Advances in Mathematics of Communications
Volume 12, No. 4, 2018, 723–739
doi:10.3934/amc.2018043

A CLASS OF SKEW-CYCLIC CODES OVER $\mathbb{Z}_4 + u\mathbb{Z}_4$ WITH DERIVATION

Amit Sharma* and Maheshanand Bhaintwal

Department of Mathematics
Indian Institute of Technology Roorkee
Roorkee, 247667, India

(Communicated by Steven Dougherty)

Abstract. In this paper, we study a class of skew-cyclic codes using a skew polynomial ring over $R = \mathbb{Z}_4 + u\mathbb{Z}_4; u^2 = 1$, with an automorphism θ and a derivation δ_θ. We generalize the notion of cyclic codes to skew-cyclic codes with derivation, and call such codes as δ_θ-cyclic codes. Some properties of skew polynomial ring $R[x, \theta, \delta_\theta]$ are presented. A δ_θ-cyclic code is proved to be a left $R[x, \theta, \delta_\theta]$-submodule of $\frac{R[x,\theta,\delta_\theta]}{\langle x^n-1\rangle}$. The form of a parity-check matrix of a free δ_θ-cyclic codes of even length n is presented. These codes are further generalized to double δ_θ-cyclic codes over R. We have obtained some new good codes over $\mathbb{Z}_4$ via Gray images and residue codes of these codes. The new codes obtained have been reported and added to the database of $\mathbb{Z}_4$-codes [2].

1. Introduction

Cyclic codes form an important family of algebraic codes among all families of codes. The structure of cyclic codes is well defined over fields. Due to their rich algebraic properties these codes are easy to study and implement. Cyclic codes were introduced by Prange [19] in 1957 and have been studied extensively since then. The study of these codes over rings was initiated by the works of Blake [5, 6] and Spiegel [22, 23]. Codes over rings have generated a lot of interest after a breakthrough paper by Hammons et al. [15] in 1994. Recently, many extension rings of $\mathbb{Z}_4$ have been considered by researchers to construct codes [24, 25]. In most of these studies, cyclic codes have been studied in commutative settings.

In 2007, Boucher and Ulmer [9] 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. They have been further generalized in many ways [8, 10, 11]. In recent years many researchers have shown interest in this direction [4, 21, 16, 14], and many new results on codes over different rings in the setting of skew polynomial rings have been obtained. However, almost all this work has been done in the setting of skew-polynomial rings with automorphism only. In [12], Boucher et al. have studied linear codes using skew-polynomial rings with automorphism and derivation. In this paper, we have considered a class of skew-cyclic codes in the setting of the skew polynomial ring

2010 *Mathematics Subject Classification:* Primary: 94B05, 94B15, 11T71; Secondary: 12D05.
Key words and phrases: Skew-cyclic codes, Gray map, automorphisms and derivations, factorization, double-cyclic codes.

* Corresponding author: Amit Sharma.

©2018 AIMS

$R[x, \theta, \delta_\theta]$, where $R = \mathbb{Z}_4 + u\mathbb{Z}_4; u^2 = 1$, θ is an automorphism of R, and δ_θ is a derivation of R.

The paper is organized as follows. In Section 2, some preliminaries and basics are presented. The structural properties of skew polynomial ring $R[x, \theta, \delta_\theta]$ are also discussed in this section. In Section 3, δ_θ-cyclic codes are studied. Their torsion codes and residue codes are also studied. We have given a table of some good linear codes over $\mathbb{Z}_4$ obtained from them. In Section 4, the duals of δ_θ-cyclic codes of even length over R. In Section 5, we have generalized δ_θ-cyclic codes to double δ_θ-cyclic codes and obtained some good codes over $\mathbb{Z}_4$ from this class also.

2. Preliminaries

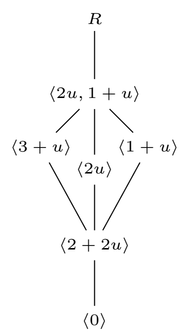

FIGURE 1.

In this section, we present some basic definitions and results that are necessary to understand the further results.

We fix the notation $R = \mathbb{Z}_4 + u\mathbb{Z}_4, u^2 = 1$. We note that $R \cong \frac{Z_4[u]}{\langle u^2-1 \rangle}$. An element $a + ub \in R$ is a unit if and only if exactly one of a and b is a unit. Therefore the units of R are

$$1, 3, u, 3u, u + 2, 2u + 3, 2u + 1, 3u + 2.$$

In a finite ring, an element is either a unit or a zero divisor, and hence the non-units of R are

$$0, 3u + 3, 2u + 2, u + 1, 2, 3u + 1, 2u, u + 3.$$

There are total 7 ideals of R (including the zero ideal), and they form a lattice with inclusion operation whose lattice diagram is shown in Figure 1.

In Figure 1, we have $\langle 0 \rangle = \{0\}, \langle 2u \rangle = \{0, 2u, 2, 2 + 2u\}, \langle 1 + u \rangle = \{0, 1 + u, 2 + 2u, 3 + 3u\}, \langle 3 + u \rangle = \{0, u + 3, 2u + 2, 3u + 2\}, \langle 2 + 2u \rangle = \{0, 2u + 2\}, \langle 2u, 1 + u \rangle = \{3u + 3, 0, 2u + 2, u + 1, 2, 3u + 1, 2u, u + 3\}, \langle 1 \rangle = R$. Thus R is a local-ring with the unique maximal ideal $\langle 2u, 1 + u \rangle$. To know more about the ring R, we refer to [18, 20].

Define a map $\theta : R \to R$ such that

$$\theta(a + ub) = a + (u + 2)b.$$

One can easily verify that θ is an automorphism of R. Moreover, since $\theta^2(x) = x$ for all $x \in R$, the order of θ is 2.

Definition 2.1. Let $\mathbf{R}$ be a finite ring and Θ be an automorphism of $\mathbf{R}$. Then a map $\Delta_\Theta : \mathbf{R} \to \mathbf{R}$ is said to be a derivation on $\mathbf{R}$ if

$$\Delta_\Theta(x+y) = \Delta_\Theta(x) + \Delta_\Theta(y)$$

and

$$\Delta_\Theta(xy) = \Delta_\Theta(x)y + \Theta(x)\Delta_\Theta(y).$$

We define a map $\delta_\theta : R \to R$ such that

$$\delta_\theta(a+ub) = (1+u)(\theta(a+ub) - (a+ub)).$$

That is, $\delta_\theta(a+ub) = (1+u)(a+ub+2b-a-ub) = 2b+2ub$.

Theorem 2.2. *The map δ_θ is a derivation on R.*

Proof. Let $x, y \in R$. Then by definition,

$$\begin{aligned}
\delta_\theta(x+y) &= (1+u)(\theta(x+y) - (x+y)) \\
&= (1+u)(\theta(x) - x) + (1+u)(\theta(y) - y) \\
&= \delta_\theta(x) + \delta_\theta(y).
\end{aligned}$$

Also,

$$\begin{aligned}
\delta_\theta(xy) &= (1+u)(\theta(xy) - xy) \\
&= (1+u)\theta(x)\theta(y) - (1+u)xy \\
&= (1+u)\theta(x)\theta(y) - (1+u)xy + (1+u)\theta(x)y - (1+u)\theta(x)y \\
&= (1+u)\theta(x)(\theta(y) - y) - (1+u)(x - \theta(x))y \\
&= \theta(x)(1+u)(\theta(y) - y) + (1+u)(\theta(x) - x)y \\
&= \delta_\theta(x)y + \theta(x)\delta_\theta(y)
\end{aligned}$$

Since δ_θ satisfies the properties of a derivation, δ_θ is therefore a derivation on R. $\square$

The following table gives images of elements of R under δ_θ.

x	0	1	2	3	u	$2u$	$3u$	$1+u$
$\delta_\theta(x)$	0	0	0	0	$2+2u$	0	$2+2u$	$2+2u$
x	$1+2u$	$1+3u$	$2+u$	$2+2u$	$2+3u$	$3+u$	$3+2u$	$3+3u$
$\delta_\theta(x)$	0	$2+2u$	$2+2u$	0	$2+2u$	$2+2u$	0	$2+2u$

Remark 1. We note that for $n \geq 2$, we have ${\delta_\theta}^n(x) = 0$ for all $x \in R$.

