

Cyclic codes over non-Frobenius ring $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$

Zahra Goodarzi^{1,†}, Mohammad Reza Alimoradi^{1,*}, Nuh Aydin²

¹ Faculty of Mathematical Sciences and Statistics, Malayer University, Malayer, Iran

[†]goodarzi.zahra61@yahoo.com

^{*}m.alimoradi@malayeru.ac.ir

² Department of Mathematics and Statistics, Kenyon College, 43022 Gambier, OH, USA

aydinn@kenyon.edu

Received: 13 May 2025; Accepted: 22 August 2026

Published Online: 7 September 2026

Abstract: In this study, cyclic codes of odd length over the ring $R = \mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$ are investigated. The structure of cyclic codes over this ring is characterized using the work Samie and Alimoradi (Comp. Appl. Math. 2018). The ranks and duals of such codes are determined. It is also shown that the equality $|C||C^\perp| = |R|^n$ holds for a cyclic code C of length n over this ring if and only if C is a cyclic code over the Frobenius subring $\mathbb{Z}_4 + u\mathbb{Z}_4$ of the non-Frobenius ring R . Moreover, we correct a false claim about this ring that appeared in the literature. Finally, several new linear codes over $\mathbb{Z}_4$ are obtained from cyclic codes over R via a Gray map.

Keywords: cyclic code, self-dual code, Frobenius ring, Gray map.

AMS Subject Classification: 94B05, 94B15

1. Introduction

Cyclic codes over finite rings have recently attracted considerable attention in algebraic coding theory. Extensive research has been conducted on codes over $\mathbb{Z}_4$ after the seminal paper by Hammons et al. [11]. Due to the importance of codes over $\mathbb{Z}_4$ in coding theory, a database of $\mathbb{Z}_4$ -codes has been created [5] (The original version was introduced in [6]). Linear and cyclic codes, MacWilliams identities, projections and formally self-dual codes over the ring $\mathbb{Z}_4 + u\mathbb{Z}_4$, which is a non-chain extension of $\mathbb{Z}_4$, were studied by Yildiz and Karadeniz in [19]. Finite Frobenius rings are significant in coding theory because two classical theorems of MacWilliams, the extension theorem

* Corresponding Author

and the MacWilliams identities, hold for codes over these rings. Moreover, for a code C of length n over a finite Frobenius ring R and its dual, the following equations are valid [18]

$$|C||C^\perp| = |R|^n, (C^\perp)^\perp = C,$$

where the Euclidean dual code $C^\perp$ of C is defined as $C^\perp = \{x \in R^n \mid \langle x, c \rangle = 0 : \forall c \in C\}$. Although Wood showed that for certain reasons finite Frobenius rings are the most general class of rings that should be used for alphabets of codes [18], Samie and Alimoradi studied the structure of cyclic codes over smallest non-Frobenius ring $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2$ with $u^2 = v^2 = uv = vu = 0$ in [16]. They also obtained some optimal binary codes as the images of cyclic codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2$ under a Gray map, which maps Lee weights to Hamming weights. In other words, contrary to Wood's claim, they showed that the study of cyclic codes over non-Frobenius rings has led to interesting results. Recently, Choi et al. studied the structure of cyclic codes over the non-Frobenius ring $\mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p$, where p is a prime number and $u^2 = v^2 = uv = vu = 0$ in [7]. They found a series of examples and tables concerning the mass formula of cyclic self-orthogonal codes, cyclic LCD (Linear complementary dual) codes and several new quasi-cyclic codes. Later, Çalışkan et al. investigated skew cyclic codes over non-Frobenius ring $R = \mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$, where $u^2 = v^2 = uv = vu = 0$ in [6]. In [13], Islam et al. claimed that the ring $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$ with $u^2 = v^2 = uv = vu = 0$ is a Frobenius ring. In this paper, we show that this claim is not valid (Theorem 1). In [15], Özen et al. studied cyclic codes over the ring $\mathbb{Z}_4 + u\mathbb{Z}_4 + u^2\mathbb{Z}_4$, where $u^3 = 0$ and obtained many new linear codes over $\mathbb{Z}_4$ by considering Gray images of cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4 + u^2\mathbb{Z}_4$. After that Shi et al. studied $(1 + 2u)$ -constacyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$, where $u^2 = 1$ in [17]. Also, they found many examples of $(1 + 2u)$ -constacyclic codes over $\mathbb{Z}_4[u]/\langle u^2 - 1 \rangle$, whose $\mathbb{Z}_4$ images are $\mathbb{Z}_4$ -cyclic codes with improved parameters according to the online database [1]. Finding new linear codes over $\mathbb{Z}_4$ is the motivation to study cyclic codes over non-Frobenius ring $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$, which is an extension of the Frobenius ring $\mathbb{Z}_4 + u\mathbb{Z}_4$, where $u^2 = 0$. In particular, we show that for a cyclic code C of length n over R and its dual code, the equation $|C||C^\perp| = |R|^n$ is valid if and only if C is a cyclic code over the Frobenius subring $\mathbb{Z}_4 + u\mathbb{Z}_4$ of R .

The paper is organized as follows. First, some notations and results about the structure of ring R are given in Section 2. Also, properties of cyclic codes of odd length over R are studied. In particular, generators of the ideals corresponding to cyclic codes over R of odd length n are characterized. Theorem 2 is the main result of Section 2, which shows that for an odd integer n , any non-principal ideal of quotient ring $R_n = R[x]/\langle x^n - 1 \rangle$ can be generated by two elements. The rank and minimal spanning sets of cyclic codes over this ring are studied in Section 3. Additionally, the structure of the dual a cyclic code with odd length over the ring R is determined. In Section 4, two Gray-like maps are defined in order to obtain codes over $\mathbb{Z}_4$ from codes over R . It is also shown that the Gray image of a cyclic code of length n over $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$ under one of these maps is a quasi-cyclic code of index 6 and length $6n$ over $\mathbb{Z}_4$. In Section 5, used computer search, some new linear codes over $\mathbb{Z}_4$ from

cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$ have been obtained. Finally, Section 6 concludes with some possible directions for research on these topics.

2. Cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$ of odd length

Let R denote the ring $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$, where $u^2 = v^2 = uv = 0$ and $uv = vu$. The ring R is isomorphic to the ring $\frac{\mathbb{Z}_4[x,y]}{\langle x^2, y^2, xy \rangle}$, which is a commutative ring with identity. It has characteristic 4 and order 64. Any element α in R can be written as $\alpha = a + bu + cv$, where $a, b, c \in \mathbb{Z}_4$. It is clear that α is a unit in R if and only if a is a unit in $\mathbb{Z}_4$. The ring $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$ is a local ring with $m = \langle 2, u, v \rangle$ as its unique maximal ideal.

