Communications in Combinatorics and Optimization
Vol. 10, No. 3 (2025), pp. 497-517
https://doi.org/10.22049/cco.2024.28837.1744

CCO
Commun. Comb. Optim.

Research Article

Skew cyclic codes over $\mathbb{Z}_4 + v\mathbb{Z}_4$ with derivation: structural properties and computational results

Djoko Suprijanto[1,*], Hopein Christofen Tang[1,2]

[1] Combinatorial Mathematics Research Group, Faculty of Mathematics and Natural Sciences, Institut Teknologi Bandung, Jl. Ganesha 10, Bandung, 40132, Indonesia
[*] djoko.suprijanto@itb.ac.id

[2] School of Mathematics and Statistics, UNSW, Sydney, Australia
hopein.tang@unsw.edu.au

Received: 14 July 2023; Accepted: 10 January 2024
Published Online: 17 January 2024

Abstract: In this work, we study a class of skew cyclic codes over the ring $R := \mathbb{Z}_4 + v\mathbb{Z}_4$, where $v^2 = v$, with an automorphism θ and a derivation Δ_θ, namely codes as modules over a skew polynomial ring $R[x; \theta, \Delta_\theta]$, whose multiplication is defined using an automorphism θ and a derivation Δ_θ. We investigate the structures of a skew polynomial ring $R[x; \theta, \Delta_\theta]$. We define Δ_θ-cyclic codes as a generalization of the notion of cyclic codes. The properties of Δ_θ-cyclic codes as well as dual Δ_θ-cyclic codes are derived. As an application, some new linear codes over $\mathbb{Z}_4$ with good parameters are obtained by Plotkin sum construction, also via a Gray map as well as residue and torsion codes of these codes.

Keywords: cyclic codes, quasi-cyclic codes, skew polynomial ring, skew cyclic codes, derivation.

AMS Subject classification: 94B05, 94B15, 11T71

1. Introduction

Cyclic codes are an important class of codes from both theoretical and practical viewpoints. Theoretically, cyclic codes have a rich mathematical theory, in particular, they have additional algebraic structures to make, practically, the process of encoding and decoding cyclic codes is more efficient.

Cyclic codes over finite fields were first studied by Prange [21] in 1957. Since then, many coding theorists have made significant progress in studying cyclic codes for both

* *Corresponding Author*

the so-called random-error correction and burst-error correction (See, for example, [13] for the detailed description of random-error and burst-error correction).

In 2007, Boucher, Geiselmann, and Ulmer [6] (see also [8],[7]) extended the notion of cyclic codes over finite fields by using generator polynomials in non-commutative skew polynomial rings. The new notion of codes is called skew cyclic codes over finite fields. In general, a skew polynomial ring is not a unique factorization ring. In this case, there are typically more factors of $x^n - 1$ in this ring than in the commutative case. Hence, there are more skew cyclic codes than cyclic codes over finite fields. This new class of codes increases the number of possibilities for finding codes with good parameters. Boucher, Geiselmann, and Ulmer [6] also give many examples of codes that improve the previously best-known linear codes over finite fields.

Later, the notion of skew cyclic codes over finite fields was generalized to the skew cyclic codes over several kinds of finite rings. Abualrub, Aydin, and Seneviratne [1] considered skew cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$, where $v^2 = v$, and constructed optimal self-dual codes over this ring. Gursoy, Siap, and Yildiz [12] investigated structural properties of skew cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q$, with $v^2 = v$. They [12] showed that skew cyclic codes over the ring are principally generated. Later, the first author together with his coauthors considered structural aspects of skew cyclic codes over the rings A_k [15] and B_k [16] (c.f. [14]), respectively. Very recently, Benbelkacem, Ezerman, Abualrub, Aydin, and Batoul [4] considered the skew cyclic codes over the mixed alphabet which are also a finite ring, denoted by $\mathbb{F}_4 R$, where $R = \mathbb{F}_4 + v\mathbb{F}_4$ with $v^2 = v$. They [4] showed a natural connection between the skew cyclic codes over the ring to DNA codes.

In the next development, Boucher and Ulmer [9] generalized the notion of skew cyclic codes over finite fields to the skew cyclic codes over finite fields with derivation. They [9] also constructed MDS as well as MRD codes from certain families of the skew cyclic codes (see Section 4.3 in [9]). Sharma and Bhaintwal [22] extended the study of these skew cyclic codes over a finite ring, namely over the ring $\mathbb{Z}_4 + u\mathbb{Z}_4$, with $u^2 = 1$. They obtained numerous linear codes over $\mathbb{Z}_4$ with good parameters using residue codes, Plotkin sum, or the Gray map they defined [22]. Very recently, Patel and Prakash [20] have investigated the same object over the ring $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$, with $u^2 = u$ and $v^2 = v$, where q is a prime power. By the decomposition method, they [20] obtained several optimal linear codes over $\mathbb{F}_q$.

Continuing the study of [22] and [20], in this paper, we investigate a class of skew cyclic codes with derivation over the ring $\mathbb{Z}_4 + v\mathbb{Z}_4$, with $v^2 = v$. We derive several structural properties of skew cyclic codes with derivation over the ring $\mathbb{Z}_4 + v\mathbb{Z}_4$. As a by-product, we construct many new linear codes over $\mathbb{Z}_4$ with good parameters.

The organization of the paper is as follows. In Section 2, we provide some definitions and basic facts related to the ring $\mathbb{Z}_4 + v\mathbb{Z}_4$ and also the linear codes over the ring $\mathbb{Z}_4 + v\mathbb{Z}_4$. We also define a Gray map from $\mathbb{Z}_4 + v\mathbb{Z}_4$ to $\mathbb{Z}_4^2$, which can be extended naturally to define the Gray map from $(\mathbb{Z}_4 + v\mathbb{Z}_4)^n$ to $\mathbb{Z}_4^{2n}$. Several properties of the skew-polynomial ring $(\mathbb{Z}_4 + v\mathbb{Z}_4)[x; \theta, \Delta_\theta]$ are derived. The notion of Δ_θ-cyclic codes, as well as dual of Δ_θ-cyclic codes as a generalization of cyclic codes together

with their properties are investigated in Section 3 and Section 4, respectively. Several examples of linear codes over $\mathbb{Z}_4$ with good parameters obtained by using the Plotkin sum construction, a Gray map, or residue and torsion codes of these classes of codes are provided in Section 5. The paper is ended with concluding remarks. We follow [13] for undefined terms in coding theory.

2. Preliminaries

In this section, we present some definitions together with some basic facts regarding the ring $\mathbb{Z}_4 + v\mathbb{Z}_4$, linear codes over the ring, and the skew-polynomial ring $(\mathbb{Z}_4 + v\mathbb{Z}_4)[x; \theta, \Delta_\theta]$ that is required in the next sections.

2.1. The ring $\mathbb{Z}_4 + v\mathbb{Z}_4$

Let $R := \mathbb{Z}_4 + v\mathbb{Z}_4 = \{a + bv : \ a, b \in \mathbb{Z}_4\}$, with $v^2 = v$. This ring is isomorphic to a polynomial ring, namely $R \cong \dfrac{\mathbb{Z}_4[v]}{\langle v^2 - v\rangle}$. An element $a + bv \in R$ is a unit if and only if a and $a + b$ both are units in $\mathbb{Z}_4$. Since the units of $\mathbb{Z}_4$ are 1 and 3, the units of R are 1, 3, $1 + 2v$, and $3 + 2v$. Hence, the non-units of R are

$$\{0,\ 2,\ v,\ 2v,\ 3v,\ 1+v,\ 1+3v,\ 2+v,\ 2+2v,\ 2+3v,\ 3+v,\ 3+3v\}.$$

R is a principal ideal ring with 7 non-trivial ideals, namely

$$\begin{aligned}
\langle 2v\rangle &= \{0, 2v\},\\
\langle 2+2v\rangle &= \{0, 2+2v\},\\
\langle 2\rangle &= \{0, 2, 2v, 2+2v\},\\
\langle v\rangle &= \{0, v, 2v, 3v\} = \langle 3v\rangle,\\
\langle 3+v\rangle &= \{0, 1+3v, 2+2v, 3+v\} = \langle 1+3v\rangle,\\
\langle 1+v\rangle &= \{0, 2, 2v, 1+v, 1+3v, 2+2v, 3+v, 3+3v\} = \langle 3+3v\rangle,\\
\langle 2+v\rangle &= \{0, 2, v, 2v, 3v, 2+v, 2+2v, 2+3v\} = \langle 2+3v\rangle.
\end{aligned}$$

The maximal ideals of R are $\langle 1 + v\rangle$ and $\langle 2 + v\rangle$. Hence, R is a semi-local ring. For more information on the structures of the ring $R = \mathbb{Z}_4 + v\mathbb{Z}_4$, the reader can refer to [3], [11], and [17].