2.1. Gray map. On $\mathbb{Z}_4$, the Lee weight (w_L) is defined as $w_L(0) = 0$, $w_L(1) = 1$, $w_L(2) = 2$, $w_L(3) = 1$. The Lee weight $w_L(u)$ of a vector $u \in {\mathbb{Z}_4}^2$ is then defined as the rational sum of the Lee weights of its coordinates. Define a map $\phi : R \to {\mathbb{Z}_4}^2$, known as Gray map, such that

$$\phi(a+ub) = (b, a+b).$$

For any $x \in R$, we define the Gray weight $w_G(x)$ of x as $w_G(x) = w_L(\phi(x))$. The Gray weights of the elements of R are as follows:

x	0	1	2	3	u	$2u$	$3u$	$1+u$
w_G(x)	0	1	2	1	2	4	2	3
x	$1+2u$	$1+3u$	$2+u$	$2+2u$	$2+3u$	$3+u$	$3+2u$	$3+3u$
$w_G(x)$	3	1	2	2	2	1	3	3

The map ϕ is extended componentwise to $\Phi : R^n \to {\mathbb{Z}_4}^{2n}$, and we define the Gray weight of $x \in R^n$ as the rational sum of Gray weights of its coordinates.

Now onward, we write the parameters of a linear code C over $\mathbb{Z}_4$ as $(n, 4^{k_1}2^{k_2}, d_L)$, and say that the type of the code is $4^{k_1}2^{k_2}$, where d_L denotes the minimum Lee distance of C.

Theorem 2.3. *(Lee Distance Bound [13]) If C is a linear code of length n over $\mathbb{Z}_4$ with parameters $(n, 4^{k_1}2^{k_2}, d_L)$, then $d_L \leq 2n - 2k_1 - k_2 + 1$.*

A linear code over $\mathbb{Z}_4$ which satisfies the above bound with equality is called a *Maximum Lee Distance Separable (MLDS)* code.

2.2. SKEW POLYNOMIAL RING $\mathbf{R}[x, \Theta, \Delta_\Theta]$. Let $\mathbf{R}$ be a ring with automorphism Θ and derivation Δ_Θ. Then the skew polynomial ring $\mathbf{R}[x, \Theta, \Delta_\Theta]$ is the set of all polynomials over $\mathbf{R}$ with addition as the ordinary addition of polynomials and multiplication defined by

$$xa = \Theta(a)x + \Delta_\Theta(a) \tag{1}$$

for any $a \in \mathbf{R}$, which is then extended to all elements of $\mathbf{R}[x, \Theta, \Delta_\Theta]$ in the usual manner. The following example illustrates it.

Example 1. Let $f = x^2 + a_0x + a_1$ and $g = x + b_0$ are in $R[x, \theta, \delta_\theta]$. Then

$$f + g = x^2 + (a_0 + 1)x + a_1 + b_0 = g + f.$$

Also,

$$\begin{aligned} fg &= (x^2 + a_0x + a_1)(x + b_0) \\ &= x^2(x + b_0) + a_0x(x + b_0) + a_1(x + b_0) \\ &= x^3 + b_0x^2 + a_0x^2 + a_0(\theta(b_0)x + \delta_\theta(b_0)) + a_1x + a_1b_0 \\ &\quad \text{(By Corollary 1 on Page 6)} \\ &= x^3 + (b_0 + a_0)x^2 + (a_0\theta(b_0) + a_1)x + a_0\delta_\theta(b_0) + a_1b_0, \end{aligned}$$

and

$$\begin{aligned} gf &= (x + b_0)(x^2 + a_0x + a_1) \\ &= x(x^2 + a_0x + a_1) + b_0(x^2 + a_0x + a_1) \\ &= x^3 + (\theta(a_0)x + \delta_\theta(a_0))x + (\theta(a_1)x + \delta_\theta(a_1)) + b_0x^2 + b_0a_0x + b_0a_1 \\ &= x^3 + (\theta(a_0) + b_0)x^2 + (\delta_\theta(a_0) + \theta(a_1) + b_0a_0)x + \delta_\theta(a_1) + b_0a_1 \end{aligned}$$

Therefore $fg \neq gf$. Thus $R[x, \theta, \delta_\theta]$ is a non-commutative ring.

Let $R^\theta = \{0, 1, 2, 3, 2u, 1 + 2u, 3 + 2u, 2 + 2u\}$. Then R^θ is a subring of R fixed, elementwise, by θ, i.e., $\theta(a) = a$ for all $a \in R^\theta$. Also $\delta_\theta(a) = 0$ for all $a \in R^\theta$. Therefore we have $xa = ax$ for all $a \in R^\theta$.

Since $R[x, \theta, \delta_\theta]$ is not a unique factorization ring, we often have more factors of a polynomial in $R[x, \theta, \delta_\theta]$ than in $R[x]$ (shown in Example 5 below). Therefore we have more possibility of finding good codes over R in this setting, and a search for good codes among these codes looks more promising than a random search for codes over R.

Definition 2.4. An element $f(x)$ in $R[x, \theta, \delta_\theta]$ is said to be a central element of $R[x, \theta, \delta_\theta]$ if $f(x)a(x) = a(x)f(x)$ for all $a(x) \in R[x, \theta, \delta_\theta]$.

Lemma 2.5. *Let $a \in R$. Then $\theta(a) - a \neq \delta_\theta(b)$ for any $b \in R$ unless a, b both are fixed by θ.*

Proof. Let $\theta(a) - a = \delta_\theta(b)$ for some arbitrary fixed values of a and b. The only possible values of $\delta_\theta(b)$ are 0 and $2u + 2$. If $\delta_\theta(b) = 0$, then a and b both are fixed by θ and we are done. Suppose $\delta_\theta(b) = 2u + 2$. But $\theta(a) - a$ does not contain u, we get a contradiction. Hence the result. $\square$

If we consider the skew polynomial ring over R with automorphism only, i.e., $R[x, \theta]$, then the center of $R[x, \theta]$ is $R^\theta[x^2]$ [17]. However, in the present case, i.e., in $R[x, \theta, \delta_\theta]$, we have the following result.

Theorem 2.6. *A polynomial $f(x) \in R[x, \theta, \delta_\theta]$ is a central element if and only if $f(x) \in R^\theta[x]$ such that the coefficients of all odd powers of x belong to the set $S = \{0, 2, 2u, 2 + 2u\}$.*

Proof. We prove the result for a polynomial of odd degree. It can be proved similarly for polynomials of even degree. Let $f(x) = f_0 + f_1 x + \cdots + f_k x^k \in R[x, \theta, \delta_\theta]$ be a polynomial of odd degree. Suppose $f(x)$ is a central element. Then

$$\begin{aligned} 0 &= xf(x) - f(x)x \\ &= \delta_\theta(f_0) + \sum_{i=0}^{k-1} (\theta(f_i) + \delta_\theta(f_{i+1}))x^{i+1} + \theta(f_k)x^{k+1} - \sum_{i=0}^{k} f_i x^{i+1}. \end{aligned}$$

Equating coefficients of all terms to zero we get

$$\delta_\theta(f_0) = 0, \tag{2}$$

$$(\theta(f_i) - f_i + \delta_\theta(f_{i+1})) = 0 \text{ for } i = 0, 1, 2, \cdots, k-1 \tag{3}$$

$$\theta(f_k) - f_k = 0. \tag{4}$$

From Equations (3), (4), (5) and Lemma 2.5, we have all f_i's fixed by θ, $i = 0, 1, \cdots, k$.

Again since $f(x)$ is a central element, we have $f(x)a = af(x)$ for all $a \in R$. Choose $a \in R$, which is not fixed by θ, i.e., $\theta(a) \neq a$. Then

$$\begin{aligned} 0 &= af(x) - f(x)a \\ &= \sum_{i=0}^{k} af_i x^i - \sum_{j=0}^{\frac{k-1}{2}} (f_{2j}a + f_{2j+1}\delta_\theta(a))x^{2j} - \sum_{l=0}^{\frac{k-1}{2}} f_{2l+1}\theta(a)x^{2l+1} \\ &= \sum_{j=0}^{\frac{k-1}{2}} (af_{2j} - f_{2j}a - f_{2j+1}\delta_\theta(a))x^{2j} + \sum_{j=0}^{\frac{k-1}{2}} (af_{2l+1} - f_{2l+1}\theta(a))x^{2l+1} \\ &= \sum_{j=0}^{\frac{k-1}{2}} (f_{2j+1}\delta_\theta(a))x^{2j} - \sum_{j=0}^{\frac{k-1}{2}} f_{2l+1}(a - \theta(a))x^{2l+1}. \end{aligned}$$

This implies that $f_{2l+1}(a-\theta(a)) = 0$ and $f_{2j+1}(\delta_\theta(a)) = 0$ for all $j, l = 0, 1, 2, \cdots \frac{k-1}{2}$. Since all f_i are fixed, the coefficients f_{2l+1} which satisfy the above conditions are precisely the elements of S. Combining both the cases we get the required result.