We divide the units of R into four subsets U_1, U_2, U_3 and U_4 calling them units of first type, second type, third type and fourth type, respectively, as follows:

$$U_1 = \{1, 3, 1 + 2u, 1 + 2v, 3 + 2u, 3 + 2v, 1 + 2u + 2v, 3 + 2u + 2v\},$$

$$U_2 = \{1 + u, 1 + 3u, 3 + u, 3 + 3u, 1 + u + 2v, 1 + 3u + 2v, 3 + u + 2v, 3 + 3u + 2v\},$$

$$U_3 = \{1 + v, 1 + 3v, 3 + v, 3 + 3v, 1 + v + 2u, 1 + 3v + 2u, 3 + v + 2u, 3 + 3v + 2u\}$$

and

$$U_4 = \{1 + u + v, 1 + u + 3v, 1 + 3u + v, 3 + u + v, 3 + u + 3v, 3 + 3u + v\}.$$

The reason for this partition is the following observation that can easily be verified:

$$\forall a \in \mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4, \quad a^2 = \begin{cases} 0 & a \in m, \\ 1 & a \in U_1, \\ 1 + 2u & a \in U_2, \\ 1 + 2v & a \in U_3, \\ 1 + 2u + 2v & a \in U_4. \end{cases} \quad (2.1)$$

A commutative ring R is called Frobenius if $\text{Soc}(R) \simeq \frac{R}{J(R)}$ as R -modules. Here, $\text{Soc}(R)$ denotes the socle of R , the sum of all minimal ideals of R , while $J(R)$, the Jacobson radical of R , is the intersection of all maximal ideals of R . In a commutative local ring, the Jacobson radical is necessarily the unique maximal ideal. We refer the reader to [10] for a characterization of Frobenius rings.

Lemma 1. [8] *Let R be a finite local ring with maximal ideal m and residue field $k = \frac{R}{m}$. Then, R is Frobenius if and only if $\dim_k \text{Ann}(m) = 1$, where $\text{Ann}(m) = \{r \in R : ra = 0, \forall a \in m\}$.*

Example 1. The ring $S = \mathbb{Z}_4 + u\mathbb{Z}_4$, where $u^2 = 0$ is a Frobenius ring. Clearly, S is a local ring with the unique maximal ideal $\langle 2, u \rangle = \{0, u, 2, 2u, 3u, 2 + u, 2 + 2u, 2 + 3u\}$. Since $\text{Ann}(m) = \{0, 2u\}$ and it has dimension 1 over its residue field then, S is a Frobenius ring.

Next, we show that the ring $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$ is not Frobenius. This disproves the claim given in [13], page 156, which is also repeated in [6].

Theorem 1. *The ring $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$ is not a Frobenius ring.*

Proof. The ring $R = \mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$ is a local ring with the unique maximal ideal $m = \langle 2, u, v \rangle$. Note that $\text{Ann}(m) = \langle 2u, 2v \rangle = \{0, 2u, 2v, 2u + 2v\}$, and $k = \frac{R}{m} \simeq \mathbb{F}_2$. Therefore, $\dim_k \text{Ann}(m) = 2$. So, by Lemma 1, R is not a Frobenius ring. $\square$

A commutative ring R is called a chain ring if its ideals form a chain under inclusion. We see that the ideals of $R = \mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$ do not form a chain. For instance, the ideals $\langle u \rangle$ and $\langle v \rangle$ are not comparable. So, the ring R is a non-chain extension of $\mathbb{Z}_4$. Throughout this paper, we use the notation R_n to denote the quotient ring $R[x]/\langle x^n - 1 \rangle$.

Theorem 2. *Let $R = \mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$. The ring R_n is not a principal ideal ring.*

Proof. The map $\gamma : R_n \rightarrow \mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$ defined as

$$\gamma(c_0 + c_1x + \cdots + c_{n-1}x^{n-1}) = c_0 + c_1 + \cdots + c_{n-1},$$

is a surjective $\mathbb{Z}_4$ -module homomorphism. Let $I = \gamma^{-1}(m)$, where $m = \langle 2, u, v \rangle$ is the unique maximal ideal of R . Clearly, I is an ideal of R_n . If I is a principal ideal and the homomorphism γ is onto, then, its homomorphic image under γ is a principal ideal. This is a contradiction because $\gamma(I) = m$ is not a principal ideal. $\square$

Lemma 2. *Let $R = \mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$. The ring R_n is a local ring, when $n = 2^k$ for $k \geq 1$.*

Proof. For $n = 2^k$, the ring $\mathbb{F}_2[x]/\langle x^n - 1 \rangle$ is a local ring with the unique maximal ideal $\langle x - 1 \rangle$, based on [3]. Let $\mu : R = \mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 \rightarrow \mathbb{F}_2$ given by $\alpha \mapsto \alpha \pmod{\langle 2, u, v \rangle}$ be the natural homomorphism mapping R to its residue field $\mathbb{F}_2$. The map μ is extended to $\bar{\mu} : R[x] \rightarrow \mathbb{F}_2[x]$. $\square$

Since the ring R_n , where $R = \mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$ is a local ring when $n = 2^k$, with $k \geq 1$. Then, any element of R_n is a unit or a zero-divisor. Note that, the ideal generated by a unit is trivial. So, in order to obtain non-trivial ideals of R_n , it is enough to consider zero-divisors of R_n .

