0 \text{ for all } \mathbf{z} \in C\},$$

where $\mathbf{w}\cdot\mathbf{z}$ denotes the usual inner product of $\mathbf{w}$ and $\mathbf{z}$, where $\mathbf{w} = (w_0, w_1, \ldots, w_{n-1})$ and $\mathbf{z} = (z_0, z_1, \ldots, z_{n-1})$ belong to S^n.

We need some lemmas for determining a generator matrix of a free θ-cyclic code C.

Lemma 5.2. *For even n, $x^n - 1$ is a central element of $S[x, \theta]$, and hence $x^n - 1 = h(x)g(x) = g(x)h(x)$ for some $g(x), h(x) \in S[x, \theta]$.*

Proof. The proof is similar to the proof of Lemma 7 [2]. □

Remark 5.3. If C is a θ-cyclic code generated by a minimum degree polynomial $g(x)$ with its leading coefficient a unit, then there exists a minimum degree monic polynomial $g_1(x)$ in C such that $C = \langle g_1(x) \rangle$.

Lemma 5.4. *Let $g(x)$ be a monic right divisor of $x^n - 1$ and C be a θ-cyclic code of even length n over S generated by $g(x)$. Then, $z(x) \in S_n$ is in C if and only if $z(x)h(x) = 0$ in S_n, where $x^n - 1 = h(x)g(x)$.*

Proof. Assume that, $z(x)h(x) = 0$ in S_n for some $z(x) \in S_n$. Then, there exists $p(x) \in S[x, \theta]$ such that

$$\begin{aligned} z(x)h(x) &= p(x)(x^n - 1) \\ &= p(x)h(x)g(x) \\ &= p(x)g(x)h(x). \end{aligned}$$

So we have $z(x) = p(x)g(x)$, thus $z(x) \in C$.

Conversely, suppose that $z(x) \in C$. Then, $z(x) = k(x)g(x)$ for some $k(x) \in S_n$. So

$$z(x)h(x) = k(x)g(x)h(x) = k(x)h(x)g(x) = 0$$

in S_n (by Lemma 5.2). Hence, the proof is completed. □

Theorem 5.5. *Let C be a θ-cyclic code of even length n over S generated by $g(x)$, such that $x^n - 1 = h(x)g(x)$ for some $h(x) = h_0 + h_1x + h_2x^2 + \cdots + h_kx^k \in S[x, \theta]$, where k is odd. Then, the matrix*

$$H = \begin{bmatrix} h_k & \theta(h_{k-1}) & \cdots & h_3 & \theta(h_2) & \cdots & 0 \\ 0 & \theta(h_k) & \cdots & h_4 & \theta(h_3) & \cdots & 0 \\ 0 & 0 & \cdots & h_5 & \theta(h_4) & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \cdots & \cdots & \cdots & \theta(h_0) \end{bmatrix}_{(n-k)\times n}$$

is a generator matrix for $C^\perp$.

Proof. Let $z(x) \in C$. Then, by Lemma 5.4, we have $z(x)h(x) = 0$ in $S_{n,\theta}$. Thus, the coefficients of $x^k, x^{k+1}, \ldots, x^{n-1}$ in $[z_0 + z_1x + z_2x^2 + \cdots + z_{n-2}x^{n-2} + z_{n-1}x^{n-1}][h_0 + h_1x + h_2x^2 + \cdots + h_{k-1}x^{k-1} + h_kx^k]$ are all zero. Then,

$$\begin{aligned} z_0h_k + z_1\theta(h_{k-1}) + z_2h_{k-2} + \cdots + z_k\theta(h_0) &= 0 \\ z_1\theta(h_k) + z_2h_{k-1} + z_3\theta(h_{k-2}) \cdots + z_{k+1}h_0 &= 0 \\ z_2h_k + z_3\theta(h_{k-1}) + z_4h_{k-2} + \cdots + z_{k+2}\theta(h_0) &= 0 \\ \vdots \qquad & \quad \vdots \\ z_{n-k-1}h_k + z_{n-k}\theta(h_{k-1}) + z_{n-k+1}h_{k-2} + \cdots + z_{n-1}\theta(h_0) &= 0. \end{aligned}$$