Conversely, suppose $f(x)$ satisfies the given conditions. Then to show $f(x)a(x) = a(x)f(x)$ for all $a(x) \in R[x, \theta, \delta_\theta]$, it is sufficient to show that $(a_i x^i)(f_j x^j) = (f_j x^j)(a_i x^i)$ for $0 \leq i \leq \deg a(x)$ and $0 \leq j \leq \deg f(x)$. We have

$$(a_i x^i)(f_j x^j) = a_i f_j x^{i+j}, \text{as all } f_i \text{ are fixed by } \theta. \tag{5}$$

Also,

$$(f_j x^j)(a_i x^i) = \begin{cases} f_j a_i x^{i+j}, & \text{if } j \text{ is even} \\ f_j(\theta(a_i)x + \delta_\theta(a_i))x^{i+j-1}, & \text{if } j \text{ is odd.} \end{cases} \tag{6}$$

If j is odd and $f_j \in S$, then $f_j \delta_\theta(a) = 0$ and $f_j \theta(a) = f_j a$ for all $a \in R$, and so (6) gives

$$(f_j x^j)(a_i x^i) = f_j(\theta(a_i)x + \delta_\theta(a_i))x^{i+j-1} = f_j a_i x^{i+j}. \tag{7}$$

Therefore by (5), (6), (7), we have the required result. □

Lemma 2.7. *For any element $a \in R$, $\delta_\theta(\theta(a)) + \theta(\delta_\theta(a)) = 0$. Also, $x^2 a = ax^2 \ \forall\ a \in R$.*

Proof. Let $a = a' + ub' \in R$. Then $\delta_\theta(\theta(a)) = \delta_\theta(a' + (u+2)b') = 2b' + 2ub'$, and $\theta(\delta_\theta(a)) = \theta(2b' + 2ub') = 2b' + 2ub' = -(2b' + 2ub') = -\delta_\theta(\theta(a))$, which proves the first part. Further, $xa = \theta(a)x + \delta_\theta(a)$. Multiplying both sides by x, we get $x^2 a = x\theta(a)x + x\delta_\theta(a) = [\theta^2(a)x + \delta_\theta(\theta(a)]x + \theta(\delta_\theta(a))x + {\delta_\theta}^2(a) = ax^2 + [\delta_\theta(\theta(a)) + \theta(\delta_\theta(a))]x + {\delta_\theta}^2(a) = ax^2$, using the first part of this lemma and noting that ${\delta_\theta}^2(a) = 0$ for all $a \in R$. □

Corollary 1. *For any element $a \in R$,*

$$x^n a = \begin{cases} (\theta(a)x + \delta_\theta(a))x^{n-1}, & \textit{if } n \textit{ is odd} \\ ax^n, & \textit{if } n \textit{ is even.} \end{cases}$$

The ring $R[x, \theta, \delta_\theta]$ is not a left/right Euclidean ring, so division algorithm does not hold in it. But we can still apply division algorithm on some particular elements of $R[x, \theta, \delta_\theta]$. This is given by the next result.

Theorem 2.8 (Right division algorithm)**.** *Let $f(x), g(x) \in R[x, \theta, \delta_\theta]$ be such that $g(x)$ has leading coefficient a unit. Then*

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

for some $q(x), r(x) \in R[x, \theta, \delta_\theta]$, where $r(x) = 0$ or deg $r(x) <$deg $g(x)$.

Proof. Let $f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_r x^r$ and $g(x) = g_0 + g_1 x + g_2 x^2 + \cdots + g_s x^s$, where g_s is a unit. If $r < s$, then $f(x) = 0 \cdot g(x) + f(x)$ gives the required result. Suppose $r \geq s$. We define a polynomial $h(x) = f(x) - A(x)g(x)$, where

$$A(x) = \begin{cases} f_r \theta(g_s^{-1})x^{r-s}, & \text{if } r - s \text{ is odd} \\ f_r g_s^{-1} x^{r-s}, & \text{if } r - s \text{ is even} \end{cases}.$$

Clearly, $h(x)$ is a polynomial of degree one less than the degree of $f(x)$. We prove the result by implementing induction on deg $f(x)$. Assume that the result is true for every polynomial having degree less than deg $f(x)$. Obviously result is true for deg $f(x) = 0$. So let deg $f(x) > 0$. Since deg $h(x) <$ deg $f(x)$, there exist $q_1(x)$,

$r_1(x)$ such that $h(x) = q_1(x)g(x) + r_1(x)$, where $r_1(x) = 0$ or deg $r_1(x) <$ deg $g(x)$ and so $f(x) = q_1(x)g(x) + r_1(x) + A(x)g(x) = (q_1(x) + A(x))g(x) + r_1(x)$. Thus we obtain $f(x) = q(x)g(x) + r(x)$, where $q(x) = q_1(x) + A(x)$ and $r(x) = r_1(x)$. Hence the result. □

A left division algorithm can similarly be proved. In this paper, division always means a right division.

Example 2. Consider the polynomials $f(x), g(x) \in R[x, \theta, \delta_\theta]$ such that $f(x) = (1+u)x^2+(2+2u)x+u$ and $g(x) = ux+(1+u)$. Here $r = 2, s = 1, f_2 = 1+u, g_1 = u$. Let $A(x) = f_2\theta(g_1^{-1})x^{2-1} = (1 + u)(u + 2)x = (3u + 3)x$. Then

$$\begin{aligned} A(x)g(x) &= (3u+3)x(ux+(1+u)) \\ &= (3u+3)(\theta(u)x+\delta_\theta(u))x+(3u+3)(\theta(1+u)x+\delta_\theta(1+u)) \\ &= (3u+3)((u+2)x+2+2u)x+(3u+3)((u+3)x+2+2u) \\ &= (u+1)x^2+0.x+0.x+0 \\ &= (u+1)x^2. \end{aligned}$$

We define $h(x) = f(x) - A(x)g(x) = (2 + 2u)x + u$. Now repeating the above argument on $h(x)$, we get $h(x) = (2+2u)g(x)+u$, and so $f(x) = h(x)+A(x)g(x) = (2 + 2u)g(x) + u + (3u + 3)xg(x) = ((2 + 2u) + (3u + 3)x)g(x) + u$. Therefore we have $f(x) = q(x)g(x) + r(x)$, where $q(x) = (2 + 2u) + (3u + 3)x$ and $r(x) = u$.

3. δ_θ-CYCLIC CODES OVER R

In this section, we define a class of skew-cyclic codes over R and call them δ_θ-cyclic codes over R.

A linear code of length n over R is a submodule of R^n. By identifying R^n with $\frac{R[x,\theta,\delta_\theta]}{\langle f(x)\rangle}$, where $f(x)$ is an arbitrary polynomial of degree n over R, we can associate a word $a = (a_0, a_1, \ldots, a_{n-1})$ to the corresponding polynomial $a(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1}$. Moreover $\frac{R[x,\theta,\delta_\theta]}{\langle f(x)\rangle}$ is a left $R[x, \theta, \delta_\theta]$-module with respect to the multiplication $r(x)(a(x) + \langle f(x)\rangle) = r(x)a(x) + \langle f(x)\rangle$.

Definition 3.1. A code C of length n over R is said to be a δ_θ-linear code if it is a left $R[x, \theta, \delta_\theta]$-submodule of $\frac{R[x,\theta,\delta_\theta]}{\langle f(x)\rangle}$, where $f(x)$ is an arbitrary polynomial of degree n over R. In addition, if $f(x)$ is a central polynomial in $R[x, \theta, \delta_\theta]$, we call C a central δ_θ-linear code.

Definition 3.2 (δ_θ-cyclic code)**.** A code C of length n over R is said to be δ_θ-cyclic code over R if C is a δ_θ-linear code and whenever $c = (c_0, c_1, \ldots, c_{n-1}) \in C$, we have $T_{\delta_\theta}(c) = (\theta(c_{n-1})+\delta_\theta(c_0), \theta(c_0)+\delta_\theta(c_1), \theta(c_1)+\delta_\theta(c_2), \ldots, \theta(c_{n-2})+\delta_\theta(c_{n-1})) \in C$, where T_{δ_θ} is the δ_θ-cyclic shift operator.