Theorem 3. *Let $R = \mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$. The ring R_n is not a local ring, when $n = 2^k t$ and $t > 1$ is an odd number.*

Proof. Let (R, m) be a finite local ring, where m is the unique maximal ideal of R . Then, each maximal ideal of $R[x]$ is of the form $\langle R, f(x) \rangle$, where $f(x)$ is a basic irreducible polynomial (see [14] Theorem XIII.13). Since t is an odd number, $x^t - 1$ can be written uniquely as the product of distinct basic irreducible factors, i.e., $x^t - 1 = h_1(x)h_2(x) \cdots h_l(x)$, where each h_i is a basic irreducible polynomial in $R[x]$. Now, we have

$$x^n - 1 = (x^t - 1)^{2^k} = h_1(x)^{2^k} h_2(x)^{2^k} \cdots h_l(x)^{2^k}.$$

Each maximal ideal of $R_t = \frac{R[x]}{\langle x^t - 1 \rangle}$ is of the form $m_i = \langle m, p_i(x) \rangle$, where $p_i(x)$ is a basic irreducible divisor of $x^t - 1$. As the number of maximal ideals of R_n is equal to the number of maximal ideals of R_t , R_n is not a local ring. $\square$

A linear code C of length n over $R = \mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$ is an R -submodule of R^n . Since R is not a finite chain ring, we cannot define a standard generating matrix for linear codes over this ring. Let $x = (x_1, x_2, \dots, x_n)$ and $y = (y_1, y_2, \dots, y_n)$ be two vectors in R^n . The Euclidean inner product of x and y is defined as $\langle x, y \rangle = x_1y_1 + x_2y_2 + \cdots + x_ny_n$, where the operation is performed in R . The Euclidean dual code $C^\perp$ of C is defined as $C^\perp = \{x \in R^n \mid \forall c \in C, \langle x, c \rangle = 0\}$. A code C is said to be Euclidean self-orthogonal if $C \subseteq C^\perp$ and Euclidean self-dual if $C = C^\perp$.

There are three weights (metrics) commonly used for codes over $\mathbb{Z}_4$. For any $x = (x_1, x_2, \dots, x_n) \in \mathbb{Z}_4^n$, let $n_i = \#\{j : x_j = i\}$ for $i = 0, 1, 2, 3$. Then, the Hamming weight $w_H(x)$ of x is defined as $w_H(x) = n_1 + n_2 + n_3$, the Lee weight $w_L(x)$ of x is defined as $w_L(x) = n_1 + 2n_2 + n_3$, and the Euclidean weight $w_E(x)$ of x is defined as $w_E(x) = n_1 + 4n_2 + n_3$. Then, given a linear code over $\mathbb{Z}_4$, the minimum Hamming, Lee and Euclidean weights of C are defined in the usual way.

A cyclic shift on R^n is a permutation τ such that $\tau(c_0, c_1, \dots, c_{n-1}) = (c_{n-1}, c_0, c_1, \dots, c_{n-2})$. A linear code over the ring R that is invariant under the cyclic shift is called a cyclic code. Let C be a code of length n over R and $P(C)$ be its polynomial representation, i.e.,

$$P(C) = \left\{ \sum_{i=0}^{n-1} c_i x^i \mid (c_0, c_1, c_2, \dots, c_{n-1}) \in C \right\}.$$

It is well known that a linear code C of length n over R is a cyclic code if and only if $P(C)$ is an ideal of the ring R_n . So, cyclic codes over R are identified with ideals in the ring R_n . Thus, in order to understand the structure of cyclic codes over ring R , it is essential to understand the structure of the polynomial ring R_n . We now present results towards this end.

Theorem 4. Let $S = \mathbb{Z}_4 + u\mathbb{Z}_4$, where $u^2 = 0$. Let C be a cyclic code of odd length n over S and let J be the ideal of $S_n = S[x]/\langle x^n - 1 \rangle$ corresponding to C . Then,

$$J = \langle g_1(x) + 2a_1(x) + up_1(x), u(g_2(x) + 2a_2(x)) \rangle,$$

where $a_i(x) \mid g_i(x) \mid (x^n - 1) \bmod 4$, and $g_i(x) + 2a_i(x)$ is a generator of a cyclic code over $\mathbb{Z}_4$, for $i = 1, 2$.

Proof. The natural map $\bar{\varphi} : S[x]/\langle x^n - 1 \rangle \rightarrow \mathbb{Z}_4[x]/\langle x^n - 1 \rangle$ is a surjective ring homomorphism. Let J be the ideal of S_n corresponding to C . Then, $\bar{\varphi}(J)$ is an ideal of $\mathbb{Z}_4[x]/\langle x^n - 1 \rangle$. By Theorem 1 in [2], for an odd integer n , there exist $g_1(x), a_1(x) \in \mathbb{Z}_4[x]$ such that $\bar{\varphi}(J) = \langle g_1(x) + 2a_1(x) \rangle$, where $a_1(x) \mid g_1(x) \mid (x^n - 1) \bmod 4$. Also, $\ker(\bar{\varphi}) \cap J$ is an $\frac{\mathbb{Z}_4[x]}{\langle x^n - 1 \rangle}$ -submodule of $\frac{u\mathbb{Z}_4[x]}{\langle x^n - 1 \rangle}$. So, there exist $g_2(x), a_2(x) \in \mathbb{Z}_4[x]$ such that $\ker(\bar{\varphi}) \cap J = \langle u(g_2(x) + 2a_2(x)) \rangle$ and $a_2(x) \mid g_2(x) \mid (x^n - 1) \bmod 4$. Then, for some $p_1(x) \in \mathbb{Z}_4[x]$, we have

$$J = \langle g_1(x) + 2a_1(x) + up_1(x), u(g_2(x) + 2a_2(x)) \rangle.$$

□

Lemma 3. Let $J = \langle f_1(x) + up_1(x), uf_2(x) \rangle$ be the ideal of S_n corresponding to a cyclic code C of odd length n over S , where $f_i(x) = g_i(x) + 2a_i(x)$ for $i = 1, 2$. Then,

(1) $\deg(p_1(x)) < \deg(f_2(x))$.

(2) $f_2(x) \mid f_1(x) \mid (x^n - 1) \bmod 4$ and $f_2(x) \mid p_1(x) \left(\frac{x^n - 1}{f_1(x)} \right) \bmod 4$.

Proof. (1) For all positive integer a, b and d , we have $\langle b, a \rangle = \langle b + da, a \rangle$. If $\deg(p_1(x)) > \deg(f_2(x))$ then, by Lemma 2 in [16], there exist polynomials $r(x), s(x) \in S[x]$ such that $p_1(x) = s(x)f_2(x) + r(x)$ and $\deg(r(x)) < \deg(f_2(x))$. Then,

$$J = \langle f_1(x) + u(s(x)f_2(x) + r(x)), uf_2(x) \rangle = \langle f_1(x) + ur(x), uf_2(x) \rangle.$$

So, it is sufficient to replace $p_1(x)$ by its remainder modulo $f_2(x)$.