2.2. Linear codes over R

Lee weight is an important weight to consider on $\mathbb{Z}_4$. For $x \in \mathbb{Z}_4$, the Lee weight of x, denoted by $w_L(x)$, is defined as $w_L(0) = 0$, $w_L(1) = 1 = w_L(3)$, $w_L(2) = 2$. The Lee weight for any vector $(r_0, r_1, \ldots, r_{n-1}) \in \mathbb{Z}_4^n$ is defined as the rational sum of Lee weights of its coordinates, namely $w_L((r_0, r_1, \ldots, r_{n-1})) = w_L(r_0) + w_L(r_1) + \cdots + w_L(r_{n-1})$. Define a Gray map $\phi : R \longrightarrow \mathbb{Z}_4^2$ as

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

The Gray weight $w_G(a+bv)$ for any $a+bv \in R$ is defined as $w_G(a+bv) = w_L(\phi(a+bv))$. The Gray weights of the elements of R are given as follows.

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

The Gray map ϕ is extended naturally to $\Phi : R^n \longrightarrow \mathbb{Z}_4^{2n}$ as

$$\Phi((a_0 + b_0v, a_1 + b_1v, \ldots, a_{n-1} + b_{n-1}v)) = (a_0, a_0 + b_0, a_1, a_1 + b_1, \ldots, a_{n-1}, a_{n-1} + b_{n-1}),$$

and the Gray weight of any vector $\mathbf{x} \in R^n$ is defined as the rational sum of Gray weights of its coordinates.

A code C of length n over R is a non-empty subset of R^n. A code C is called linear over R if it is an R-submodule of R^n. A linear code over R is called free if it is free as an R-submodule. The Gray distance of any vectors $\mathbf{x}, \mathbf{y} \in R^n$ is defined as $d_G(\mathbf{x}, \mathbf{y}) = w_G(\mathbf{x} - \mathbf{y})$ and the Lee distance of any vectors $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_4^n$ is defined as $d_L(\mathbf{x}, \mathbf{y}) = w_L(\mathbf{x} - \mathbf{y})$. The minimum Gray distance $d_G(C)$ and the minimum Lee distance $d_L(C)$ of C is defined as $d_G(C) := \min\{d_G(\mathbf{x}, \mathbf{y}) : \ \mathbf{x}, \mathbf{y} \in C, \ \mathbf{x} \neq \mathbf{y}\}$ and $d_L(C) := \min\{d_L(\mathbf{x}, \mathbf{y}) : \ \mathbf{x}, \mathbf{y} \in C, \ \mathbf{x} \neq \mathbf{y}\}$, respectively. It is easy to verify that the Gray map Φ is a distance-preserving map (isometry) from (R^n, d_G) to $(\mathbb{Z}_4^{2n}, d_L)$.

A (linear) code over the ring $\mathbb{Z}_4$ is defined similarly. We write the parameters of a linear code C over $\mathbb{Z}_4$ as $[n, 4^{k_1}2^{k_2}, d_L]$, where n is the length of C, $|C| = 4^{k_1}2^{k_2}$, and $d_L = d_L(C)$. Moreover, following Hammons, Kumar, Calderbank, Sloane, and Solé [10] (cf. [24]), we say that the code C is of type $4^{k_1}2^{k_2}$. For a linear code $C \subseteq R^n$ over R, we define the residue code $Res(C)$ and the torsion code $Tor(C)$ of C, respectively, as

$$Res(C) := \{\mathbf{a} : \ \mathbf{a} + \mathbf{b}v \in C, \text{ for some } \mathbf{b} \in \mathbb{Z}_4^n\},$$

and

$$Tor(C) := \{\mathbf{b} : \ \mathbf{b}v \in C\}.$$

We note that $Res(C)$ and $Tor(C)$ are linear codes of length n over $\mathbb{Z}_4$. Regarding the residue and torsion codes, we have the following property.

Lemma 1. *Let C be a free linear code of length n over R and $\{\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_k\}$, with $\mathbf{c}_i = \mathbf{a}_i + \mathbf{b}_i v$, be a basis of C. Then the following statements hold:*

(1) $Res(C)$ is a free linear code over $\mathbb{Z}_4$ with $\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_k\}$ as a basis.

(2) $Tor(C)$ is a free linear code over $\mathbb{Z}_4$ with $\{\mathbf{a}_1 + \mathbf{b}_1, \mathbf{a}_2 + \mathbf{b}_2, \ldots, \mathbf{a}_k + \mathbf{b}_k\}$ as a basis.

Proof. We prove only part (1).
Let $\mathbf{a} \in Res(C)$. Then there exists $\mathbf{b} \in \mathbb{Z}_4^n$ such that $\mathbf{a}+\mathbf{b}v \in C$. Since $\{\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_k\}$ is a basis of C, there exist $r_1, r_2, \ldots, r_k \in R$, with $r_i = s_i + t_i v$, for $i \in [1,k]_{\mathbb{Z}}$, such that

$$\mathbf{a} + \mathbf{b}v = \sum_{i=1}^{k} s_i \mathbf{a}_i + \left(\sum_{i=1}^{k} (s_i \mathbf{b}_i + t_i \mathbf{a}_i + t_i \mathbf{b}_i) \right) v,$$

which means $\mathbf{a} = \sum_{i=1}^{k} s_i \mathbf{a}_i$, and $\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_k\}$ generates $Res(C)$. Next, suppose on the contrary that $\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_k\}$ is linearly dependent. It is easy to prove that $\{\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_k\}$ is also linearly dependent, a contradiction. Therefore, $\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_k\}$ must be linearly independent and we conclude that $\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_k\}$ is a basis of $Res(C)$. □

Similarly, we obtain the following theorem.

Theorem 1. *If C be a free linear code of length n over R having a basis $\{\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_k\}$, then $\{\Phi(\mathbf{c}_1), \Phi(\mathbf{c}_1 v), \Phi(\mathbf{c}_2), \Phi(\mathbf{c}_2 v), \ldots, \Phi(\mathbf{c}_k), \Phi(\mathbf{c}_k v)\}$ is a basis of a free linear code $\Phi(C)$.*

2.3. Skew-polynomial ring $R[x; \theta, \Delta_\theta]$

We first recall the definition of a derivation on a finite ring $\mathbf{R}$ following [9].

Definition 1. Let $\mathbf{R}$ be a finite ring and $\Theta : \mathbf{R} \longrightarrow \mathbf{R}$ be an automorphism on $\mathbf{R}$. Then a map $\Delta_\Theta : \mathbf{R} \longrightarrow \mathbf{R}$ is called a derivation on $\mathbf{R}$ if the following two conditions are satisfied:

(i) $\Delta_\Theta(x+y) = \Delta_\Theta(x) + \Delta_\Theta(y)$, and

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

Let $\mathbf{R}$ be a finite ring with an automorphism Θ and a derivation Δ_Θ. The skew-polynomial ring $\mathbf{R}[x; \Theta, \Delta_\Theta]$ is the set of all polynomials over $\mathbf{R}$ with ordinary addition of polynomials and multiplication defined by

$$xa := \Theta(a)x + \Delta_\Theta(a),$$

for any $a \in \mathbf{R}$. This multiplication is extended to all polynomials in $\mathbf{R}[x; \Theta, \Delta_\Theta]$ in the usual manner. This kind of ring was introduced by Ore [19] in 1933, where $\mathbf{R}$ is the finite field $\mathbb{F}_q$. See also McDonald [18].
Consider a map $\theta : R \longrightarrow R$ defined by $\theta(a+bv) = a + b - bv$. It is easy to see that θ defines an automorphism of R. Moreover, since for all $a + bv \in R$ we have $\theta^2(a+bv) = a + bv$, we conclude that the order of θ is 2.

Lemma 2. *For all $x \in R$, a map $\Delta_\theta : R \longrightarrow R$ such that*

$$\Delta_\theta(x) = (1 + 2v)(\theta(x) - x)$$

defines a derivation on R.

Proof. Straightforward by definition. □

We prove several properties related to the derivation Δ_θ on R. We begin with the following that can be derived by a routine computation.

Lemma 3. *Let $\Delta_\theta(x) = (1 + 2v)(\theta(x) - x)$ be a derivation on R. Then the following statements hold:*

(1) $\Delta_\theta\theta + \theta\Delta_\theta \equiv 0$.