Lemma 3.3. *If $v(x) = v_0 + v_1x + v_2x^2 + \ldots + v_{n-1}x^{n-1} \in \frac{R[x,\theta,\delta_\theta]}{\langle x^n-1\rangle}$ represents the word $v = (v_0, v_1, \ldots, v_{n-1})$ in R^n, then $xv(x)$ represents the word $(\theta(v_{n-1}) + \delta_\theta(v_0), \theta(v_0) + \delta_\theta(v_1), \theta(v_1) + \delta_\theta(v_2), \ldots, \theta(v_{n-2}) + \delta_\theta(v_{n-1}))$ in R^n.*

Proof. We have

$$xv(x) = x\left(\sum_{i=0}^{n-1} v_ix^i\right) = \sum_{i=0}^{n-1} x(v_ix^i) = \sum_{i=0}^{n-1}(\theta(v_i)x + \delta_\theta(v_i))x^i$$

$$\begin{aligned}
&= \sum_{i=0}^{n-1}\theta(v_i)x^{i+1} + \sum_{i=0}^{n-1}\delta_\theta(v_i)x^i = \sum_{i=1}^{n}\theta(v_{i-1})x^i + \sum_{i=0}^{n-1}\delta_\theta(v_i)x^i\\
&= \sum_{i=1}^{n-1}\theta(v_{i-1})x^i + \sum_{i=1}^{n-1}\delta_\theta(v_i)x^i + \theta(v_{n-1})x^n + \delta_\theta(v_0)x^0\\
&= \sum_{i=1}^{n-1}(\theta(v_{i-1}) + \delta_\theta(v_i))x^i + (\theta(v_{n-1}) + \delta_\theta(v_0)) \text{ (as } x^n = 1)\\
&= \sum_{i=0}^{n-1}(\theta(v_{i-1}) + \delta_\theta(v_i))x^i,
\end{aligned}$$

where the indices are computed modulo n. Hence the result. □

Theorem 3.4. *A code C of length n over R is a δ_θ-cyclic code if and only if C is an $R[x,\theta,\delta_\theta]$-submodule of $R_{n,\delta_\theta} = \frac{R[x,\theta,\delta_\theta]}{\langle x^n-1\rangle}$.*

Proof. Suppose C is a δ_θ-cyclic code of length n over R. Then for any $c(x) \in C$, the δ_θ-cyclic shift, $xc(x)$ also belongs to C (by Lemma 3.3), and hence all $x^ic(x) \in C$ for all $i \in \mathbb{N}$. It follows that $a(x)c(x) \in C$ for all $a(x) \in R[x,\theta,\delta_\theta]$. Hence the result. Converse is straightforward. □

Corollary 2. *If C is a δ_θ-cyclic code of even length n, then C is an ideal of $R_{n,\delta_\theta} = \frac{R[x,\theta,\delta_\theta]}{\langle x^n-1\rangle}$.*

Proof. For even n, the ideal $\langle x^n - 1\rangle$ is a two sided ideal and so R_{n,δ_θ} is a ring. Hence the result. □

Remark 2. A δ_θ-cyclic code of an even length n over R is a central δ_θ-linear code. However, the converse is not true. This is shown by the following example.

Example 3. Let C be a code of length 4 over R generated by the right divisor $g(x) = (1+2u)x^2-1$ of $f(x) = (2u+1)x^4+(2u+2)x^2+1 = (x^2-1)((1+2u)x^2-1)$. Since $f(x)$ is a central polynomial in $R[x,\theta,\delta_\theta]$, C is a central δ_θ-linear code. We obtain, using $MAGMA$, that $(3u+1, 3u+2, 3u+1, u) \in C$, but its δ_θ-cyclic shift, i.e., $(3u, u+1, u+2, u+1) \notin C$. Hence C is not a δ_θ-cyclic code over R.

Theorem 3.5. *Let C be a δ_θ-cyclic code of length n over R. Then we have the following results:*

1. *C is simply a cyclic code of length n over R, if n is odd.*
2. *C is a quasi-cyclic code of length n and index 2 over R, if n is even.*

Proof. 1. Since n is odd, we have $(n, 2) = 1$. Therefore there exist two integers a, b such that $na+2b = 1$ and so $2b = 1-na = 1+nl$, where $l \equiv -a \ (mod\ n)$. Let $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ be a codeword. Now by Lemma 2.7, $x^{2b}c(x) = x^{2b}(c_0+c_1x+\cdots+c_{n-1}x^{n-1}) = c_0x^{2b}+c_1x^{2b+1}+\cdots+c_{n-1}x^{2b+n-1}$. Therefore $x^{2b}c(x) = c_0x^{1+nl} + c_1x^{1+nl+1} + \cdots + c_{n-1}x^{(1+nl)+(n-1)} = c_0x + c_1x^2 + \cdots + c_{n-2}x^{n-1} + c_{n-1}$, which is a cyclic shift of $c(x)$. Hence the result.
2. For any codeword $c(x)$ in C, $x^2c(x) \in C$ and it represents the cyclic shift of c by two positions (by Lemma 2.7). Also, in general, C is not cyclic. So 2 is the smallest integer t such that $x^tc(x) \in C$ for any $c(x) \in C$. Therefore C is quasi-cyclic code of index 2.

□

Theorem 3.6. *Let C be a δ_θ-cyclic code of length n over R such that C contains a minimum degree polynomial $g(x)$ with its leading coefficient a unit. Then $C = \langle g(x)\rangle$. Moreover $g(x) \mid (x^n - 1)$ and the set $\{g(x), xg(x), \ldots, x^{n-deg\ g(x)-1}g(x)\}$ forms a basis for C.*

Proof. Since C contains a minimum degree polynomial having its leading coefficient a unit, the proof follows from similar arguments as in the case of finite fields [21]. □

The converse of Theorem 3.6 is also true.

Theorem 3.7. *Let C be a free δ_θ-cyclic code of length n over R. Then there exists a minimum degree polynomial $g(x)$ such that $C = \langle g(x)\rangle$ and $g(x) \mid x^n - 1$.*

Proof. Straightforward. □

Example 4. Let C be a δ_θ-cyclic code of length 6 over R generated by the right divisor $g(x) = (u+2)x^3 + 2x^2 + 3u$ of $x^6 - 1$. Then the set $\{g(x), xg(x), x^2g(x)\} = \{(u+2)x^3 + 2x^2 + 3u, ux^4 + 2ux^3 + (3u+2)x + 2u + 2, (u+2)x^5 + 2x^4 + 3ux^2\}$ forms a basis for C. Therefore C has cardinality 16^3.

Now we present a form of the generator matrix of a free δ_θ-cyclic code of length n over R.

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

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

where $g(x) = g_0 + g_1x + g_2x^2 + \cdots + g_kx^k$. More precisely, if $n-k$ is even, then $G =$

$$\begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_k & 0 & \cdots & 0 \\ \delta_\theta(g_0) & \theta(g_0)+\delta_\theta(g_1) & \theta(g_1)+\delta_\theta(g_2) & \cdots & \theta(g_{k-1})+\delta_\theta(g_k) & \theta(g_k) & \cdots & 0 \\ 0 & 0 & g_0 & \cdots & g_{k-3} & g_{k-2} & \cdots & 0 \\ \cdots & \cdots & \cdots & \ddots & \cdots & \ddots & \ddots & \cdots \\ 0 & 0 & \cdots & \delta_\theta(g_0) & \theta(g_0)+\delta_\theta(g_1) & \cdots & \theta(g_{k-1})+\delta_\theta(g_k) & \theta(g_k) \end{bmatrix}$$

and if $n-k$ is odd, then

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_k & 0 & \cdots & 0 \\ \delta_\theta(g_0) & \theta(g_0)+\delta_\theta(g_1) & \theta(g_1)+\delta_\theta(g_2) & \cdots & \theta(g_{k-1})+\delta_\theta(g_k) & \theta(g_k) & \cdots & 0 \\ 0 & 0 & g_0 & \cdots & g_{k-3} & g_{k-2} & \cdots & 0 \\ \cdots & \cdots & \cdots & \ddots & \cdots & \ddots & \ddots & \cdots \\ 0 & 0 & \cdots & 0 & g_0 \cdots & g_{k-2} & g_{k-1} & g_k \end{bmatrix}.$$

For example, for the δ_θ-cyclic code C given in Example 4, the generator matrix of C can be given as

$$\begin{bmatrix} 3u & 0 & 2 & u+2 & 0 & 0 \\ 2u+2 & 3u+2 & 0 & 2u & u & 0 \\ 0 & 0 & 3u & 0 & 2 & u+2 \end{bmatrix}.$$

3.1. RESIDUE AND TORSION CODES. In this sub-section, we study the residue codes and torsion codes associated with linear codes over R.

Definition 3.8. Let C be a linear code of length n over R. Then

$$Res(C) = \{x : \ x + uy \in C \text{ for some } y \in \mathbb{Z}_4{}^n\}$$

and

$$Tor(C) = \{x : \ ux \in C\}$$

are called the residue code and the torsion code, respectively, of C.

$Res(C), Tor(C)$ are linear codes of length n over $\mathbb{Z}_4$.