(2) Since $uf_1(x) = u(f_1(x) + up_1(x)) \in \ker(\bar{\varphi}) \cap J = \langle uf_2(x) \rangle$, we have $f_2(x) \mid f_1(x) \mid (x^n - 1) \bmod 4$. Since

$$\left(\frac{x^n - 1}{f_1(x)} \right) (f_1(x) + up_1(x)) = up_1(x) \left(\frac{x^n - 1}{f_1(x)} \right) \in \ker(\bar{\varphi}) \cap J = uf_2(x),$$

we have $f_2(x) \mid p_1(x) \left(\frac{x^n - 1}{f_1(x)} \right) \bmod 4$.

□

Theorem 5. Let C be a cyclic code of odd length n over $R = \mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$ and let I be the ideal of $R_n = R[x]/\langle x^n - 1 \rangle$ corresponding to C . Then,

$$I = \langle g_1(x) + 2a_1(x) + up_1(x) + vp_2(x), u(g_2(x) + 2a_2(x)) + vq_1(x), v(g_3(x) + 2a_3(x)) \rangle,$$

where $a_i(x) \mid g_i(x) \mid (x^n - 1) \bmod 4$ and $g_i(x) + 2a_i(x)$ is a generator of a cyclic code over $\mathbb{Z}_4$ for $i = 1, 2, 3$.

Proof. Let I be the ideal of R_n corresponding to C . Since $\bar{\phi} : R[x]/\langle x^n - 1 \rangle \rightarrow S[x]/\langle x^n - 1, u^2 \rangle$, where $u^2 = 0$ is a surjective ring homomorphism, $\bar{\phi}(I)$ is an ideal of the ring $\frac{S[x]}{\langle x^n - 1, u^2 \rangle}$. By Theorem 4,

$$\bar{\phi}(I) = \langle g_1(x) + 2a_1(x) + up_1(x), u(g_2(x) + 2a_2(x)) \rangle.$$

Note that $\ker(\bar{\phi}) \cap I$ is an $\frac{\mathbb{Z}_4[x]}{\langle x^n - 1 \rangle}$ -submodule of $\frac{v\mathbb{Z}_4[x]}{\langle x^n - 1 \rangle}$. So, there exist $g_3(x), a_3(x) \in \mathbb{Z}_4[x]$ such that $\ker(\bar{\phi}) \cap I = \langle v(g_3(x) + 2a_3(x)) \rangle$ and $a_3(x) \mid g_3(x) \mid (x^n - 1) \pmod{4}$. Therefore, for some $p_2(x), q_1(x) \in \mathbb{Z}_4[x]$, $I = \langle g_1(x) + 2a_1(x) + up_1(x) + vp_2(x), u(g_2(x) + 2a_2(x)) + vq_1(x), v(g_3(x) + 2a_3(x)) \rangle$. $\square$

Lemma 4. Let $I = \langle f_1(x) + up_1(x) + vp_2(x), uf_2(x) + vq_1(x), vf_3(x) \rangle$ be the ideal of R_n corresponding to a cyclic code C of odd length n over R , where $f_i(x) = g_i(x) + 2a_i(x)$ for $i = 1, 2, 3$. Then, the following conditions hold:

- (1) $\deg(p_1(x)) < \deg(f_2(x))$, $\deg(q_1(x)) < \deg(f_3(x))$ and $\deg(p_2(x)) < \deg(\gcd(f_3(x), q_1(x)))$.
- (2) $f_2(x) \mid f_1(x) \mid (x^n - 1) \pmod{4}$ and $f_2(x) \mid p_1(x) \left(\frac{x^n - 1}{f_1(x)} \right) \pmod{4}$.
- (3) $f_3(x) \mid f_1(x)$, $f_3(x) \mid q_1(x) \left(\frac{x^n - 1}{f_2(x)} \right) \pmod{4}$ and $f_3(x) \mid p_2(x) \left(\frac{x^n - 1}{f_1(x)} \right) \left(\frac{x^n - 1}{f_2(x)} \right) \pmod{4}$.

Proof. (1) If $\deg(p_1(x)) > \deg(f_2(x))$ then, by Lemma 2 in [16], there exist polynomials $t(x), r(x) \in R[x]$ such that $p_1(x) = t(x)f_2(x) + r(x)$, where $\deg(r(x)) < \deg(f_2(x))$. So, $I = \langle f_1(x) + u(t(x)f_2(x) + r(x)) + vp_2(x), uf_2(x) + vq_1(x), vf_3(x) \rangle = \langle f_1(x) + ur(x) + vp_2(x), uf_2(x) + vq_1(x), vf_3(x) \rangle$. It is sufficient to replace $p_1(x)$ by its remainder modulo $f_2(x)$. Similarly, we can show that $\deg(q_1(x)) < \deg(f_3(x))$.

Now, we define homomorphism $\tau_v : \mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 \rightarrow \mathbb{Z}_4 + v\mathbb{Z}_4$ as $\tau_v(a + bu + cv) = a + cv$. This homomorphism can be extended to a homomorphism

$$\bar{\tau}_v : R[x]/\langle x^n - 1 \rangle \rightarrow (\mathbb{Z}_4 + v\mathbb{Z}_4)[x]/\langle x^n - 1, v^2 \rangle.$$

Let I be the ideal of R_n corresponding to C . Then,

$$\bar{\tau}_v(I) = \langle f_1(x) + vp_2(x), vq_1(x), vf_3(x) \rangle.$$

Let $h(x) = \gcd(f_3(x), q_1(x)) \in \mathbb{Z}_4[x]$. Then, $\bar{\tau}_v(I) = \langle f_1(x) + vp_2(x), vh(x) \rangle$. As the rings $\mathbb{Z}_4 + u\mathbb{Z}_4$ and $\mathbb{Z}_4 + v\mathbb{Z}_4$ are isomorphic, similar to the proof of Lemma 3, we have $\deg(p_2(x)) < \deg(\gcd(f_3(x), q_1(x)))$.

(2) Let I be the ideal of R_n corresponding to C . Then, $\bar{\phi}(I) = \langle f_1(x) + up_1(x), uf_2(x) \rangle$. Now, using Lemma 3, the proof is complete.