(2) $\Delta_\theta\Delta_\theta \equiv 0$.

(3) for all $x \in R$, $\Delta_\theta(x) = 0 \iff \theta(x) = x$.

Lemma 4. *For all $a \in R$, we have $x^2a = ax^2$.*

Proof. Since $xa = \theta(a)x + \Delta_\theta(a)$,

$$\begin{aligned} x^2a &= x\theta(a)x + x\Delta_\theta(a) \\ &= (\theta^2(a)x + \Delta_\theta(\theta(a)))x + \theta(\Delta_\theta(a))x + \Delta_\theta^2(a) \\ &= \theta^2(a)x^2 + ((\Delta_\theta\theta + \theta\Delta_\theta)(a))x + \Delta_\theta^2(a) \\ &= ax^2 \qquad \text{(by Lemma 3).} \end{aligned}$$

□

We can generalize Lemma 4 using mathematical induction.

Corollary 1. *For all $a \in R$, $n \in \mathbb{Z}^+$, we have*

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

Proof. We know that $xa = \theta(a)x + \Delta_\theta(a)$ and $x^2a = ax^2$. Suppose the above statement holds for all $n \leq k$, with $k \geq 2$. Consider two cases. If $k + 1$ is even, then $k - 1$ is also even. From the induction hypothesis,

$$x^{k+1}a = x^2(x^{k-1}a) = x^2ax^{k-1} = (ax^2)x^{k-1} = ax^{k+1}.$$

If $k+1$ is odd, then k is even. Again, from the induction hypothesis,

$$x^{k+1}a = x(x^k a) = x(ax^k) = (xa)x^k = (\theta(a)x + \Delta_\theta(a))x^k.$$

Then the result follows. □

Let R^θ be a subset of R, fixed element-wise by θ, namely $R^\theta := \{a \in R : \ \theta(a) = a\}$. It is easy to verify that R^θ is a subring of R. In our case, $R^\theta = \{0, 1, 2, 3\} = \mathbb{Z}_4$. Also, for all $a \in R^\theta$, we have $\Delta_\theta(a) = 0$. It implies, by Corollary 1, that for all $a \in R^\theta$ and $n \in \mathbb{Z}^+$, we have $x^n a = ax^n$.

Definition 2. A polynomial $f(x) \in R[x; \theta, \Delta_\theta]$ is called a central element if it satisfies

$$f(x)a(x) = a(x)f(x),$$

for all $a(x) \in R[x; \theta, \Delta_\theta]$. The center of $R[x; \theta, \Delta_\theta]$, denoted by $Z(R[x; \theta, \Delta_\theta])$, is defined as

$$Z(R[x; \theta, \Delta_\theta]) := \{f(x) \in R[x; \theta, \Delta_\theta] : \ f(x)a(x) = a(x)f(x), \text{ for all } a(x) \in R[x; \theta, \Delta_\theta]\}.$$

The central element satisfies the following property.

Theorem 2. *$f(x) \in Z(R[x; \theta, \Delta_\theta])$ if and only if $f(x) \in R^\theta[x]$ and for all odd integers i, the coefficient of x^i is equal to 0.*

Proof. ($\Longrightarrow$) Let $f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_k x^k$. Observe that

$$xf(x) = \sum_{i=0}^{k} (xf_i)x^i = \sum_{i=0}^{k} (\theta(f_i)x + \Delta_\theta(f_i))x^i = \Delta_\theta(f_0) + \sum_{i=1}^{k} (\theta(f_{i-1}) + \Delta_\theta(f_i))\, x^i + \theta(f_k)x^{k+1}$$

and

$$f(x)x = f_0 x + f_1 x^2 + \cdots + f_k x^{k+1}.$$

Since $f(x)$ is a central element, $xf(x) = f(x)x$, which implies

$$\Delta_\theta(f_0) = 0, \tag{2.1}$$

$$\theta(f_{i-1}) + \Delta_\theta(f_i) = f_{i-1}, \text{ for } 1 \le i \le k, \tag{2.2}$$

$$\theta(f_k) = f_k. \tag{2.3}$$

The Equation (2.3) implies $f_k \in R^\theta$. By Lemma 3 we have $\Delta_\theta(f_k) = 0$. By substituting the Equation (2.2) repeatedly we obtain $f_1, f_2, \ldots, f_{k-1} \in R^\theta$. Moreover, by Equation (2.1) and Lemma 3 obtain $f_0 \in R^\theta$. Thus, $f(x) \in R^\theta[x]$.

Now, take $a = v \in R$. Observe that

$$af(x) = af_0 + af_1x + \cdots + af_kx^k \text{ and } f(x)a = f_0a + \sum_{i=1}^{k} f_i(x^ia).$$

In this case, for $0 \leq 2j < k$, the coefficient of x^{2j} in $af(x)$ and $f(x)a$ is equal to af_{2j} and $f_{2j}a + f_{2j+1}\Delta_\theta(a)$, respectively. Since $f(x)$ is a central element and $\Delta_\theta(a) = 1$, we conclude that $f_{2j+1} = 0$.
($\Longleftarrow$) Let $f(x) = f_0 + f_2x^2 + f_4x^4 + \cdots + f_{2m}x^{2m} \in R^\theta[x]$. Let $a(x) = a_0 + a_1x + a_2x^2 + \cdots + a_kx^k \in R[x;\theta,\Delta_\theta]$. Observe that

$$(f_{2i}x^{2i})(a_jx^j) = f_{2i}(x^{2i}a_j)x^j = f_{2i}a_jx^{2i+j},$$

and

$$\begin{aligned}(a_jx^j)(f_{2i}x^{2i}) &= a_j(x^jf_{2i})x^{2i}\\ &= \begin{cases} a_j\theta(f_{2i})x^{2i+j} + a_j\Delta_\theta(f_{2i})x^{2i+j-1}, & \text{if } j \text{ is odd},\\ a_jf_{2i}x^{2i+j}, & \text{if } j \text{ is even},\end{cases}\\ &= a_jf_{2i}x^{2i+j} \text{ (by Lemma 3)}.\end{aligned}$$

Then $(f_{2i}x^{2i})(a_jx^j) = (a_jx^j)(f_{2i}x^{2i})$, for all i, j. Hence, $f(x)a(x) = a(x)f(x)$, for all $a(x) \in R[x;\theta,\Delta_\theta]$. □

We end this section by establishing the right-division algorithm below.

Lemma 5 (Right-Division Algorithm). *Let $f(x), g(x) \in R[x;\theta,\Delta_\theta]$ such that the leading coefficient of $g(x)$ is a unit. Then there exist $q(x), r(x) \in R[x;\theta,\Delta_\theta]$ such that*

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

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

Proof. Similar to the proof of Theorem 2.8 in [22] and Theorem 1 in [20]. □

3. Δ_θ-cyclic codes over R

For $f(x)$ a polynomial of degree n in $R[x;\theta,\Delta_\theta]$, let

$$\langle f(x)\rangle = \{a(x)f(x) :\ a(x) \in R[x;\theta,\Delta_\theta]\}.$$

It is easy to see that $R[x;\theta,\Delta_\theta]/\langle f(x)\rangle$ is a left module over $R[x;\theta,\Delta_\theta]$, where the scalar multiplication is defined by

$$r(x)\,(a(x) + \langle f(x)\rangle) := r(x)a(x) + \langle f(x)\rangle.$$

Definition 3. A code $C \subseteq R^n$ is called a Δ_θ-linear code of length n over R if C is a left $R[x;\theta,\Delta_\theta]$-submodule of $R[x;\theta,\Delta_\theta]/\langle f(x)\rangle$ for $f(x) \in R[x;\theta,\Delta_\theta]$ a polynomial of degree n. If $f(x)$ is a central element, then C is called a central Δ_θ-linear code.

Definition 4. A code $C \subseteq R^n$ is called a Δ_θ-cyclic code of length n over R if C is a Δ_θ-linear code and for all $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in C$ we have

$$T_{\Delta_\theta}(\mathbf{c}) := (\theta(c_{n-1}) + \Delta_\theta(c_0), \theta(c_0) + \Delta_\theta(c_1), \ldots, \theta(c_{n-2}) + \Delta_\theta(c_{n-1})) \in C.$$

Here, T_{Δ_θ} is called a Δ_θ-cyclic shift operator.