Theorem 3.9. *Let C be a linear code of length n over R.*

1. *If $x + uy \in C$, then $x, y \in Res(C)$, and hence $Res(C) = \{y \mid x + uy \in C$ for some $x \in \mathbb{Z}_4{}^n\}$.*
2. *$Tor(C) \subseteq C$, hence $min\{d_L(Tor(C))\} \geq min\{d_G(C)\}$.*

Proof. For first part, since $x + uy \in C$, we have $ux + y \in C$ as $u^2 = 1$. This gives $y \in Res(C)$. Also $x + uy \in C$ implies $x \in Res(C)$. The proof of the second part is straightforward. ☐

Example 5. Let $f(x) = x^8 - 1$. Then two different factorizations of $f(x)$ are as follows:

$$\begin{aligned} x^8 - 1 &= (x^2-1)(x^6+x^4+x^2+1) \\ &= ((3u+2)x^2+2ux+u+2)((3u+2)x^6+2ux^5+(3u+2)x^4+(3u+2)x^2+2ux+3u+2). \end{aligned}$$

Consider two distinct factors of degree 6 of $x^8 - 1$ as $f_1 = x^6 + x^4 + x^2 + 1, f_2 = (3u+2)x^6 + 2ux^5 + (3u+2)x^4 + (3u+2)x^2 + 2ux + 3u + 2$. Then we have δ_θ-cyclic codes $C_1 = \langle f_1 \rangle$ and $C_2 = \langle f_2 \rangle$ of length 8 over R. Also the spanning set for C_i is $\{f_i, xf_i\}$ for $i = 1, 2$. Moreover, C_2 exists due to the factors f_2, which exists in $R[x, \theta, \delta_\theta]$ only. Now $\Phi(C_1)$ and $\Phi(C_2)$ are linear codes of length 16 over $\mathbb{Z}_4$ having parameters $(16, 4^4, 4)$, $(16, 4^4, 8)$, respectively. Also $Res(C_1)$ has the parameters $(8, 4^2, 4)$ and $Res(C_2)$ has the parameters $(8, 4^2, 8)^*$, which is a good linear code over $\mathbb{Z}_4$ [2].

Example 6. Let C be a δ_θ-cyclic code of length 9 over R generated by $g(x) = 3x^8+2ux^7+(u+1)x^6+(2u+2)x^5+2ux^4+(u+2)x^3+2x^2+(u+2)x+u+2$. Consider a subcode C_1 of C having spanning set $\{g(x), xg(x), x^2g(x), x^3g(x), x^4g(x)\}$. Now the parameters of $\Phi(C_1)$ are $(18, 4^{10}, 4)$ and the parameters of $Res(C_1)$ are $(\mathbf{9}, \mathbf{4^8 2^1}, \mathbf{2})$. $Res(C_1)$ is a new good linear code over $\mathbb{Z}_4$ and has twice as many codewords as in the existing best known code with comparable parameters [2]. A generator matrix of $Res(C_1)$ over $\mathbb{Z}_4$ is given by

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{bmatrix}.$$

Further, let $C_2 = \{(u \mid u + v) \mid u, v \in Res(C_1)\}$. Then the parameters C_2 are $(\mathbf{18}, \mathbf{4^{16} 2^2}, \mathbf{2})$, which is a new good linear code over $\mathbb{Z}_4$ and improves minimum

Lee distance of code by 1 when compared to existing best code with comparable parameters [2].

Example 7. Let C be a δ_θ-cyclic code of length 4 over R with generator matrix

$$\begin{bmatrix} 1+u & u & 1 & 0 \\ 2+2u & 1+3u & 2+u & 1 \\ 1 & 0 & 1+u & u \end{bmatrix}.$$

Then $\Phi(C)$ has parameters $(8, 4^6, 2)$, which is a best known linear code over $\mathbb{Z}_4$.

Also $Res(C)$ has a generator matrix

$$\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 2 \end{bmatrix}.$$

The parameters for $Res(C)$ are $(4, 4^3 2^1, 2)$, which is a best known good code over $\mathbb{Z}_4$. Moreover $Res(C)$ satisfies the bound given in Theorem 2.3, and is therefore an $MLDS$ code. Now let $C_1 = \{(u \mid u+v) \mid u, v \in Res(C)\}$. Then C_1 is an $(\mathbf{8}, \mathbf{4^6 2^2}, \mathbf{2})$ code over $\mathbb{Z}_4$, which is a new good linear code over $\mathbb{Z}_4$ and improves the minimum Lee distance of code by 1 when compared to existing best code with comparable parameters [2].

	C	$\Phi(C)$	$Res(C)$	C^*
Set of generators	Code	$(n, 4^{k_1}2^{k_2}, d_L)$	$(n, 4^{k_1}2^{k_2}, d_L)$	$(n, 4^{k_1}2^{k_2}, d_L)$
$\{g_1(x), xg_1(x), x^2g_1(x)\}$	C_1	$(10, 4^6, 2)$	$(5, 4^4 2^1, 2)^*$	$(\mathbf{10}, \mathbf{4^8 2^2}, \mathbf{2})^{**}$
$\{g_2(x), xg_2(x), x^2g_2(x)\}$	C_2	$(20, 4^6, 8)$	$(10, 4^6, 4)^*$	$(20, 4^{12}, 4)^*$
$\{g_3(x), xg_3(x), x^2g_3(x)\}$	C_3	$(20, 4^6, 6)$	$(10, 4^5, 6)^*$	$(20, 4^{10}, 6)$
$\{g_4(x), xg_4(x), x^2g_4(x), x^3g_4(x)\}$	C_4	$(24, 4^8, 6)$	$(12, 4^8, 4)^*$	$(24, 4^{16}, 4)^*$
$\{g_5(x), xg_5(x), x^2g_5(x), x^3g_5(x)\}$	C_5	$(28, 4^8, 6)$	$(14, 4^8, 5)^*$	$(28, 4^{16}, 5)^*$
$\{g_6(x), xg_6(x), x^2g_6(x), x^3g_6(x)\}$	C_6	$(30, 4^8, 6)$	$(15, 4^8, 6)^*$	$(30, 4^{16}, 6)$
$\{g_7(x), xg_7(x), x^2g_7(x), x^3g_7(x)\}$	C_7	$(36, 4^8, 8)$	$(18, 4^8, 8)^*$	$(36, 4^{16}, 8)^*$

TABLE 1. *:= Existing good code [2, 1], **:=New good code

Table 1 shows some good linear codes over $\mathbb{Z}_4$ we have obtained via the Gray images and residue codes of skew-linear codes with derivation (not necessarily δ_θ-cyclic codes) over R. In table 1, we have

$$C^* = \{(u \mid u+v) : u, v \in Res(C)\},$$
$$g_1(x) = 2ux^4 + x^3 + (u+2)x^2 + 2ux + (u+1)$$
$$g_2(x) = ux^9 + (u+1)x^8 + 2ux^7 + (u+2)x^6 + 2x^5 + (u+1)x^4 + x^2 + ux + (u+1)$$
$$g_3(x) = ux^9 + (u+1)x^8 + (3u+3)x^7 + (2u+2)x^6 + (3u+2)x^5 + 2x^4 + x^2 + ux + u + 1$$

$$g_4(x) = 2x^{11} + ux^{10} + 2x^9 + (u+1)x^8 + 2ux^7 + (u+1)x^6 + 2x^5 + 2ux^4 + (3u + 3)x^3 + (2u+3)x^2 + (u+2)x + 2$$
$$g_5(x) = 2ux^{13} + (u+1)x^{12} + ux^{11} + (u+2)x^{10} + 2x^9 + (u+1)x^8 + 2ux^7 + (u + 1)x^6 + 2x^5 + ux^4 + (u+3)x^3 + 2x^2 + 2x + 2$$
$$g_6(x) = (u+1)x^{14} + 2x^{13} + (u+1)x^{12} + 2x^{11} + ux^{10} + 2x^9 + (u+1)x^8 + 2ux^7 + (u+1)x^6 + 2x^5 + (2u+3)x^4 + 3x^3 + (u+2)x^2 + 2x + 2$$
$$g_7(x) = 2x^{17} + 2x^{16} + 2x^{15} + (3u+3)x^{14} + (2u+2)x^{13} + (u+1)x^{12} + 2x^{11} + ux^{10} + 2x^9 + (u+1)x^8 + 2x^7 + (u+1)x^6 + 2x^5 + 2ux^4 + (u+2)x^3 + ux^2 + (u+2)x + 2$$

4. DUALS OF δ_θ-CYCLIC CODES OVER R

In this section, we find the structure of the dual of a free δ_θ-cyclic code of even length n over R.