(3) Since $uf_1(x) = u(f_1(x) + up_1(x) + vp_2(x)) \in \ker(\bar{\phi}) \cap I = \langle vf_3(x) \rangle$, we must have $f_3(x) \mid f_1(x)$. Also,

$$vq_1(x) \left(\frac{x^n - 1}{f_2(x)} \right) = \left(\frac{x^n - 1}{f_2(x)} \right) (uf_2(x) + vq_1(x)) \in \ker(\bar{\phi}) \cap I = \langle vf_3(x) \rangle$$

and $f_3(x)|q_1(x) \left(\frac{x^n-1}{f_2(x)} \right) \pmod{4}$. Since

$$vp_2(x) \left(\frac{x^n-1}{f_1(x)} \right) \left(\frac{x^n-1}{f_2(x)} \right) = \left(\frac{x^n-1}{f_1(x)} \right) \left(\frac{x^n-1}{f_2(x)} \right) (f_1(x)+up_1(x)+vp_2(x)) \in \ker(\bar{\phi}) \cap I,$$

we must have $f_3(x) | p_2(x) \left(\frac{x^n-1}{f_1(x)} \right) \left(\frac{x^n-1}{f_2(x)} \right) \pmod{4}$. $\square$

Similar to Theorem 2 in [16], we obtain the following theorem.

Theorem 6. *Let C be a cyclic code of odd length n over $R = \mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$ and let I be the ideal of $R_n = \frac{R[x]}{\langle x^n-1 \rangle}$ corresponding to C . Then, I has a unique representation as*

$$I = \langle f_1(x) + up_1(x) + vp_2(x), uf_2(x) + vq_1(x), vf_3(x) \rangle.$$

Now, we recall some definitions, which will be used in Theorem 7. Let $\mu : R = \mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 \rightarrow \mathbb{F}_2$ given by $\alpha \mapsto \alpha \pmod{\langle 2, u, v \rangle}$ be the natural homomorphism mapping R to its residue field $\mathbb{F}_2$. The map μ is extended to $\bar{\mu} : R[x] \rightarrow \mathbb{F}_2[x]$ in the usual way. The image of the polynomial $f(x) \in R[x]$ under this projection is denoted by $\bar{f}(x)$. A monic polynomial $f(x) \in R[x]$ is said to be a basic irreducible polynomial over R if $\bar{f}(x)$ is irreducible in $\mathbb{F}_2[x]$. A polynomial $f(x) \in R[x]$ is called regular if is not a zero divisor. Since $(R, \langle 2, u, v \rangle)$ is a finite local ring, by Theorem XIII. 2 in [14], the polynomial $f(x)$ is regular if and only if $\bar{f}(x) \neq 0$. The polynomial $f(x)$ is called primary if $\langle f(x) \rangle$ is a primary ideal, i.e., if for all $gh \in \langle f \rangle$, we have $g \in \langle f \rangle$ or $h^\ell \in \langle f \rangle$, $\ell \geq 1$ is an integer. Also, two polynomials $f(x), g(x) \in R[x]$ are called coprime if $\langle f(x) \rangle + \langle g(x) \rangle = R[x]$.

Now, we recall some basic facts about Galois extensions of $\mathbb{Z}_4$. Let $h(x)$ be a monic basic irreducible polynomial over $\mathbb{Z}_4$ of degree $s \geq 1$. Then, the Galois ring $GR(4, s)$ is defined as the quotient ring $\mathbb{Z}_4[x]/\langle h(x) \rangle$. The ring $GR(4, s)$ is a local ring with the unique maximal ideal $\langle 2 \rangle$ and the residue field $\mathbb{F}_{2^s}$. Let $\mathcal{T} = \{0, 1, \xi, \xi^2, \dots, \xi^{2^s-2}\}$ be the Teichmüller representatives of $GR(4, s)$, where ξ is a root of a basic primitive polynomial with degree s in $\mathbb{Z}_4[x]$. Then, any element $\alpha \in GR(4, s)$ can be written uniquely as $\alpha = a_0 + 2a_1$, where $a_0, a_1 \in \mathcal{T}$. Moreover, α is a unit in $GR(4, s)$ if and only if $a_0 \neq 0$, and α is a zero divisor or 0 if and only if $a_0 = 0$. We consider the factorization of $x^n - 1$ over the ring R as it plays a vital role in the study of cyclic codes with length n over R . Pursuant to Lemma 4.1 in [7], we give the following essential theorem:

Theorem 7. *Let C be a cyclic code of odd length n over the ring $R = \mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$ and let I be the ideal of R_n corresponding to C . Then,*

(1) *For any $h_1(x), h_2(x), h_3(x) \in \mathbb{Z}_4[x]/\langle x^n-1 \rangle$, we have $h_1(x) \in \langle h_1(x) + uh_2(x) + vh_3(x) \rangle$. Hence,*

$$\langle h_1(x), uh_2(x) + vh_3(x) \rangle = \langle h_1(x) + uh_2(x) + vh_3(x) \rangle.$$

(2) *Let $I = \langle f_1(x) + up_1(x) + vp_2(x), uf_2(x) + vq_1(x), vf_3(x) \rangle$, where polynomials $f_1(x), p_1(x), p_2(x), f_2(x), q_1(x)$ and $f_3(x)$ in $\frac{\mathbb{Z}_4[x]}{\langle x^n-1 \rangle}$ satisfying the conditions of Theorem 5. Then, $I = \langle f_1(x) + uf_2(x) + vq_1(x), vf_3(x) \rangle$.*

Proof. (1) Since n is an odd integer, the polynomial $x^n - 1 \in R[x]$ is regular. Using Theorem 12.3.7 in [12], $x^n - 1 = f_1(x)f_2(x) \dots f_r(x)$, where $f_1(x), f_2(x), \dots, f_r(x)$ are unique monic irreducible (and basic irreducible) pairwise coprime polynomials in $\mathbb{Z}_4[x]$. By the Chinese remainder theorem,

$$\mathbb{Z}_4[x]/\langle x^n - 1 \rangle \cong \mathbb{Z}_4[x]/\langle f_1(x) \rangle \times \mathbb{Z}_4[x]/\langle f_2(x) \rangle \times \dots \times \mathbb{Z}_4[x]/\langle f_r(x) \rangle.$$