Remark 1. If θ is the identity automorphism and $\Delta_\theta \equiv 0$, then we obtain a (usual) cyclic code. Hence, the Δ_θ-cyclic code is a generalization of a cyclic code. Moreover, recall that if θ is the identity automorphism and $\Delta_\theta \equiv 0$, then a linear code $C \subseteq R^n$ is called quasi-cyclic of index k (k is a divisor of n) if for all $\mathbf{c} \in C$, we have $T^k_{\Delta_\theta}(\mathbf{c}) \in C$. Here $T^k_{\Delta_\theta}(\mathbf{c}) = \underbrace{(T_{\Delta_\theta} \circ T_{\Delta_\theta} \circ \cdots \circ T_{\Delta_\theta})}_{k}(\mathbf{c})$, the composition of k numbers of Δ_θ-cyclic shift operator.

For our purpose, to convert the algebraic structures of Δ_θ-cyclic codes into combinatorial structures and vice versa, we consider the following correspondence:

$$\begin{array}{ccc} R[x;\theta,\Delta_\theta]/\langle f(x)\rangle & \longrightarrow & R^n, \\ c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1}x^{n-1} & \longmapsto & (c_0, c_1, \ldots, c_{n-1}). \end{array}$$

From now on, let $R_{n,\Delta_\theta} := R[x;\theta,\Delta_\theta]/\langle x^n - 1\rangle$.

Lemma 6. *If $c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1}x^{n-1} \in R_{n,\Delta_\theta}$ is identified by a codeword $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in R^n$, then $xc(x) \in R_{n,\Delta_\theta}$ is identified by $T_{\Delta_\theta}(\mathbf{c}) \in R^n$.*

Proof. We have

$$\begin{aligned} xc(x) &= x\left(\sum_{i=0}^{n-1} c_i x^i\right) \\ &= \sum_{i=1}^{n-1} \left(\theta(c_{i-1}) + \Delta_\theta(c_i)\right) x^i + \left(\theta(c_{-1}) + \Delta_\theta(c_0)\right) \text{ (denoting that } c_{-1} = c_{n-1}) \\ &= \sum_{i=0}^{n-1} (\theta(c_{i-1}) + \Delta_\theta(c_i)) x^i. \end{aligned}$$

It means that $xc(x)$ is identified by $T_{\Delta_\theta}(\mathbf{c}) \in R^n$. □

Lemma 7. *A code $C \subseteq R^n$ is Δ_θ-cyclic code if and only if C is a left $R[x;\theta,\Delta_\theta]$-submodule of R_{n,Δ_θ}.*

Proof. ($\Longrightarrow$) Since C is a Δ_θ-linear code, $(C,+)$ is a subgroup of $(R_{n,\Delta_\theta},+)$, and for any $\mathbf{c} \in C$, identified by $c(x) \in R_{n,\Delta_\theta}$, we have $T_{\Delta_\theta}(\mathbf{c}) \in C$. By Lemma 6, $T_{\Delta_\theta}(\mathbf{c}) \in C$ can be identified by $xc(x) \in R_{n,\Delta_\theta}$. Inductively, we obtain $x^i c(x) \in C$, for all $i \in \mathbb{Z}^+$. By the linearity of the scalar multiplication, we have $a(x)c(x) \in C$ for all $a(x) \in R[x;\theta,\Delta_\theta]$. Hence, C is a left submodule of R_{n,Δ_θ}.
($\Longleftarrow$) If C is a left submodule of R_{n,Δ_θ}, then for all $\mathbf{c} \in C$, identified by $c(x) \in R_{n,\Delta_\theta}$, we have $xc(x) \in C$. By Lemma 6, $xc(x)$ can be identified by $T_{\Delta_\theta}(\mathbf{c}) \in R^n$. Hence, $T_{\Delta_\theta}(\mathbf{c}) \in C$, which implies that C is a Δ_θ-cyclic code. □

Corollary 2. *If $C \subseteq R^n$ is a Δ_θ-cyclic code of even length n, then C is an ideal of R_{n,Δ_θ}.*

Proof. Since n is even, by Theorem 2, $x^n - 1$ is a central element. Then for all $a(x) \in R[x;\theta,\Delta_\theta]$, we have $a(x)(x^n-1) = (x^n-1)a(x)$. Then $\langle x^n-1\rangle$ is a two-sided ideal of $R[x;\theta,\Delta_\theta]$. Since C is a left submodule of R_{n,Δ_θ}, C is an ideal of R_{n,Δ_θ}. □

Lemma 8. *Let $C \subseteq R^n$ be a Δ_θ-cyclic code. Then the following two statements hold.*

(1) C is 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) If n is odd, then there exists $b \in \mathbb{Z}$ such that $2b = n+1$. Let $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in C$ be a codeword identified by $c(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{n-1}x^{n-1} \in R_{n,\Delta_\theta}$. It is clear that $x^{2b}c(x) \in C$. Observe that

$$x^{2b}c(x) = x^{2b}\sum_{i=0}^{n-1} c_ix^i = \sum_{i=0}^{n-1}(x^{2b}c_i)x^i = \sum_{i=0}^{n-1} c_ix^{n+1+i} = \sum_{i=0}^{n-1} c_{i-1}x^i \text{ (denoting that } c_{-1} = c_{n-1}).$$

Note that $x^{2b}c_i = c_ix^{2b}$ is derived from Corollary 1. The equation above says that the codeword $x^{2b}c(x) \in C$ can be identified by the vector $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$. Thus, C is a cyclic code.

(2) Observe that for every vector $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in C$ identified by the polynomial $c(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{n-1}x^{n-1} \in R_{n,\Delta_\theta}$ we have $x^2c(x) \in C$. By the similar way as in part (1), we can show that $x^2c(x)$ can be identified by $(c_{n-2}, c_{n-1}, c_0, \ldots, c_{n-3}) \in C$. Then C is a quasi-cyclic code of index 2.

□

Lemma 9. *If $C \subseteq R^n$ is a Δ_θ-cyclic code and $g(x)$ is a nonzero polynomial in C of smallest degree with leading coefficient is a unit, then the following three statements hold.*

(1) $C = \langle g(x)\rangle$.

(2) $g(x)$ is a right divisor of $x^n - 1$.

(3) $\{g(x), xg(x), \ldots, x^{n-k-1}g(x)\}$ is a basis of C, with $k = \deg(g(x))$.

Proof. (1) It is clear that $\langle g(x)\rangle \subseteq C$. Let $c(x) \in C$. By the right-division algorithm, there exist $q(x), r(x) \in R[x;\theta,\Delta_\theta]$ such that

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

with $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$. Since C is a left submodule of R_{n,Δ_θ} over $R[x;\theta,\Delta_\theta]$, $r(x) = c(x) - q(x)g(x) \in C$. Moreover, since $g(x)$ is a nonzero polynomial of smallest degree, $r(x) = 0$. Thus, $c(x) = q(x)g(x) \in \langle g(x)\rangle$, and hence $C \subseteq \langle g(x)\rangle$.

(2) Again, by right-division algorithm, there exist $q(x), r(x) \in R[x;\theta,\Delta_\theta]$ such that

$$x^n - 1 = q(x)g(x) + r(x),$$

with $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$. By the same argument with above, we have $x^n - 1 = q(x)g(x)$. It means that $g(x)$ is is a right divisor of $x^n - 1$.

(3) From the above result, let $x^n - 1 = h(x)g(x)$, for some $h(x) \in R[x;\theta,\Delta_\theta]$. Let $c(x) \in C = \langle g(x)\rangle$ and let $c(x) = \ell(x)g(x)$ for some $\ell(x) \in R[x;\theta,\Delta_\theta]$. If $\deg(\ell(x)) \leq n-k-1$, then $c(x) \in \langle g(x), xg(x), \ldots, x^{n-k-1}g(x)\rangle$. If $\deg(\ell(x)) > n-k-1$, by using the right-division algorithm we come up with the conclusion that $c(x) = \ell(x)g(x) = r(x)g(x)$ (in R_{n,Δ_θ}) for some polynomial $r(x) \in R[x;\theta,\Delta_\theta]$ with $r(x) = 0$ or $\deg(r(x)) < \deg(h(x)) = n-k$, so $\{g(x), xg(x), \ldots, x^{n-k-1}g(x)\}$ generates C. Moreover, it is easy to see that the set is also linearly independent. Hence, we conclude that $\{g(x), xg(x), \ldots, x^{n-k-1}g(x)\}$ is a basis for C.

□

Since $\langle g(x)\rangle$ is a submodule of R_{n,Δ_θ} over $R[x;\theta,\Delta_\theta]$, by Lemma 7, C is a Δ_θ-cyclic code. The Lemma 9 above says that if $C = \langle g(x)\rangle$ is a Δ_θ-cyclic code, where $g(x)$ is a nonzero polynomial in C of smallest degree with a unit leading coefficient and $g(x)$ is also a right divisor of $x^n - 1$, then C is free. Hence, we obtained a construction method for Δ_θ-cyclic codes as described by the following.