It is easy check that for any $z \in C$, $zH^T = 0$, and therefore $GH^T = 0$. Since the rows of H are orthogonal to each $z \in C$, $span(H) \subseteq C^\perp$. Further, since H is a lower triangular matrix with all diagonal entries units (by Lemma 3.2), it contains a square sub-matrix of order $n - k$ with non-zero determinant. So we have that all rows of H are linearly independent. Hence, $|Span(H)| = |S|^{n-k}$. Moreover, $|C|\left|C^\perp\right| = |S|^n$ and $|C| = |S|^k$ give $\left|C^\perp\right| = |S|^{n-k}$. Thus, $Span(H) = C^\perp$, and so H is a generator matrix for $C^\perp$. □

When k is even, H can be taken as:

$$H = \begin{bmatrix} h_k & \theta(h_{k-1}) & \cdots & h_0 & 0 & \cdots & 0 \\ 0 & \theta(h_k) & \cdots & h_1 & \theta(h_0) & \cdots & 0 \\ 0 & 0 & \cdots & h_2 & \theta(h_1) & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \cdots & \theta(h_k) & \cdots & h_0 \end{bmatrix}_{(n-k)\times n}.$$

Example 5.6. Let C be a θ-cyclic code of length 6 generated by the polynomial $g(x) = (1 + 2u + 2v)x^3 + (6 + 6u + 6v)x^2 + (2 + 2u + 2v)x + 1 + 4u + 4v$ of $x^6 - 1$ such that

$$\begin{aligned} x^6 - 1 &= \Big((1 + 2u + 2v)x^3 + (2 + 2u + 2v)x^2 + (2 + 2u + 2v)x + 7 + 4u + 4v\Big) \\ &\quad \Big((1 + 2u + 2v)x^3 + (6 + 6u + 6v)x^2 + (2 + 2u + 2v)x + 1 + 4u + 4v\Big). \end{aligned}$$

Let $h(x) = (1 + 2u + 2v)x^3 + (2 + 2u + 2v)x^2 + (2 + 2u + 2v)x + 7 + 4u + 4v$. Then, a parity check matrix of C (by Theorem 5.5) is given by

$$H = \begin{bmatrix} 1+2u+2v & 2+2u+2v & 2+2u+2v & 7+4u+4v & 0 & 0 \\ 0 & 1+2u+2v & 2+2u+2v & 2+2u+2v & 7+4u+4v & 0 \\ 0 & 0 & 1+2u+2v & 2+2u+2v & 2+2u+2v & 7+4u+4v \end{bmatrix}.$$

It is clear that, $GH^T = 0$ and the rows of H are linearly independent. Thus, H forms a generator matrix for $C^{\perp}$.

6. Double θ-Cyclic Codes over S

A linear code C is a double θ-linear code if the set of coordinates can be partitioned into two subsets of lengths s and t such that the set of the first blocks of s symbols and the set of second blocks of t symbols form θ-cyclic codes of lengths s and t, respectively. Let s and t be non-negative integers such that $n = s + t$. We consider a partition of the set of the n coordinates into two subsets of s and t coordinates respectively. For any $d \in S$ and $w = (e_0, e_1, \ldots, e_{s-1}, f_0, f_1, \ldots, f_{t-1}) \in S^{s+t}$, we define

$$dw = (de_0, de_1, \ldots, de_{s-1}, df_0, df_1, \ldots, df_{t-1}).$$

With this multiplication, S^{s+t} is an S-module. A double θ-linear code is an S-submodule of S^{s+t}.

Definition 6.1. For an element $w = (e_0, e_1, \ldots, e_{s-1}, f_0, f_1, \ldots, f_{t-1}) \in S^{s+t}$, the $\sigma_{\theta(s,t)}$-cyclic shift of w, denoted by $\sigma_{\theta(s,t)}(w)$, is defined as $\sigma_{\theta(s,t)}(w) = (\theta(e_{s-1}), \theta(e_0), \ldots, \theta(e_{s-2}), \theta(f_{t-1}), \theta(f_0), \ldots, \theta(f_{t-2}))$.

Definition 6.2. A double θ-linear code C is called double θ-cyclic code if C is invariant under the $\sigma_{\theta(s,t)}$-cyclic shift.