Let $\deg(f_j) = s_j$ for $j = 1, 2, \dots, r$. Then, $\mathbb{Z}_4[x]/\langle f_j(x) \rangle = GR(4, s_j)$. Let $R_j = GR(4, s_j)$. Clearly, $R[x]/\langle x^n - 1 \rangle \cong \prod_{j=1}^r (R_j + uR_j + vR_j)$. Choose $h_1(x), h_2(x), h_3(x) \in \mathbb{Z}_4[x]/\langle x^n - 1 \rangle$. We can write $h_i(x) = (h_{i1}(x), h_{i2}(x), \dots, h_{ir}(x))$, where $h_{ij}(x) \in R_j$ for $i = 1, 2, 3$ and $j = 1, 2, \dots, r$. Now, fix j . If $h_{1j}(x) \neq 0$ then, by the 2-adic representation of elements $GR(4, s_j)$, we have $h_{1j}(x) = a_{1j}(x) + 2b_{1j}(x)$. If $a_{1j}(x) \neq 0$, then, $h_{1j}(x)$ is a unit in $GR(4, s_j)$. Then,

$$h_{1j}(x) = (h_{1j}(x) + uh_{2j}(x) + vh_{3j}(x))^4 (h_{1j}(x)^{-1})^4 h_{1j}(x) \in (h_{1j}(x) + uh_{2j}(x) + vh_{3j}(x))(R_j + uR_j + vR_j).$$

Therefore, $h_1(x) \in \langle h_1(x) + uh_2(x) + vh_3(x) \rangle$. If $a_{1j}(x) = 0$ then, $h_{1j}(x) = 2b_{1j}(x)$, where $b_{1j}(x) \in \mathcal{T}$. Note that the Teichmüller set is isomorphic to field $\mathbb{F}_{2^s}$ and so b_{1j} is a unit in $\mathbb{F}_{2^s}$. Since

$$h_{1j}(x) = 2(b_{1j}(x) + uh_{2j}(x) + vh_{3j}(x))^4 b_{1j}(x)^{-3} \in (h_{1j}(x) + uh_{2j}(x) + vh_{3j}(x))(R_j + uR_j + vR_j)$$

$h_1(x) \in \langle h_1(x) + uh_2(x) + vh_3(x) \rangle$. The second statement immediately follows from the first statement.

(2) By Lemma 3, $f_2(x) \mid f_1(x) \mid (x^n - 1) \bmod 4$ and $f_2(x) \mid p_1(x) \left(\frac{x^n - 1}{f_1(x)} \right) \bmod 4$. Since $x^n - 1$ factors into distinct basic irreducible polynomials of $R[x]$, it is obvious that two polynomials $f(x), g(x) \in R[x]$ are coprime if and only if $\bar{f}(x), \bar{g}(x)$ are coprime in $\mathbb{F}_2[x]$. Then, $\gcd(f_2(x), \frac{x^n - 1}{f_1(x)}) = 1$, and $f_2(x) \mid p_1(x)$. By Lemma 3, we have $\deg(p_1(x)) < \deg(f_2(x))$. Therefore, $p_1(x) = 0$. Using (1), we have $I = \langle f_1(x), vp_2(x), uf_2(x) + vq_1(x), vf_3(x) \rangle$. Now, it is enough to show that $p_2(x) = 0$. Since $vp_2(x) \in \ker(\bar{\phi}) \cap I = \langle vf_3(x) \rangle$, $f_3(x) \mid p_2(x)$ and $\deg(p_2(x)) < \deg(\gcd(f_3(x), q_1(x))) \leq \deg(f_3(x))$ by Lemma 3, we have $p_2(x) = 0$. Applying (1), we obtain $I = \langle f_1(x) + uf_2(x) + vq_1(x), vf_3(x) \rangle$. $\square$

Corollary 1. *The homomorphic image of a cyclic code with odd length n over $R = \mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$ is a principal ideal in S_n .*

Proof. By Theorem 7, any cyclic code with odd length n over R can be written uniquely as $C = \langle f_1(x) + uf_2(x) + vq_1(x), vf_3(x) \rangle$. Now, we define the natural homomorphism

$$\tau_u : \mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 \rightarrow \mathbb{Z}_4 + u\mathbb{Z}_4, \quad \tau_u(a + bu + cv) = a + bu,$$

which can be extended to a homomorphism $\bar{\tau}_u : R[x]/\langle x^n - 1 \rangle \longrightarrow S[x]/\langle x^n - 1, u^2 \rangle$, where $u^2 = 0$. Then, $\bar{\tau}_u(C) = \langle f_1(x) + uf_2(x) \rangle$, which is a cyclic code and therefore a principal ideal of ring S_n . $\square$

3. Rank, minimal spanning sets and dual of cyclic codes

Following Dougherty and Shiromoto [8], for a code C with length n over a ring R , we define the rank of C , denoted by $\text{rank}(C)$, as the minimum number of generators of C . Define the free rank of C , denoted by f-rank , by the maximum of the ranks of R -free submodules of C . Recall that, a free module C is a module with a basis. To obtain main results of this section, we will make use of the following lemma and the subsequent theorem.

Lemma 5. *Let $C = \langle f_1(x) + uf_2(x) + vq_1(x), vf_3(x) \rangle$ be a cyclic code with odd length n over the ring $R = \mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$. If $\deg(f_1) = \deg(f_3)$ and $f_3(x)$ be a regular element. Then, $C = \langle f_1(x) + uf_2(x) + vq_1(x) \rangle$ and $f_1(x) + uf_2(x) + vq_1(x) \mid (x^n - 1)$.*

Proof. From Lemma 4, we have $f_3 \mid f_1$. Since $\deg(f_1) = \deg(f_3)$ and $f_1(x)$ is a monic polynomial, it follows that $f_1(x) = f_3(x)$. Since $vf_3(x) = vf_1(x) = v(f_1(x) + uf_2(x) + vq_1(x))$, we have $vf_3(x) \in \langle f_1(x) + uf_2(x) + vq_1(x) \rangle$. Therefore, $C = \langle f_1(x) + uf_2(x) + vq_1(x) \rangle$. Since $f_3(x) = f_1(x)$ is regular, it is clear that $f_1(x) + uf_2(x) + vq_1(x)$ is also regular. Then, by Lemma 2 in [16], there exist polynomials $\ell(x), r(x) \in R[x]$ such that

$$x^n - 1 = \ell(x)(f_1(x) + uf_2(x) + vq_1(x)) + r(x),$$

where $r(x) = 0$ or $\deg(r(x)) < \deg(f_1(x) + uf_2(x) + vq_1(x))$. If $r(x) = 0$ then, the proof is complete. Otherwise, we have $r(x) = -\ell(x)(f_1(x) + uf_2(x) + vq_1(x)) \in C$. This yields a contradiction, since $f_1(x) + uf_2(x) + vq_1(x)$ is a generator of C and therefore, it has the minimal degree in C . $\square$

Following [9], we give the definition of modular independence. Note that the definition and properties of modular independence not only are valid for any finite local Frobenius ring but also are valid for any finite local ring.