Definition 4.1. Let C be a δ_θ-cyclic code of length n over R. Then its dual is defined as

$$C^\perp = \{x \mid x \cdot y = 0 \text{ for all } y \in C\},$$

where $x \cdot y$ denotes the usual inner product of x and y, where $x = (x_0, x_1, \cdots, x_{n-1})$ and $y = (y_0, y_1, \cdots, y_{n-1})$ belong to R^n.

To determine a generator matrix of the dual of a free δ_θ-cyclic code C, we need to find the parity-check matrix of C. For this, we first require some lemmas.

Lemma 4.2. *For even n, $x^n - 1$ is a central element of $R[x, \theta, \delta_\theta]$, and hence $x^n - 1 = h(x)g(x) = g(x)h(x)$ for some $g(x), h(x) \in R[x, \theta, \delta_\theta]$.*

Proof. The proof is similar to the proof of Lemma 7 [8]. □

Remark 3. If C is a δ_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 $g'(x)$ in C such that $C = \langle g'(x) \rangle$.

Lemma 4.3. *Let C be a δ_θ-cyclic code of even length n over R generated by a monic right divisor $g(x)$ of $x^n - 1$. Then $v(x) \in R_{n,\delta_\theta}$ is in C if and only if $v(x)h(x) = 0$ in R_{n,δ_θ}, where $x^n - 1 = h(x)g(x)$.*

Proof. Suppose $v(x) \in C$. Then $v(x) = a(x)g(x)$ for some $a(x) \in R_{n,\delta_\theta}$. So $v(x)h(x) = a(x)g(x)h(x) = a(x)h(x)g(x) = 0$ in R_{n,δ_θ} (by Lemma 4.2). Conversely, suppose $v(x)h(x) = 0$ in R_{n,δ_θ} for some $v(x) \in R_{n,\delta_\theta}$. Then there exists $q(x) \in R[x, \theta, \delta_\theta]$ such that $v(x)h(x) = q(x)(x^n - 1) = q(x)h(x)g(x) = q(x)g(x)h(x)$. Since $h(x)$ is regular, $v(x) = q(x)g(x)$. Hence the result. □

Lemma 4.4. *Let $a \in R$ be a unit in R. Then $\theta(a) + \delta_\theta(b)$ is a unit for all $b \in R$.*

Proof. Let $d = \theta(a) + \delta_\theta(b)$, where $a, b \in R$ such that a is a unit. Let $\theta(a) = \alpha + u\beta$. Then $\alpha + u\beta$ is a unit, and hence either α or β is a unit but not both. We know $\delta_\theta(b)$ is either 0 or $2u + 2$ for all $b \in R$. If $\delta_\theta(b) = 0$, then we are done. Otherwise $d = (\alpha + 2) + u(\beta + 2)$. Also, any $c \in \mathbb{Z}_4$ is a unit if and only if $c + 2$ is a unit. Hence d is a unit. □

Theorem 4.5. *Let $C = \langle g(x) \rangle$ be a principally generated δ_θ-cyclic code of even length n over R such that $x^n - 1 = h(x)g(x)$ for some $h(x) = h_0 + h_1x + h_2x^2 +$*

$\cdots + h_k x^k \in R[x, \theta, \delta_\theta]$, *where* k *is odd. Then the matrix* $H =$

$$\begin{bmatrix} h_k & \theta(h_{k-1}) + \delta_\theta(h_k) & h_{k-2} & \cdots & \theta(h_0) + \delta_\theta(h_1) & \cdots & 0 & 0 \\ 0 & \theta(h_k) & h_{k-1} & \cdots & h_0 & \delta_\theta(h_0) & \cdots & 0 \\ 0 & 0 & h_k & h_{k-2} & \theta(h_{k-3}) + \delta_\theta(h_{k-2}) & \cdots & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & & \ddots & \vdots \\ 0 & 0 & \cdots & h_k & \theta(h_{k-1}) + \delta_\theta(h_k) & \cdots & h_1 & \theta(h_0) + \delta_\theta(h_1) \end{bmatrix}$$

is a parity-check matrix for C.

Proof. Let $c(x) \in C$. Then by Lemma 4.3, we have $c(x)h(x) = 0$ in R_{n,δ_θ}. Therefore the coefficients of $x^k, x^{k+1}, \cdots, x^{n-1}$ in $[c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-2}x^{n-2} + c_{n-1}x^{n-1}][h_0 + h_1 x + h_2 x^2 + \cdots + h_{k-1}x^{k-1} + h_k x^k]$ are all zero. So we have

$$\begin{aligned} c_0 h_k + c_1(\theta(h_{k-1}) + \delta_\theta(h_k)) + c_2 h_{k-2} + \cdots + c_k(\theta(h_0) + \delta_\theta(h_1)) &= 0 \\ c_1(\theta(h_k)) + c_2 h_{k-1} + c_3(\theta(h_{k-2}) + \delta_\theta(h_{k-1})) + \cdots + c_{k+1}h_0 + c_{k+2}\delta_\theta(h_0) &= 0 \\ c_2 h_k + c_3(\theta(h_{k-1}) + \delta_\theta(h_k)) + c_4 h_{k-2} + \cdots + c_{k+1}h_1 + c_{k+2}(\theta(h_0) + \delta_\theta(h_1)) &= 0 \\ &\vdots \\ c_{n-k-1}h_k + c_{n-k}(\theta(h_{k-1}) + \delta_\theta(h_k)) + \cdots + c_{n-2}h_1 + c_{n-1}(\theta(h_0) + \delta_\theta(h_1)) &= 0. \end{aligned}$$

From these equations, it is clear that for any $c \in C$, $cH^T = 0$, and hence $GH^T = 0$. Now each row of H is orthogonal to each $c \in C$, so $span(H) \subseteq C^\perp$. Moreover, H contains a square sub-matrix of order $n-k$ (by taking first $n-k$ coordinates of each row) with non-zero determinant, as it is a lower triangular matrix with all diagonal entries units (by Lemma 4.4). This implies that all rows of H are linearly independent. Therefore $|Span(H)| = |R|^{n-k}$. Also $|C||C^\perp| = |R|^n$ and $|C| = |R|^k$ give $|C^\perp| = |R|^{n-k}$. Hence $Span(H) = C^\perp$, and so H is a parity check matrix of C. □

The above result can similarly be proved for the case when k is even. In this case, matrix H is given as:

$$\begin{bmatrix} h_k & \theta(h_{k-1}) + \delta_\theta(h_k) & h_{k-2} & \cdots & h_0 & \delta_\theta(h_0) & \cdots & 0 \\ 0 & \theta(h_k) & h_{k-1} & \cdots & h_1 & \theta(h_0) + \delta_\theta(h_1) & \cdots & 0 \\ 0 & 0 & h_k & \cdots & h_2 & \theta(h_1) + \delta_\theta(h_2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & & \ddots & \vdots \\ 0 & 0 & \cdots & \theta(h_k) & h_{k-1} & \cdots & h_1 & \theta(h_0) + \delta_\theta(h_1) \end{bmatrix}.$$

Example 8. Let C be a δ_θ-cyclic code of length 6 generated by the polynomial $g(x) = (u+2)x^3 + 2x^2 + 3u$ such that $x^6 - 1 = (ux^3 + 2ux^2 + u)((u+2)x^3 + 2x^2 + 3u)$. Let $h(x) = ux^3 + 2ux^2 + u$. Then a parity check matrix of C (by Theorem 4.5) is given by

$$H = \begin{bmatrix} u & 2 & 0 & u+2 & 0 & 0 \\ 0 & u+2 & 2u & 0 & u & 2+2u \\ 0 & 0 & u & 2 & 0 & u+2 \end{bmatrix}.$$

One may verify that $GH^T = 0$ and the rows of H are linearly independent. Therefore H forms a parity check matrix for C.

5. Double δ_θ-cyclic codes over R

In this section, we study double δ_θ-cyclic codes over R.

A code C of length n is said to be a double δ_θ-linear code if the coordinates of the codewords are partitioned in two blocks of lengths α and β such that the set of the first blocks of α symbols and the set of second blocks of β symbols form δ_θ-linear codes of lengths α and β, respectively, over R.

For any $d \in R$ and $v = (a_0, a_1, \cdots, a_{\alpha-1}, b_0, b_1, \cdots, b_{\beta-1}) \in R^{\alpha+\beta}$, we define

$$dv = (da_0, da_1, \cdots, da_{\alpha-1}, db_0, db_1, \cdots, db_{\beta-1}).$$

With this multiplication, $R^{\alpha+\beta}$ is an R-module.