Corollary 3. *If $g(x)$ is a right divisor of $x^n - 1$, with leading coefficient a unit, then $C = \langle g(x)\rangle$ is a free Δ_θ-cyclic code.*

Let $C = \langle g(x)\rangle$ be a free Δ_θ-cyclic code of length n generated by a right divisor $g(x)$ of $x^n - 1$, whose leading coefficient is a unit. Then the generator matrix G of C of dimension $(n-k)\times n$ is given by

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

where $g(x) = g_0 + g_1x + g_2x^2 + \cdots + g_kx^k$. To be more precise, if $n-k$ is odd, then

$$G = \begin{pmatrix} g_0 & g_1 & g_2 & \cdots & g_k & 0 & \cdots & 0 \\ \Delta_\theta(g_0) & \theta(g_0)+\Delta_\theta(g_1) & \theta(g_1)+\Delta_\theta(g_2) & \cdots & \theta(g_{k-1})+\Delta_\theta(g_k) & \theta(g_k) & \cdots & 0 \\ 0 & 0 & g_0 & \cdots & g_{k-3} & g_{k-2} & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots & & & \vdots \\ 0 & 0 & \cdots & g_0 & g_{k-2} & \cdots & g_{k-1} & g_k \end{pmatrix},$$

and if $n-k$ is even, then

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

4. Dual of Δ_θ-cyclic codes over R

In this section, we investigate the structure of the dual of a free Δ_θ-cyclic code over R with even length.

Definition 5. Let $C \subseteq R^n$ is a Δ_θ-cyclic code. Dual of C, denoted by $C^\perp$, is defined by

$$C^\perp = \{\mathbf{x} \in R^n : \ \mathbf{x} \cdot \mathbf{y} = 0, \text{ for all } \mathbf{y} \in C\}.$$

Here, $\mathbf{x} \cdot \mathbf{y} = x_0y_0 + x_1y_1 + \cdots + x_{n-1}y_{n-1}$ denotes the usual inner product in R^n.

It is easy to check that $C^\perp$ is a linear code over R. Moreover, for any even n, if C is a free Δ_θ-cyclic code principally generated by a polynomial whose leading coefficient is a unit, then $C^\perp$ is free, as we show below.

Lemma 10. *Let n be an even integer. Let $g(x), h(x) \in R[x;\theta,\Delta_\theta]$, where the leading coefficient of $g(x)$ is a unit, and $h(x)g(x) = x^n - 1$. Then we have*

$$h(x)g(x) = g(x)h(x).$$

Proof. If n is even, then $x^n - 1 = h(x)g(x)$ is a central element (by Theorem 2). Then we have

$$h(x)h(x)g(x) = h(x)g(x)h(x).$$

Since $h(x)$ is not a zero divisor, $x^n - 1 = h(x)g(x) = g(x)h(x)$. □

Lemma 11. *Let C be a Δ_θ-cyclic code, where $C = \langle g(x)\rangle$, for some right divisor $g(x)$ of $x^n - 1$, whose leading coefficient is a unit and n is even. Let $x^n - 1 = h(x)g(x)$. Then $c(x) \in R_{n,\Delta_\theta}$ is contained in C if and only if $c(x)h(x) = 0$ (in R_{n,Δ_θ}).*

Proof. ($\Longrightarrow$) Since $c(x) \in C$, there exists $a(x) \in R[x;\theta,\Delta_\theta]$ such that $c(x) = a(x)g(x)$. Hence,

$$c(x)h(x) = a(x)g(x)h(x) = a(x)h(x)g(x) = a(x)(x^n - 1) = 0 \text{ (in } R_{n,\Delta_\theta}).$$

($\Longleftarrow$) Since $c(x)h(x) = 0$ (in R_{n,Δ_θ}) for some $c(x) \in R_{n,\Delta_\theta}$, we have $c(x)h(x) = q(x)(x^n - 1)$ for some $q(x) \in R[x;\theta,\Delta_\theta]$. In this case

$$c(x)h(x) = q(x)(x^n - 1) = q(x)h(x)g(x) = q(x)g(x)h(x).$$

Since $h(x)$ is not a zero divisor, we have $c(x) = q(x)g(x) \in \langle g(x)\rangle = C$.

□

We also have known that all unit in R are $\{1, 3, 1+2v, 3+2v\}$. It is easy to check that for all units a in R, we have $\theta(a)'$s are also units in R. Hence, we have the following.

Lemma 12. *If $a \in R$ is a unit, then $\theta(a) \in R$ is also a unit.*

Now, consider a Δ_θ-cyclic code C of even length n. Let $C = \langle g(x)\rangle$, where $g(x)$ is a right divisor of $x^n - 1$ and its leading coefficient is a unit. Then there exists $h(x) = h_0 + h_1x + \cdots + h_kx^k \in R_{n,\Delta_\theta}$ such that $x^n - 1 = h(x)g(x)$. For $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1} \in C$, by Lemma 11, we have $c(x)h(x) = 0$ (in R_{n,Δ_θ}). By considering the coefficients of $x^k, x^{k+1}, \ldots, x^{n-1}$ in the last equation, we obtain two systems of equations each consisting of $n-k$ linear equations in $c_0, c_1, \ldots, c_{n-1}$. To be more precise, we have the following two systems of equations, for k is odd and even, respectively.

$$\begin{cases} c_ih_k + c_{i+1}(\theta(h_{k-1}) + \Delta_\theta(h_k)) + c_{i+2}h_{k-2} + \cdots + c_{k+i}(\theta(h_0) + \Delta_\theta(h_1)) = 0, & \text{if } i \text{ is even,} \\ c_i\theta(h_k) + c_{i+1}h_{k-1} + c_{i+2}(\theta(h_{k-2}) + \Delta_\theta(h_{k-1})) + \cdots + c_{k+i}h_0 + c_{k+i+1}\Delta_\theta(h_0) = 0, & \text{if } i \text{ is odd.} \end{cases}$$

$$\begin{cases} c_ih_k + c_{i+1}(\theta(h_{k-1}) + \Delta_\theta(h_k)) + c_{i+2}h_{k-2} + \cdots + c_{k+i}h_0 + c_{k+i+1}\Delta_\theta(h_0) = 0, & \text{if } i \text{ is even,} \\ c_i\theta(h_k) + c_{i+1}h_{k-1} + c_{i+2}(\theta(h_{k-2}) + \Delta_\theta(h_{k-1})) + \cdots + c_{k+i}(\theta(h_0) + \Delta_\theta(h_1)) = 0, & \text{if } i \text{ is odd,} \end{cases}$$

If we write the system of equations in a matrix form, we obtain $H\mathbf{c}^T = 0$, for the matrix H of dimension $(n-k) \times n$. It implies that $GH^T = 0$, for a generator matrix G of C. Moreover, it is easy to check that H is of the row echelon form with diagonal elements h_k or $\theta(h_k)$, and having a submatrix of dimension $(n-k)\times(n-k)$. Since h_k is a unit, by Lemma 12, we have $\theta(h_k)$ is also a unit. Then the rows of H are linearly independent. Hence, |Row space of H| $= |R|^{n-k} = |C^\perp|$. Thus, H is a parity check matrix of C and we have proven the following theorem.

Theorem 3. *Let C be a Δ_θ-cyclic code of even length n, where $C = \langle g(x)\rangle$, for some right divisor $g(x)$ of $x^n - 1$, whose leading coefficient is a unit and $x^n - 1 = h(x)g(x)$, for some $h(x) = h_0 + h_1x + h_2x^2 + \cdots + h_kx^k \in R_{n,\Delta_\theta}$. Then the $(n-k)\times n$ parity-check matrix H for C is given by*

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

for an odd k, and

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

for an even k.

5. New linear codes over $\mathbb{Z}_4$

In this section, we obtained many linear codes over $\mathbb{Z}_4$ with new parameters from the Gray image, residue code, and torsion code of skew-linear and skew-cyclic codes with derivation over R. First, we construct linear codes over $\mathbb{Z}_4$ from principally generated free Δ_θ-cyclic codes over R in Corollary 3. The linear codes over $\mathbb{Z}_4$, some of them are with new parameters, are listed in the table below.