Definition 1. Let R be a local ring with unique maximal ideal m and $v_1, v_2, \dots, v_k$ be elements of R^n . Then, $v_1, v_2, \dots, v_k$ are called modular independent if $\sum_{i=1}^k \alpha_i v_i = 0$ implies that $\alpha_i \in m$ for all $i = 1, 2, \dots, k$.

Theorem 8. (1) *Let $C = \langle f(x) \rangle$ be a cyclic code with odd length n over R , where $f(x) = f_1(x) + uf_2(x) + vq_1(x)$ is regular with $\deg(f(x)) = t$. Then, C is a free code of rank $n - t$ and $X = \{f(x), xf(x), \dots, x^{n-t-1}f(x)\}$ is a basis for C .*

(2) *Let $C = \langle f_1(x), uf_2(x) + vq_1(x), vf_3(x) \rangle$ be a cyclic code with odd length n over $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$. If $\deg(f_1(x)) = r, \deg(uf_2(x) + vq_1(x)) = s, \deg(vf_3(x)) = t$ and $f_1(x), f_2(x), f_3(x)$ are monic in $\mathbb{Z}_4[x]/\langle x^n - 1 \rangle$ then, $\beta = \{f_1(x), xf_1(x), \dots, x^{n-r-1}f_1(x), uf_2(x) +$*

$vq_1(x), \dots, x^{r-s-1}(uf_2(x) + vq_1(x)), vf_3(x), xv f_3(x), \dots, x^{r-t-1}vf_3(x)\}$ is a minimal spanning set for C .

Proof. (1) By Lemma 5, we must have $f(x) \mid (x^n - 1)$. Then, there exists a polynomial $g(x) \in R[x]$ with $\deg(g(x)) = n - t$ such that $f(x)g(x) = x^n - 1$. Now, let $c(x)$ be an element of C . Then, there exists a polynomial $h(x) \in R[x]$ such that $c(x) = h(x)f(x)$. If $\deg(h(x)) \leq n - t - 1$ then, the proof is done. Else, since $f(x)$ is regular, Lemma 2 in [16], implies that there exist polynomials $q(x), r(x) \in R[x]$ such that $h(x) = q(x)g(x) + r(x)$, where $r(x) = 0$ or $\deg(r(x)) \leq n - t - 1$. Thereby $c(x) = h(x)f(x) = r(x)f(x)$. This shows that X is a generating set for code C . Now, we must show that X is linearly independent over R . Let $\ell(x) = \ell_0 + \ell_1x + \dots + \ell_{n-t-1}x^{n-t-1} \in R[x]$ be a polynomial such that $\ell(x)f(x) = 0$. Since $f(x)$ is regular, Theorem (XIII.6) in [14] implies that there exist unit $v \in R[x]$ and monic polynomial $p(x) = p_0 + p_1x + \dots + p_tx^t \in R[x]$, where p_t is a unit in R , such that $f(x) = vp(x)$. Then, $\ell(x)vp(x) = 0$, and since v is unit, this implies that $\ell(x)p(x) = 0$. Note that the coefficient of the highest degree of x in $\ell(x)p(x)$ is $\ell_{n-t-1}p_t = 0$. Since p_t is a unit, we must have $\ell_{n-t-1} = 0$. Similarly, we can show that $\ell_i = 0$ for $i = 0, 1, \dots, n - t - 2$.

(2) Without loss of generality, we assume that $t \leq s$ and so, $vf_3(x)$ is the lowest degree polynomial in C . Therefore, it is sufficient to show that β spans $S = \{f_1(x), xf_1(x), \dots, x^{n-r-1}f_1(x), uf_2(x) + vq_1(x), x(uf_2(x) + vq_1(x)), \dots, x^{n-s-1}(uf_2(x) + vq_1(x)), vf_3(x), vx f_3(x), \dots, vx^{n-t-1}f_3(x)\}$. Now, we need to show that $vx^{r-t}f_3(x) \in \text{span}(\beta)$. Suppose that the leading coefficient of $x^{r-t}f_3(x)$ is a_0 and the leading coefficient of the monic polynomial $f_1(x)$ is b_0 . Then, there exists $c_0 \in \mathbb{Z}_4$ such that $a_0 = b_0c_0$. By Lemma 2 in [16], we have $vx^{r-t}f_3(x) = vc_0f_1(x) + vd(x)$, where $d(x)$ is a polynomial in C of degree less than r . By the structure of C , each polynomial in C has degree greater than or equal to $\deg(f_3(x)) = \deg(vf_3(x)) = t$. Then, $t \leq \deg(d(x)) < r$ and $vd(x) = a_0vf_3(x) + a_1vx f_3(x) + \dots + a_{r-t-1}vx^{r-t-1}f_3(x)$. Hence, $vx^{r-t}f_3(x) \in \text{span}(\beta)$. Similarly, we can show that $vx^{r-t+1}f_3(x), vx^{r-t+2}f_3(x), \dots, vx^{n-t-1}f_3(x) \in \text{span}(\beta)$ and $x^{r-s}(uf_2 + vq_1), x^{r-s+1}(uf_2 + vq_1), \dots, x^{n-s-1}(uf_2 + vq_1) \in \text{span}(\beta)$. Therefore, β is a generating set for C . Now, we must show that β is modular independent. Let $f_1(x) = h_0 + h_1x + \dots + h_rx^r$, $uf_2(x) + vq_1(x) = g_0 + g_1x + \dots + g_tx^t$ and $vf_3(x) = k_0 + k_1x + \dots + k_sx^s$, where h_r, g_t and k_s are units in R . Let

$$e(x) = \sum_{i=0}^{n-r-1} e_i x^i, w(x) = \sum_{i=0}^{r-t-1} w_i x^i, z(x) = \sum_{i=0}^{r-s-1} z_i x^i \in R[x]$$

such that $e(x)f_1(x) + w(x)(uf_2(x) + vq_1(x)) + z(x)(vf_3(x)) = 0$. Comparing the coefficient x^{n-1} on both sides of the equation implies that $h_re_{n-r-1} = 0$. Since h_r is unit, we must have $e_{n-r-1} = 0$. Moreover, by comparing the coefficients x^{n-2} on both sides of the equation, we obtain $h_{r-1}e_{n-r-1} + e_{n-r-2}h_r = 0$. Since e_{n-r-1} is zero and h_r is unit, we have $e_{n-r-2} = 0$. Similarly, we can show that $e_{n-r-3} = \dots = e_1 = e_0 = 0$. Note that u, v are zero divisors in the ring $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$ and so the

coefficient of x containing any w_i , for $i = 0, 1, \dots, r-t-1$, is zero when $w_i \in \langle 2, u, v \rangle$. Again, z_i , for $i = 0, 1, \dots, r-s-1$, are zero when $z_i \in \langle 2, u, v \rangle$. This shows that β is modular independent. $\square$