Let $w = (e_0, e_1, \ldots, e_{s-1}, f_0, f_1, \ldots, f_{t-1}) \in C$. Then, w can be represented with $w(x) = (e(x)|f(x))$, where $e(x) = e_0 + e_1 x + \ldots + e_{s-1}x^{s-1} \in \frac{S[x,\theta]}{\langle x^s - 1\rangle}$ and $f(x) = f_0 + f_1 x + \ldots + f_{t-1}x^{t-1} \in \frac{S[x,\theta]}{\langle x^t - 1\rangle}$. This gives a one-to-one correspondence between S^{s+t} and $S_{s,t} = \frac{S[x,\theta]}{\langle x^s - 1\rangle} \times \frac{S[x,\theta]}{\langle x^t - 1\rangle}$. The multiplication of any $d(x) \in S[x,\theta]$ and $(p_1(x)|p_2(x)) \in \frac{S[x,\theta]}{\langle x^s - 1\rangle} \times \frac{S[x,\theta]}{\langle x^t - 1\rangle}$ is defined as

$$d(x)(p_1(x)|p_2(x)) = (d(x)p_1(x)|d(x)p_2(x)),$$

where $d(x)p_1(x)$ and $d(x)p_2(x)$ are the multiplication of polynomials in $\frac{S[x,\theta]}{\langle x^s - 1\rangle}$ and $\frac{S[x,\theta]}{\langle x^t - 1\rangle}$, respectively. With this multiplication, $S_{s,t}$ is a left $S[x,\theta]$-module. It is clear that, $xw(x)$ represents the $\sigma_{\theta(s,t)}$-cyclic shift of w.

Theorem 6.3. *Let C be a θ-linear code of length $n = s + t$ over S. Then, C is a double θ-cyclic code if and only if it is a left $S[x,\theta]$-submodule of the left-module $\frac{S[x,\theta]}{\langle x^s - 1\rangle} \times \frac{S[x,\theta]}{\langle x^t - 1\rangle}$.*

Proof. Assume that, C is a double θ-cyclic code. Let $w(x)$ be a polynomial representation of $w \in C$. Since $xw(x)$ is a $\sigma_{\theta(s,t)}$-cyclic shift of w, $xw(x) \in C$. As C is a linear code, $d(x)w(x) \in C$ for any $d(x) \in S[x,\theta]$. Therefore, C is left $S[x,\theta]$- submodule of $S_{s,t}$. Opposite direction of the proof is clear. □

Theorem 6.4. *Let $g'(x)$ and $g''(x)$ be monic polynomials such that $g'(x)|x^m - 1$ and $g''(x)|x^n - 1$. Let M and N be two free θ-cyclic codes of lengths m and n over S generated by $g'(x)$ and $g''(x)$, respectively. Then, a code C generated by $g(x) = (g'(x)|g''(x))$ is a double θ-cyclic code and $B = \left\{g(x), xg(x), \ldots, x^{k-1}g(x)\right\}$ is a spanning set of C, where $k = deg(h(x))$ and $h(x)$ is the least left common multiple of $h'(x)$ and $h''(x)$.*

Proof. Let $x^m - 1 = h'(x)g'(x)$ and $x^n - 1 = h''(x)g''(x)$ for some monic polynomials $h'(x), h''(x) \in S[x,\theta]$. Then, $h(x)g(x) = h(x)(g'(x)|g''(x)) = 0$, since $h(x)g'(x) = h(x)h'(x)g'(x) = 0$ and $h(x)g''(x) = h(x)h''(x)g''(x) = 0$. Let $z(x) \in C$ be any non-zero codeword. Then, $z(x) = k(x)g(x)$ for some $k(x) \in S[x,\theta]$. By the division algorithm, we have $k(x) = q(x)h(x) + r(x)$, where $r(x) = 0$ or $deg(r(x)) < deg(h(x))$. Then, $z(x) = k(x)g(x) = r(x)g(x) = 0$. Since $r(x) = 0$ or $deg(r(x)) < deg(h(x))$. Hence, the proof is completed. □

Example 6.5. Let C be a double θ-cyclic code of length $n = 6(= 4 + 2)$ over S, which is principally generated by $g(x) = (g_1(x)|g_2(x))$, where $g_1(x) = (3 + 2u + 2v)x^3 + (1 + 6u + 2v)x^2 + (3 + 6u + 6v)x + 1 + 2u + 6v$ and $g_2(x) = (7 + 4u + 4v)x + 5 + 2u + 2v$ such that $g_1(x)|x^4 - 1$ and $g_2(x)|x^2 - 1$. Now, let $h(x)$ be the least left common multiple of $h_1(x)$ and $h_2(x)$. Then, deg $h(x) = 2$. Therefore, the set $\{g(x), xg(x)\}$ forms a spanning set for C. Hence a generator matrix of C is

$$G = \begin{bmatrix} 1+2u+6v & 3+6u+6v & 1+6u+2v & 3+2u+2v & 5+2u+2v & 7+4u+4v \\ 3+2u+2v & 1+2u+6v & 3+6u+6v & 1+6u+2v & 7+4u+4v & 5+2u+2v \end{bmatrix}.$$