C	$\Phi(C)$	$Res(C)$	$Tor(C)$	C^{PS}
	$[n, 4^{k_1}2^{k_2}, d_L]$	$[n, 4^{k_1}2^{k_2}, d_L]$	$[n, 4^{k_1}2^{k_2}, d_L]$	$[n, 4^{k_1}2^{k_2}, d_L]$
$\langle 3+x \rangle$	$[8, 4^6 2^0, 2]^{*)}$	$[4, 4^3 2^0, 2]^{*)}$	$[4, 4^3 2^0, 2]^{*)}$	$[8, 4^6 2^0, 2]^{*)}$
$\langle (3+2v)+(3+2v)x+2x^2 +(1+2v)x^3+(3+2v)x^4 \rangle$			$[6, 4^2 2^0, 6]^{*)}$	
$\langle 3v+(3+v)x+(3+v)x^2+(1+ 2v)x^3+(2+2v)x^4+2x^5+vx^6+ (1+3v)x^7+(1+v)x^8+x^9 \rangle$		$[12, 4^3 2^0, 10]^{*)}$		
$\langle (1+3v)+3x+x^2+(3+2v)x^4 +2x^5+2vx^6+2x^7+(1+3v)x^8 +3x^9+3x^{10}+x^{12} \rangle$		$[16, 4^4 2^0, 12]^{**}$		

Table 1: Free linear codes over $\mathbb{Z}_4$

Notes for Table 1, Table 2, Example 1, and Example 2:

- * means that the code has new k_1 and k_2, but there is/are other codes of equal length in the database [2] with the same minimum Lee distance but with greater cardinalities.
- ** means that the code has minimum Lee distance greater than all existing linear codes of equal length with the same values of k_1 and k_2 in the database [2].
- *** means that the code has new k_1 and k_2, with greater or equal cardinalities compared with all existing linear codes of equal length with the same value of minimum Lee distance in the database [2].
- $^{*)}$ means that the code has the same parameters as some existing good linear codes of equal length in the database [2].

- C^{PS} is the code obtained by Plotkin-sum construction, namely $C^{PS} := \{(\mathbf{x} \mid \mathbf{x}+\mathbf{y}) : \mathbf{x}, \mathbf{y} \in Res(C)\}$ or $C^{PS} := \{(\mathbf{x} \mid \mathbf{x}+\mathbf{y}) : \mathbf{x}, \mathbf{y} \in Tor(C)\}$.

In the Table 1 above, notice that all linear codes over $\mathbb{Z}_4$ constructed by this method are free. This is not a coincidence. In fact, this is a direct consequence of Theorem 1, as follows.

Corollary 4. *Let C be a free Δ_θ-cyclic code of length n over R with $|C| = 16^k$. Then the free linear codes $Res(C)$ and $Tor(C)$ have parameter $4^k 2^0$, and the free linear code $\Phi(C)$ has parameter $4^{2k}2^0$.*

Remark 2. The part of Corollary 4 related to the parameters of $Res(C)$ and $Tor(C)$ does not hold for linear codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$, with $u^2 = 1$ considered by Sharma and Bhaintwal [22] (e.g., see Example 7 in [22]).

5.1. Notes on a computational simplification

From Corollary 4, we conclude that we need non-free linear codes over R to obtain non-free Gray images, residue codes, and torsion codes. Here, we use a slightly modified construction from principally generated Δ_θ-cyclic codes. Notice that for any $g(x) \in R_{n,\Delta_\theta}$, the set $\{g(x), xg(x), \ldots, x^{n-1}g(x)\}$ is a generating set, which is not necessary minimal, of the (not necessarily free) Δ_θ-cyclic code $C = \langle g(x)\rangle$ over R. We consider the subcode $C_k = \langle g(x), xg(x), \ldots, x^{k-1}g(x)\rangle$ of C for some $k \le n$. From there, we can obtain $Res(C_k), Tor(C_k)$, and $\Phi(C_k)$. For the case of Δ_θ-cyclic codes over R, we can simplify our computation as follows.
Let C be a Δ_θ-cyclic code over R of length n generated by $\{g(x), xg(x), \ldots, x^{n-1}g(x)\}$, where $g(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{n-1}x^{n-1} \in R_{n,\Delta_\theta}$ and $c_i = a_i + b_iv$, for $0 \le i \le n-1$. To be more precise, for an even and an odd n, the generator of $C \subseteq R^n$ consists of the following vectors, respectively:

$$
\begin{aligned}
g_1 &= (a_0 + b_0v,\ a_1 + b_1v,\ \ldots,\ a_{n-2} + b_{n-2}v,\ a_{n-1} + b_{n-1}v),\\
g_2 &= (a_{n-1} + b_{n-1} + b_0 - b_{n-1}v,\ a_0 + b_0 + b_1 - b_0v,\ \ldots,\ a_{n-3} + b_{n-3} + b_{n-2} - b_{n-3}v,\\
&\quad\ a_{n-2} + b_{n-2} + b_{n-1} - b_{n-2}v),\\
g_3 &= (a_{n-2} + b_{n-2}v,\ a_{n-1} + b_{n-1}v,\ \ldots,\ a_{n-4} + b_{n-4}v,\ a_{n-3} + b_{n-3}v),\\
&\ \ \vdots\\
g_n &= (a_1 + b_1 + b_2 - b_1v,\ a_2 + b_2 + b_3 - b_2v,\ \ldots,\ a_{n-1} + b_{n-1} + b_0 - b_{n-1}v,\\
&\quad\ a_0 + b_0 + b_1 - b_0v),
\end{aligned}
$$

and

$$
\begin{aligned}
g_1 &= (a_0 + b_0v,\ a_1 + b_1v,\ \ldots,\ a_{n-2} + b_{n-2}v,\ a_{n-1} + b_{n-1}v),\\
g_2 &= (a_{n-1} + b_{n-1} + b_0 - b_{n-1}v,\ a_0 + b_0 + b_1 - b_0v,\ \ldots,\ a_{n-3} + b_{n-3} + b_{n-2} - b_{n-3}v,\\
&\quad\ a_{n-2} + b_{n-2} + b_{n-1} - b_{n-2}v),\\
g_3 &= (a_{n-2} + b_{n-2}v,\ a_{n-1} + b_{n-1}v,\ \ldots,\ a_{n-4} + b_{n-4}v,\ a_{n-3} + b_{n-3}v),\\
&\ \ \vdots\\
g_n &= (a_1 + b_1v,\ a_2 + b_2v,\ \ldots,\ a_{n-1} + b_{n-1}v,\ a_0 + b_0v).
\end{aligned}
$$

By applying the Lemma 1, we obtain the generator of $Res(C)$ for an even and an odd n that consists of the following vectors, respectively:

$$\begin{aligned}
Res(g_1) &= (a_0,\ a_1,\ a_2,\ \ldots,\ a_{n-2},\ a_{n-1}),\\
Res(g_2) &= (a_{n-1}+b_{n-1}+b_0,\ a_0+b_0+b_1,\ \ldots,\ a_{n-3}+b_{n-3}+b_{n-2},\ a_{n-2}+b_{n-2}+b_{n-1}),\\
Res(g_3) &= (a_{n-2},\ a_{n-1},\ \ldots,\ a_{n-4},\ a_{n-3}),\\
&\vdots\\
Res(g_n) &= (a_1+b_1+b_2,\ a_2+b_2+b_3,\ \ldots,\ a_{n-1}+b_{n-1}+b_0,\ a_0+b_0+b_1),
\end{aligned}$$

and

$$\begin{aligned}
Res(g_1) &= (a_0,\ a_1,\ a_2,\ \ldots,\ a_{n-2},\ a_{n-1}),\\
Res(g_2) &= (a_{n-1}+b_{n-1}+b_0,\ a_0+b_0+b_1,\ \ldots,\ a_{n-3}+b_{n-3}+b_{n-2},\ a_{n-2}+b_{n-2}+b_{n-1}),\\
Res(g_3) &= (a_{n-2},\ a_{n-1},\ \ldots,\ a_{n-4},\ a_{n-3}),\\
&\vdots\\
Res(g_n) &= (a_1,\ a_2,\ \ldots,\ a_{n-1},\ a_0).
\end{aligned}$$