Definition 5.1. For an element $v = (a_0, a_1, \cdots, a_{\alpha-1}, b_0, b_1, \cdots, b_{\beta-1}) \in R^{\alpha+\beta}$, the $\delta_\theta(\alpha,\beta)$-*cyclic shift* of v, denoted by ${}^{\alpha\beta}T_{\delta_\theta}(v)$, is defined as ${}^{\alpha\beta}T_{\delta_\theta}(v) = (\theta(a_{\alpha-1}) + \delta_\theta(a_0), \theta(a_0) + \delta_\theta(a_1), \theta(a_1) + \delta_\theta(a_2), \cdots, \theta(a_{\alpha-2}) + \delta_\theta(a_{\alpha-1}),$
$\theta(b_{\beta-1}) + \delta_\theta(b_0), \theta(b_0) + \delta_\theta(b_1), \theta(b_1) + \delta_\theta(b_2), \cdots, \theta(b_{\beta-2}) + \delta_\theta(b_{\beta-1}))$.

A double δ_θ-linear code is an R-submodule of $R^{\alpha+\beta}$.

Definition 5.2. A double δ_θ-linear code C is called double δ_θ-cyclic code if C is invariant under the $\delta_\theta(\alpha,\beta)$-cyclic shift ${}^{\alpha\beta}T_{\delta_\theta}$.

In polynomial representation, an element $c = (a_0, a_1, \cdots, a_{\alpha-1}, b_0, b_1, \cdots, b_{\beta-1})$ in C can be identified with $c(x) = (c_1(x), c_2(x))$, where $c_1(x) = a_0 + a_1x + \cdots + a_{\alpha-1}x^{\alpha-1} \in \frac{R[x,\theta,\delta_\theta]}{\langle x^\alpha-1\rangle}$ and $c_2(x) = b_0 + b_1x \cdots + b_{\beta-1}x^{\beta-1} \in \frac{R[x,\theta,\delta_\theta]}{\langle x^\beta-1\rangle}$. This identification gives a one-to-one correspondence between $R^{\alpha+\beta}$ and $R_{\alpha,\beta} = \frac{R[x,\theta,\delta_\theta]}{\langle x^\alpha-1\rangle} \times \frac{R[x,\theta,\delta_\theta]}{\langle x^\beta-1\rangle}$. For convenience, we denote $(c_1(x), c_2(x))$ by $(c_1(x) \mid c_2(x))$. We define the multiplication of any $r(x) \in R[x,\theta,\delta_\theta]$ and $(g_1(x) \mid g_2(x)) \in \frac{R[x,\theta,\delta_\theta]}{\langle x^\alpha-1\rangle} \times \frac{R[x,\theta,\delta_\theta]}{\langle x^\beta-1\rangle}$ as

$$r(x)(g_1(x) \mid g_2(x)) = (r(x)g_1(x) \mid r(x)g_2(x)),$$

where $r(x)g_1(x)$ and $r(x)g_2(x)$ are the multiplication of polynomials in $\frac{R[x,\theta,\delta_\theta]}{\langle x^\alpha-1\rangle}$ and $\frac{R[x,\theta,\delta_\theta]}{\langle x^\beta-1\rangle}$, respectively. With this multiplication, $R_{\alpha,\beta}$ is a left $R[x,\theta,\delta_\theta]$ -module.

It can easily be seen that if $c(x) = (c_1(x) \mid c_2(x))$ represents the codeword c, then $xc(x)$ represents the $\delta_\theta(\alpha,\beta)$-cyclic shift of c.

Theorem 5.3. *Let C be a δ_θ-linear code of length $n = \alpha+\beta$ over R. Then C is a double δ_θ-cyclic code if and only if it is a left $R[x,\theta,\delta_\theta]$-submodule of the left-module $R[x,\theta,\delta_\theta]/\langle x^\alpha - 1\rangle \times R[x,\theta,\delta_\theta]/\langle x^\beta - 1\rangle$.*

Proof. Suppose C is a double δ_θ-cyclic code. Let $c \in C$, and let the associated polynomial of c be $c(x)$. As $xc(x)$ is a $\delta_\theta(\alpha,\beta)$-cyclic shift of c, so $xc(x) \in C$. By linearity of C, $r(x)c(x) \in C$ for any $r(x) \in R[x,\theta,\delta_\theta]$. So C is left $R[x,\theta,\delta_\theta]$-submodule of $R_{\alpha,\beta}$. Converse is straightforward. □

Theorem 5.4. *A double δ_θ-cyclic code of length $n = \alpha+\beta$ is a double cyclic code if α and β both are odd integers.*

Proof. Let C be a double δ_θ-cyclic code. Let $\gamma = lcm(\alpha,\beta)$. Then γ is odd, and so $gcd(\gamma,2) = 1$. Therefore there exist two integers a, b such that $\gamma a + 2b = 1$ and so $2b = 1 - \gamma a = 1 + \gamma l$ for some $l > 0$, where $l = -a \pmod{\gamma}$. Let $c(x) =$

$(a(x) \mid b(x)) \in C$, where $a(x) = \sum_{i=0}^{\alpha-1} a_i x^i$ and $b(x) = \sum_{i=0}^{\beta-1} b_i x^i$. Then

$$\begin{aligned}
x^{2b}c(x) = &\ x^{2b}\left(\sum_{i=0}^{\alpha-1} a_i x^i \mid \sum_{i=0}^{\beta-1} b_i x^i\right) = \left(\sum_{i=0}^{\alpha-1} a_i x^{i+2b} \mid \sum_{i=0}^{\beta-1} b_i x^{i+2b}\right) \\
= &\ \left(\sum_{i=0}^{\alpha-1} a_i x^{i+1+\gamma l} \mid \sum_{i=0}^{\beta-1} b_i x^{i+1+\gamma l}\right) \\
= &\ \left(\sum_{i=0}^{\alpha-2} a_i x^{i+1+\gamma l} + a_{\alpha-1}x^{\alpha+\gamma l} \mid \sum_{i=0}^{\alpha-2} a_i x^{i+1+\gamma l} + a_{\beta-1}x^{\beta+\gamma l}\right) \\
= &\ \left(\sum_{i=0}^{\alpha-2} a_i x^{i+1} + a_{\alpha-1} \mid \sum_{i=0}^{\beta-2} a_i x^{i+1} + a_{\beta-1}\right), (\text{since } x^\alpha = x^\beta = x^\gamma = 1).
\end{aligned}$$

Thus $x^{2b}c(x) = (a'(x) \mid b'(x))$, where $a'(x), b'(x)$ are cyclic shifts of $a(x)$ and $b(x)$, respectively. Hence C is a double cyclic code. □

Theorem 5.5. *Let C_1 and C_2 be two free δ_θ-cyclic codes of lengths n_1 and n_2 over R having monic generator polynomials $g_1(x)$ and $g_2(x)$, respectively, such that $g_1(x)|x^{n_1}-1$ and $g_2(x)|x^{n_2}-1$. Then a code C generated by $g(x) = (g_1(x) \mid g_2(x))$ is a double δ_θ-cyclic code and $A = \{g(x), xg(x), \cdots, x^{l-1}g(x)\}$ is a spanning set of C, where $l = \deg h(x)$ and $h(x)$ is the least left common multiple of $h_1(x)$ and $h_2(x)$.*

Proof. Let $x^{n_1} - 1 = h_1(x)g_1(x)$ and $x^{n_2} - 1 = h_2(x)g_2(x)$ for some monic polynomials $h_1(x), h_2(x) \in R[x, \theta, \delta_\theta]$. Then $h(x)g(x) = h(x)(g_1(x)|g_2(x)) = 0$, as $h(x)g_i(x) = h'(x)h_i(x)g_i(x) = 0$ for $i = 1, 2$. Now let $v(x) \in C$ be any non-zero codeword in C. Then $v(x) = a(x)g(x)$ for some $a(x) \in R[x, \theta, \delta_\theta]$. By the division algorithm, we have $a(x) = q(x)h(x) + r(x)$, where $r(x) = 0$ or $\deg r(x) < \deg h(x)$. Then $v(x) = a(x)g(x) = r(x)g(x) = 0$. Since $r(x) = 0$ or $\deg r(x) < \deg h(x)$, the result follows. □

Example 9. Let C be a double δ_θ-cyclic code of length $n = 10(= 6 + 4)$ over R, which is principally generated by $g(x) = (g_1(x)|g_2(x))$, where $g_1(x) = ux^3+2ux^2+u$ and $g_2(x) = x^2 + 2ux + 1$ such that $g_1(x)|x^6 - 1$ and $g_2(x)|x^4 - 1$. Now let $h(x)$ be the least left common multiple of $h_1(x)$ and $h_2(x)$. Then $\deg h(x) = 5$. Therefore the set $\{g(x), xg(x), x^2g(x), x^3g(x), x^4g(x)\}$ forms a spanning set for C. Hence a generator matrix of C is

$$\left[\begin{array}{cccccc|cccc}
u & 0 & 2u & u & 0 & 0 & 1 & 2u & 1 & 0 \\
2u+2 & u+2 & 0 & 2 & u+2 & 0 & 0 & 1 & 2u & 1 \\
0 & 0 & u & 0 & 2u & u & 1 & 0 & 1 & 2u \\
u+2 & 0 & 2u+2 & u+2 & 0 & 2 & 2u & 1 & 0 & 1 \\
2u & u & 0 & 0 & u & 0 & 1 & 2u & 1 & 0
\end{array}\right].$$

The parameters for $\Phi(C)$ are $[20, 4^9, 4]$. Moreover, $Res(C)$ and $Tor(C)$ have the parameters $[10, 4^5 2^1, 2]$ and $[10, 4^3 2^1, 4]$, respectively.