7. Conclusion

In this paper, skew-cyclic codes over $S = \mathbb{Z}_8 + u\mathbb{Z}_8 + v\mathbb{Z}_8$, where $u^2 = u$, $v^2 = v$, $uv = vu = 0$ are introduced. We have studied these codes as left $S[x, \theta]$-submodules. A Gray map is defined on S. The generator and parity-check matrices of a free θ-cyclic code of even length over S are obtained. Also, these codes are generalized to double skew-cyclic codes. One can study skew-cyclic codes over S with derivation if it exists.

Acknowledgment

The authors wish to express their thanks to the anonymous reviewers for their careful checking and valuable remarks that improved the presentation and the content of the paper.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this article.

Authors Contribution Statement

All authors jointly worked on the results and they have read and agreed to the published version of the manuscript.

References

[1] Bosma, W. Cannon J., Playoust, C., *The Magma algebra system I. The user language*, J. Symbolic Comput., **24**(1997), 235–265.
[2] Boucher, D., Ulmer, F., *Coding with skew polynomial rings*, J. of Symbolic Comput., **44**(2009), 1644–1656.
[3] Boucher, D., Geiselmann, W., Ulmer, F., *Skew-cyclic codes*, Appl. Alg. in Eng., Comm. and Comput., **18**(4)(2007), 379–389.
[4] Cengellenmis, Y., *On the cyclic codes over $F3 + vF3$*, Int. J. of Algebra, **4**(6)(2010), 253–259.
[5] Çalışkan, B., Balıkçı, K., *Counting $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$-additive codes*, European J. of Pure and Applied Math., **12**(2)(2019), 668–679.
[6] Çalışkan, B., *Linear Codes over the Ring $\mathbb{Z}_8 + u\mathbb{Z}_8 + v\mathbb{Z}_8$*, (ICOMAA-2020), Conference Proceeding Science and Technology, **3**(1)(2020), 19–23.
[7] Çalışkan, B., *Cylic Codes over the Ring $\mathbb{Z}_8 + u\mathbb{Z}_8 + v\mathbb{Z}_8$*, (ICMASE 2020), Proceedings Book, Ankara Hacı Bayram Veli University, Ankara, Turkey, (2020), 7–12.
[8] Dertli, A., Cengellenmis, Y., *On the codes over the ring $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$ cyclic, constacyclic, quasi-cyclic codes, their skew codes, cyclic DNA and skew cyclic DNA codes*, Prespacetime Journal, **10**(2)(2019), 196–213.
[9] Gao, J., *Skew cyclic codes over $F_p + vF_p$*, J. Appl. Math. Inform, **31**(3-4)(2013), 337–342.
[10] Hammons A.R., Kumar V., Calderbank A.R., Sloane N.J.A., Sole P., *The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory, **40**(1994), 301–319.
[11] Jin, L., *Skew cyclic codes over ring $F_p + vF_2$*, J. of Electronics (China), **31**(3)(2014), 228–231.
[12] Melakhessou, A., Aydin, N., Hebbache, Z., Guenda, K., *$\mathbb{Z}_q(\mathbb{Z}_q + u\mathbb{Z}_q)$-linear skew constacyclic codes*, J. Algebra Comb. Discrete Appl., **7**(1)(2019), 85–101.
[13] Mohammadi, R., Rahimi S., Mousavi, H., *On skew cyclic codes over a finite ring*, Iranian J. of Math. Sci. and Inf., **14**(1)(2019), 135–145.
[14] Sharma, A., Bhaintwal, M., *A class of skew-constacyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$*, Int. J. Inf. and Coding Theory, **4**(4)(2017), 289–303.
[15] Siap, I., Abualrub, T., Aydin, N., Seneviratne, P., *Skew cyclic codes of arbitrary length*, Int. J. of Inf. and Coding Theory, **2**(1)(2011), 10–20.