Moreover, we obtain the generator of $Tor(C)$ for an even and an odd n that consists of the following vectors, respectively:

$$\begin{aligned}
Tor(g_1) &= (a_0+b_0,\ a_1+b_1,\ a_2+b_2,\ \ldots,\ a_{n-2}+b_{n-2},\ a_{n-1}+b_{n-1}),\\
Tor(g_2) &= (a_{n-1}+b_0,\ a_0+b_1,\ \ldots,\ a_{n-3}+b_{n-2},\ a_{n-2}+b_{n-1}),\\
Tor(g_3) &= (a_{n-2}+b_{n-2},\ a_{n-1}+b_{n-1},\ \ldots,\ a_{n-4}+b_{n-4},\ a_{n-3}+b_{n-3}),\\
&\vdots\\
Tor(g_n) &= (a_1+b_2,\ a_2+b_3,\ \ldots,\ a_{n-1}+b_0,\ a_0+b_1),
\end{aligned}$$

and

$$\begin{aligned}
Tor(g_1) &= (a_0+b_0,\ a_1+b_1,\ a_2+b_2,\ \ldots,\ a_{n-2}+b_{n-2},\ a_{n-1}+b_{n-1}),\\
Tor(g_2) &= (a_{n-1}+b_0,\ a_0+b_1,\ \ldots,\ a_{n-3}+b_{n-2},\ a_{n-2}+b_{n-1}),\\
Tor(g_3) &= (a_{n-2}+b_{n-2},\ a_{n-1}+b_{n-1},\ \ldots,\ a_{n-4}+b_{n-4},\ a_{n-3}+b_{n-3}),\\
&\vdots\\
Tor(g_n) &= (a_1+b_1,\ a_2+b_2,\ \ldots,\ a_{n-1}+b_{n-1},\ a_0+b_0).
\end{aligned}$$

For any $k \leq n$, if C_k is generated by the set $\{g_1, g_2, \ldots, g_k\}$, then the $Res(C_k)$ and $Tor(C_k)$ is generated by $\{Res(g_1), Res(g_2), \ldots, Res(g_k)\}$ and $\{Tor(g_1), Tor(g_2), \ldots, Tor(g_k)\}$, respectively. This method can reduce the computation time significantly. Using this method, we can obtain some linear codes over $\mathbb{Z}_4$ with good parameters, as listed in the table below.

Generators of C	$Res(C)$	$Tor(C)$	C^{PS}
	$[n, 4^{k_1}2^{k_2}, d_L]$	$[n, 4^{k_1}2^{k_2}, d_L]$	$[n, 4^{k_1}2^{k_2}, d_L]$
$\{g_1(x), xg_1(x)\}$	$[4, 4^1 2^1, 4]^*$		$[8, 4^2 2^2, 4]$
$\{g_2(x), xg_2(x), x^2g_2(x)\}$	$[4, 4^1 2^2, 2]$		$[8, 4^2 2^4, 2]^*$
$\{g_3(x), xg_3(x), x^2g_3(x)\}$	$[5, 4^2 2^1, 4]^{***}$		
$\{g_4(x), xg_4(x), x^2g_4(x)\}$	$[6, 4^2 2^1, 4]^*$		
$\{g_5(x), xg_5(x), x^2g_5(x), x^3g_5(x), x^4g_5(x)\}$	$[6, 4^2 2^3, 4]^{*)}$		$[12, 4^4 2^6, 4]^*$
$\{g_6(x), xg_6(x), x^2g_6(x), x^3g_6(x)\}$	$[6, 4^3 2^1, 4]^*$		$[12, 4^6 2^2, 4]^*$
$\{g_7(x), xg_7(x), x^2g_7(x), x^3g_7(x), x^4g_7(x), x^5g_7(x), x^6g_7(x)\}$	$[8, 4^4 2^3, 4]^{*)}$		$[16, 4^8 2^6, 4]$
$\{g_8(x), xg_8(x), x^2g_8(x), x^3g_8(x), x^4g_8(x), x^5g_8(x)\}$		$[8, 4^5 2^1, 4]^{***}$	$[16, 4^{10} 2^2, 4]^*$
$\{g_9(x), xg_9(x), x^2g_9(x)\}$	$[9, 4^3 2^0, 7]^{*)}$		
$\{g_{10}(x), xg_{10}(x), x^2g_{10}(x)\}$	$[10, 4^3 2^0, 8]^{*)}$		
$\{g_{11}(x), xg_{11}(x)\}$	$[15, 4^2 2^0, 15]$		
$\{g_{12}(x), xg_{12}(x), x^2g_{12}(x)\}$		$[18, 4^3 2^0, 14]$	

Table 2: Linear codes over $\mathbb{Z}_4$

In Table 2,

- $g_1(x) = (1+3v) + 2x + (3+3v)x^2$.
- $g_2(x) = (1+v) + (2+2v)x + (1+3v)x^2$.
- $g_3(x) = (1+3v) + 2vx + (2+2v)x^2 + 2vx^3 + (1+3v)x^4$.
- $g_4(x) = 3 + (1+3v)x + (3+v)x^2 + (2+3v)x^3$.
- $g_5(x) = (3+3v) + (1+3v)x + (3+3v)x^3 + (3+v)x^4 + 2x^5$.
- $g_6(x) = (1+v) + x + (2+v)x^2 + vx^3 + 3vx^5$.
- $g_7(x) = (1+v) + 3x + (2+3v)x^2 + (3+v)x^3 + (2+2v)x^4 + 2x^6 + x^7$.
- $g_8(x) = 2v + (2+3v)x + (1+3v)x^2 + (1+2v)x^3 + 2vx^4 + (1+v)x^5 + x^6 + 3vx^7$.
- $g_9(x) = (1+v) + (1+3v)x + (3+2v)x^2 + 3x^3 + (3+3v)x^4 + (2+2v)x^5 + (2+3v)x^6 + (3+3v)x^7 + (1+3v)x^8$.
- $g_{10}(x) = (1+3v) + (2+2v)x + 3x^2 + vx^4 + 3x^5 + (3+3v)x^6 + x^7 + x^8$.
- $g_{11}(x) = (1+v) + (2+v)x^2 + (3+2v)x^3 + (3+v)x^5 + (1+2v)x^6 + 2x^7 + (3+v)x^8 + 3x^9 + 2vx^{10} + (3+2v)x^{11} + (1+2v)x^{12} + (2+v)x^{13} + (1+3v)x^{14}$.
- $g_{12}(x) = 1 + 2vx + (3+2v)x^2 + (2+2v)x^3 + (1+2v)x^4 + x^5 + vx^6 + x^7 + (1+2v)x^8 + (3+2v)x^9 + (1+3v)x^{10} + (3+3v)x^{11} + (2+v)x^{12} + (3+3v)x^{13} + x^{14} + (2+v)x^{15} + (2+2v)x^{16}$.

Exactly the same method can also be used for $\Phi(C_k)$. This observation brings us to the conclusion that the codes $Res(C_k)$, $Tor(C_k)$, and $\Phi(C_k)$ have at most 4^k, 4^k, and 4^{2k} codewords, respectively. Moreover, the similar observation can also be applied to the codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$, with $u^2 = 1$, investigated by Sharma and Bhaintwal [22] and it is easy to verify that in this case, the codes $Res(C_k)$, $Tor(C_k)$, and $\Phi(C_k)$ have at most 4^{2k} codewords.

5.2. Construction from another method

By applying the construction in [23], we can obtain even more new linear codes over $\mathbb{Z}_4$ with the highest known minimum Lee distance, previously unknown to exist in the database [2]. As illustrations, we provide several examples below. In the following examples, the code C_i refers to the code generated by the polynomial $g_i(x)$ in Table 2.

Example 1. In these examples, we use Lemma 4.6 in [23] to construct new linear codes over $\mathbb{Z}_4$.

- From the code with parameters $[6, 4^2 2^0, 6]$ in Table 1, we obtained linear codes with parameters $[12, 4^2 2^1, 12]^{*)}$, $[24, 4^3 2^0, 24]^{*)}$, $[24, 4^2 2^2, 24]^{*)}$, $[48, 4^3 2^1, 48]^{***}$, and $[48, 4^2 2^3, 48]^{*)}$.
- From the code with parameters $[12, 4^3 2^0, 10]$ in Table 1, we obtained linear codes with parameters $[24, 4^3 2^1, 20]$, $[48, 4^4 2^0, 40]$, and $[48, 4^3 2^2, 40]^{***}$.
- From the code C_3 with parameters $[5, 4^2 2^1, 4]$ we obtained linear codes with parameters $[10, 4^2 2^2, 8]^{***}$, $[20, 4^3 2^1, 16]$, $[20, 4^2 2^3, 16]^{*}$, $[40, 4^3 2^2, 32]^{*}$, and $[40, 4^2 2^4, 32]$.
- From the code C_5 with parameters $[6, 4^2 2^3, 4]$ we obtained a linear code with parameters $[12, 4^2 2^4, 8]^{**}$.
- From the code C_6 with parameters $[6, 4^3 2^1, 4]$ we obtained a linear code with parameters $[12, 4^3 2^2, 8]^{*}$.
- From the code C_9 with parameters $[9, 4^3 2^0, 7]$ we obtained linear codes with parameters $[18, 4^3 2^1, 14]^{**}$, $[36, 4^4 2^0, 28]^{**}$, and $[36, 4^3 2^2, 28]^{**}$.
- From the code C_{10} with parameters $[10, 4^3 2^0, 8]$ we obtained a linear code with parameters $[40, 4^4 2^0, 32]$.