In Table 2, we present some good linear codes over $\mathbb{Z}_4$ as Gray images and residue codes of double skew-linear codes with derivation (not necessarily δ_θ-cyclic codes) over R.

In Table 2, we have $C^* = \{(u \mid u + v) : u, v \in Res(C)\}$

$$h_0(x) = ((2 + 3u) + (1 + 2u)x + ux^2 \mid 2u + (2 + 2u)x),$$

	C	$\Phi(C)$	$Res(C)$	C^*
Set of generators	Name	(n, M, d_L)	$(n, 4^{k_1}2^{k_2}, d_L)$	$(n, 4^{k_1}2^{k_2}, d_L)$
$\{h_0(x), xh_1(x)\}$	A_1	$(10, 128, 2)$	$(5, 4^3 2^1, 2)^*$	$(10, 4^6 2^2, 2)$
$\{h_1(x), xh_1(x), x^2h_1(x)\}$	A_2	$(12, 4096, 2)$	$(6, 4^5 2^1, 2)^*$	$(\mathbf{12}, \mathbf{4^{10}2^2}, \mathbf{2})^{**}$
$\{h_2(x), xh_2(x), x^2h_2(x), x^3h_2(x)\}$	A_3	$(14, 65536, 2)$	$(7, 4^6 2^1, 2)^*$	$(14, 4^{12} 2^2, 2)$
$\{h_3(x), xh_3(x), x^3h_2(x), x^3h_3(x)\}$	A_3	$(16, 65536, 4)$	$(\mathbf{8}, \mathbf{4^7}, \mathbf{2})^{**}$	$(\mathbf{16}, \mathbf{4^{14}}, \mathbf{2})^{**}$

TABLE 2. *:= Existing good code [2, 1], **:=New good code;

$$h_1(x) = ((3u+2) + (1+2u)x + ux^2 \mid 2 + (1+2u)x + 2ux^2),$$
$$h_2(x) = ((1+u) + (1+2u)x + (2+u)x^2 + ux^3 \mid 1 + 2ux + (u+1)x^2),$$
$$h_3(x) = ((1+u) + (1+2u)x + (2+u)x^2 + ux^3 \mid 1 + 2ux + (u+1)x^2 + 2ux^3).$$

Remark 4. The codes whose parameters are written in bold letters in Table 1 and Table 2 have improved the parameters of the existing codes having comparable parameters. These codes have been reported and added to the Database of $\mathbb{Z}_4$-codes [2].

6. Conclusion

This paper studies a class of skew-cyclic codes over $R = \mathbb{Z}_4 + u\mathbb{Z}_4$ with derivation. We have studied these codes as left $R[x, \theta, \delta_\theta]$-submodules. A Gray map is defined on R, and some good linear codes over $\mathbb{Z}_4$ via Gray images, residue codes of these codes have been obtained. The generator matrix of dual code of a free δ_θ-cyclic code of even length over R is obtained. These codes are generalized to double skew-cyclic codes with derivation. All new linear codes over $\mathbb{Z}_4$, obtained in this paper, have been reported and added to the database of Z4-codes. It will be interesting to obtain criteria under which the dual of a free δ_θ-cyclic code of even length over R is a δ_θ-cyclic code of same length.

All the computations to find codes were done with Magma computational algebra system [7].

Acknowledgments

This work was partially supported by DST, Govt. of India, under Grant No. SB/S4/MS: 893/14. Also, the first author would like to thank the Council of Scientific & Industrial Research (CSIR), India for providing financial support. The authors would also like to thank the anonymous referees for their valuable comments and suggestions.

References

[1] M. Araya, M. Harada, H. Ito and K. Saito, On the classification of Z4-codes, *Adv. Math. Commun.*, **11** (2017), 747–756.

[2] N. Aydin and T. Asamov, `http://www.z4codes.info` *The database of Z4 codes (Accessed March, 2018).*

[3] N. Aydin and T. Asamov, A database of Z4 codes, *J. Comb. Inf. Syst. Sci.*, **34** (2009), 1–12.
[4] M. Bhaintwal, Skew quasi-cyclic codes over Galois rings, *Des. Codes Cryptogr.*, **62** (2012), 85–101.
[5] I. F. Blake, Codes over certain rings, *Information and Control.*, **20** (1972), 396–404.
[6] I. F. Blake, Codes over integer residue rings, *Information and Control.*, **29** (1975), 295–300.
[7] W. Bosma, J. J. Cannon, C. Fieker and A. Steel, Handbook of magma functions, *Edition,* **2** (2010), 5017 pages.
[8] D. Boucher and F. Ulmer, Coding with skew polynomial rings, *J. of Symbolic Comput.*, **44** (2009), 1644–1656.
[9] D. Boucher , W. Geiselmann and F. Ulmer, Skew cyclic codes, *Appl. Algebra Engrg. Comm. Comput.*, **18** (2007), 379–389.
[10] D. Boucher and F. Ulmer, Codes as modules over skew polynomial rings, *In Proc. of* 12^{th} *IMA International Conference, Cryptography and Coding, Cirencester, UK, LNCS*, **5921** (2009), 38–55.
[11] D. Boucher, P. Solé and F. Ulmer, Skew constacyclic codes over Galois rings, *Adv. Math. Commun.*, **2** (2008), 273–292.
[12] D. Boucher and F. Ulmer, Linear codes using skew polynomials with automorphisms and derivations, *Des. Codes Cryptogr.*, **70** (2014), 405–431.
[13] S. T. Dougherty and K. Shiromoto, Maximum distance codes over rings of order 4, *IEEE Trans. Info Theory*, **47** (2001), 400–404.
[14] F. Gursoy, I. Siap and B. Yildiz, Construction of skew cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q$, *Adv. Math. Commum.*, **8** (2014), 313–322.
[15] Jr. A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. Sloane and P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes, *IEEE Trans. Inform. Theory*, **40** (1994), 301–319.
[16] S. Jitman, S. Ling and P. Udomkavanich, Skew constacyclic codes over finite chain rings, *Adv. Math. Commun.*, **6** (2012), 39–63.
[17] B. R. McDonald, *Finite Rings with Identity*, Marcel Dekker Inc, New York, 1974.
[18] M. Ozen, F. Z. Uzekmek, N. Aydin and N. T. Ozzaim, Cyclic and some constacyclic codes over the ring $\frac{Z_4[u]}{\langle u^2-1\rangle}$, *Finite Fields Appl.*, **38** (2016), 27–39.
[19] E. Prange, Cyclic error-correcting codes in two symbols, *Air Force Cambridge Research Center, Cambridge, MA, Tech. Rep. AFCRC-TN*, (1957), 57–103.
[20] M. Shi, L. Qian, L. Sok, N. Aydin and P. Sole, On constacyclic codes over $\frac{Z_4[u]}{\langle u^2-1\rangle}$ and their Gray images, *Finite Fields Appl.*, **45** (2017), 86–95.
[21] I. Siap, T. Abualrub, N. Aydin and P. Seneviratne, Skew cyclic codes of arbitrary length, *Int. J. Inf. Coding Theory*, **2** (2011), 10–20.
[22] E. Spiegel, Codes over $\mathbb{Z}_m$, *Information and Control.*, **35** (1977), 48–51.
[23] E. Spiegel, Codes over $\mathbb{Z}_m$ (revisited), *Information and Control.*, **37** (1978), 100–104.
[24] B. Yildiz and N. Aydin, On codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$ and their $\mathbb{Z}_4$-images, *Int. J. Inf. Coding Theory*, **2** (2014), 226–237.
[25] B. Yildiz and S. Karadeniz, Linear codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$: MacWilliams identities, projections, and formally self dual codes, *Finite Fields Appl.*, **27** (2014), 24–40.

Received October 2017; revised March 2018.

E-mail address: apsharmaiitr@gmail.com
E-mail address: mahesfma@iitr.ac.in