Example 2. In these examples, we use Lemma 4.3 in [23] to construct new linear codes over $\mathbb{Z}_4$.

- From the code with parameters $[12, 4^3 2^0, 10]$ in Table 1 and the code with parameters $[24, 4^3 2^0, 24]$, respectively, we obtained a linear code with parameters $[36, 4^3 2^0, 34]^{*)}$.
- From the code C_3 with parameters $[5, 4^2 2^1, 4]$ and the code with parameters $[12, 4^2 2^1, 12]$ we obtained a linear code with parameters $[17, 4^2 2^1, 16]^{*}$.
- From the code C_6 with parameters $[6, 4^3 2^1, 4]$ and the code with parameters $[20, 4^3 2^1, 16]$ we obtained a linear code with parameters $[26, 4^3 2^1, 20]^{*}$.

6. Concluding remarks

We have investigated the algebraic structures of skew-cyclic codes, also known as θ-cyclic codes, with a derivation Δ_θ over the ring $R = \mathbb{Z}_4 + v\mathbb{Z}_4$, with $v^2 = v$, extending the observation of Boucher and Ulmer [9], where they defined and

considered the skew-cyclic codes with derivation over a finite field. To our best knowledge, this is the third attempt after the paper by Sharma and Bhaintwal [22] and Patel and Prakash [20]. As a consequence, we constructed several new codes over $\mathbb{Z}_4$ unknown to exist before due to the database [2], with good parameters. All computations to find the codes were done by Python and Magma computational algebra system [5]. Regarding the derivation, it is easy to show that the map $\Delta_\theta(x) = (3+2v)(\theta(x)-x)$ also defines a derivation on R. All properties which hold for the derivation $\Delta_\theta(x) = (1+2v)(\theta(x)-x)$ in this paper also hold for the derivation $\Delta_\theta(x) = (3+2v)(\theta(x)-x)$. The method explained in Section 5 can be modified for the case of derivation $\Delta_\theta(x) = (3+2v)(\theta(x)-x)$. There is some hope to obtain many more examples of linear codes over $\mathbb{Z}_4$ with better parameters. As an example, $Tor(C)$ of the code $C := \langle g(x), xg(x), x^2g(x)\rangle$, with $g(x) = 3v+(2+v)x+3vx^2+vx^3$, has parameters $[4, 4^1 2^2, 4]$, which is better than the one in Table 1.

Acknowledgements: This research is supported by the Institut Teknologi Bandung (ITB) and the Ministry of Education, Culture, Research and Technology (*Kementerian Pendidikan, Kebudayaan, Riset dan Teknologi (Kemdikbudristek)*), Republic of Indonesia.

Conflict of Interest: The author declares no conflict of interest.

Data Availability: Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

References

[1] T. Abualrub, N. Aydin, and P. Seneviratne, *On θ-cyclic codes over* $\mathbb{F}_2 + v\mathbb{F}_2$, Australas. J. Combin **54** (2012), no. 2, 115–126.

[2] N. Aydin and T. Asamov, *The database of* $\mathbb{Z}_4$ *codes*, available at http://quantumcodes.info/Z4 (accessed at January 5, 2024).

[3] R.K. Bandi and M. Bhaintwal, *Codes over* $\mathbb{Z}_4 + v\mathbb{Z}_4$, 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2014, pp. 422–427. https://doi.org/10.1109/ICACCI.2014.6968489.

[4] N. Benbelkacem, M.F. Ezerman, T. Abualrub, N. Aydin, and A. Batoul, *Skew cyclic codes over* $\mathbb{F}_4 R$, J. Algebra Appl. **21** (2022), no. 4, Article ID: 2250065. https://doi.org/10.1142/S0219498822500657.

[5] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system I: The user language*, J. Symb. Comput. **24** (1997), no. 3-4, 235–265. https://doi.org/10.1006/jsco.1996.0125.

[6] D. Boucher, W. Geiselmann, and F. Ulmer, *Skew-cyclic codes*, Appl. Algebra

Engrg. Comm. Comput. **18** (2007), no. 4, 379–389.
https://doi.org/10.1007/s00200-007-0043-z.

[7] D. Boucher and F. Ulmer, *Codes as modules over skew polynomial rings*, Cryptography and Coding: 12th IMA International Conference, Cryptography and Coding 2009, Cirencester, UK, December 15-17, 2009. Proceedings 12 (M.G. Parker, ed.), Springer, 2009, pp. 38–55.

[8] ———, *Coding with skew polynomial rings*, J. Symb. Comput. **44** (2009), no. 12, 1644–1656.
https://doi.org/10.1016/j.jsc.2007.11.008.

[9] ———, *Linear codes using skew polynomials with automorphisms and derivations*, Des. Codes, Cryptogr. **70** (2014), no. 3, 405–431.
https://doi.org/10.1007/s10623-012-9704-4.

[10] A.R. Calderbank, A.R. Hammons Jr, P.V. Kumar, N.J.A. Sloane, and P. Solé, *The $\mathbb{Z}_4$-linearity of kerdock, preparata, goethals and related codes*, IEEE Trans. Inf. Theory **40** (1994), no. 2, 301–319.

[11] J. Gao, F.W. Fu, and Y. Gao, *Some classes of linear codes over $\mathbb{Z}_4 + v\mathbb{Z}_4$ and their applications to construct good and new $\mathbb{Z}_4$ linear codes*, Appl. Algebra Engrg. Comm. Comput. **28** (2016), no. 2, 131–153.
https://doi.org/10.1007/s00200-016-0300-0.

[12] F. Gursoy, I. Siap, and B. Yildiz, *Construction of skew cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q$*, Adva. Math. Commun. **8** (2014), no. 3, 313–322.
https://doi.org/10.3934/amc.2014.8.313.

[13] W.C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge university press, New York, 2003.

[14] A. B. Irwansyah and D. Suprijanto, *Structure of linear codes over the ring B_k*, J. Appl. Math. Comput. **58** (2018), no. 1–2, 755–775.
https://doi.org/10.1007/s12190-018-1165-0.

[15] A.B. Irwansyah, S.T. Dougherty, A. Muchlis, I. Muchtadi-Alamsyah, P. Solé, D. Suprijanto, and O. Yemen, *θ_s-cyclic codes over A_k*, Int. J. Comput. Math. Comput. Syst. Theory **1** (2016), no. 1, 14–31.

[16] A.B. Irwansyah, I. Muchtadi-Alamsyah, A. Muchlis, and D. Suprijanto, *Skew-cyclic codes over B_k*, J. Appl. Math. Comput. **57** (2018), no. 1-2, 69–84.
https://doi.org/10.1007/s12190-017-1095-2.

[17] J. Liu and H. Liu, *Construction of cyclic DNA codes over the ring $\mathbb{Z}_4 + v\mathbb{Z}_4$*, IEEE Access **8** (2020), 111200–111207.
https://doi.org/10.1109/ACCESS.2020.3001283.

[18] B.R. McDonald, *Finite Rings with Identity*, Marcel Dekker Inc., New York, 1974.

[19] O. Ore, *Theory of non-commutative polynomials*, Annals. Math. **34** (1933), no. 3, 480–508.
https://doi.org/10.2307/1968173.

[20] S. Patel and O. Prakash, *(θ, δ_θ)-cyclic codes over $\mathbb{F}_q[u,v]/\langle u^2 - u, v^2 - vuv - vu\rangle$*, Des. Codes Cryptogr. **90** (2021), no. 11, 2763–2781.
https://doi.org/10.1007/s10623-021-00964-7.

[21] E. Prange, *Cyclic Error-correcting Codes in Two Symbols*, AFCRC-TN, Air Force

Cambridge Research Center, 1957.

[22] A. Sharma and M. Bhaintwal, *A class of skew-cyclic codes over* $\mathbb{Z}_4 + u\mathbb{Z}_4$ *with derivation*, Adv. Math. Commun. **12**, no. 4, 723–739. https://doi.org/10.3934/amc.2018043.

[23] H.C. Tang and D. Suprijanto, *New optimal linear codes over* $\mathbb{Z}_4$, Bull. Aust. Math. Soc. **107** (2023), no. 1, 158–169. https://doi.org/10.1017/S0004972722000399.

[24] Z.X. Wan, *Quaternary Codes*, vol. 8, World Scientific, Singapore, 1997.