Definition 2. Let I be an ideal of ring $R[x]$. The annihilator of I , denoted by $\text{Ann}(I)$, is defined as

$$\text{Ann}(I) = \{h(x) : h(x)f(x) = 0, \forall f(x) \in I\}.$$

The reciprocal $f^*(x)$ of a polynomial $f(x)$ of degree n is defined by $f^*(x) = x^n f(\frac{1}{x})$. It is clear that if C is a cyclic code with associated ideal I then, the associate ideal of $C^\perp$ is $\text{Ann}(I)^* = \{f^*(x) : f(x) \in \text{Ann}(I)\}$.

We present the following lemma, which is required for the proof of Theorem 9.

Lemma 6. Let n be an odd integer and $g(x), h(x)$ be divisors of $x^n - 1$ in $R[x]$. Then,

$$\frac{x^n - 1}{\gcd(g(x), h(x))} = \text{lcm}\left(\frac{x^n - 1}{g(x)}, \frac{x^n - 1}{h(x)}\right).$$

Proof. Since n is an odd integer, the polynomial $x^n - 1 \in R[x]$ is regular. By Theorem 12.3.7 in [12], we have $x^n - 1 = f_1(x)f_2(x) \dots f_r(x)$, where $f_1(x), f_2(x), \dots, f_r(x)$ are distinct monic, irreducible and pairwise coprime polynomials in $\mathbb{Z}_4[x]$. Without loss of generality, we assume that $g(x), h(x)$ are irreducible divisors of $x^n - 1$. Let $g(x) = f_i(x)$ and $h(x) = f_j(x)$, where $1 \leq i \neq j \leq r$. Since $\gcd(g(x), h(x)) = 1$, we have

$$\text{lcm}\left(\frac{x^n - 1}{g(x)}, \frac{x^n - 1}{h(x)}\right) = \text{lcm}(f_1(x) \dots f_{i-1}(x)f_{i+1}(x) \dots f_r(x), f_1(x) \dots f_{j-1}(x)f_{j+1}(x) \dots f_r(x)) = x^n - 1,$$

and the proof is complete. $\square$

Theorem 9. Let $I = \langle f_1(x) + uf_2(x) + vq_1(x), vf_3(x) \rangle$, where I is the ideal of R_n corresponding to a cyclic code C of odd length n over the ring $R = \mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$. Then,

$$\text{Ann}(I) = \left\langle \frac{x^n - 1}{\gcd(f_3(x), f_2(x))} + u \frac{x^n - 1}{f_1(x)}, v \frac{x^n - 1}{f_1(x)} \right\rangle$$

and the ideal

$$\left\langle \frac{x^n - 1}{(\gcd(f_3(x), f_2(x)))^*} + u \left(\frac{x^n - 1}{f_1^*(x)}\right), v \left(\frac{x^n - 1}{f_1^*(x)}\right) \right\rangle,$$

corresponds to the dual code $C^\perp$ of C .

Proof. Note that $\text{Ann}(I)$ is an ideal of R_n . By Theorem 7,

$$\text{Ann}(I) = \langle g_1(x) + ug_2(x) + v\ell_1(x), vg_3(x) \rangle = \langle g_1(x), ug_2(x) + v\ell_1(x), vg_3(x) \rangle,$$

where $g_1(x), g_2(x), \ell_1(x), g_3(x) \in \mathbb{Z}_4[x]/\langle x^n - 1 \rangle$ satisfying the conditions (1), (2) and (3) of Lemma 4. Again, by Theorem 7, the ideal I corresponding to the cyclic code C also has a representation as $I = \langle f_1(x), uf_2(x) + vq_1(x), vf_3(x) \rangle$. Since $g_1(x) + ug_2(x) + v\ell_1(x) \in \text{Ann}(I)$, $(g_1(x) + ug_2(x) + v\ell_1(x))vf_3(x) = 0$. Hence, $g_1(x)f_3(x) = x^n - 1$, so $\frac{x^n-1}{f_3(x)} \mid g_1(x) \pmod{4}$. This shows that $uf_2(x) + vq_1(x) \in I$. Moreover, since $g_1(x)(uf_2(x) + vq_1(x)) \equiv 0 \pmod{4}$, it follows that $\frac{x^n-1}{f_2(x)} \mid g_1(x)$ in $\mathbb{Z}_4[x]$. By Lemma 6,

$$\text{lcm}\left(\frac{x^n-1}{f_2(x)}, \frac{x^n-1}{f_3(x)}\right) = \frac{x^n-1}{\gcd(f_2(x), f_3(x))}.$$

Therefore, $g_1(x) = \frac{x^n-1}{\gcd(f_2(x), f_3(x))}h_1(x)$ for some $h_1(x) \in \mathbb{Z}_4[x]/\langle x^n - 1 \rangle$. Also, $ug_2(x) + v\ell_1(x) \in \text{Ann}(I)$, then, $(ug_2(x) + v\ell_1(x))f_1(x) = 0$. Therefore, $g_2(x) = \left(\frac{x^n-1}{f_1(x)}\right)h_2(x)$ and $\ell_1(x) = \left(\frac{x^n-1}{f_1(x)}\right)h_3(x)$ for some $h_2(x), h_3(x) \in \mathbb{Z}_4[x]/\langle x^n - 1 \rangle$. Finally, since $vg_3(x)f_1(x) = 0$, we have $g_3(x) = \left(\frac{x^n-1}{f_1(x)}\right)h_4(x)$ for some $h_4(x) \in \mathbb{Z}_4[x]/\langle x^n - 1 \rangle$. Hence, by Theorem 7, $\text{Ann}(I)$ is a subset of the following set:

$$\left\langle \frac{x^n-1}{\gcd(f_3(x), f_2(x))}, u\frac{x^n-1}{f_1(x)}, v\frac{x^n-1}{f_1(x)} \right\rangle = \left\langle \frac{x^n-1}{\gcd(f_3(x), f_2(x))} + u\frac{x^n-1}{f_1(x)}, v\frac{x^n-1}{f_1(x)} \right\rangle.$$

It is obvious that $\left\langle \frac{x^n-1}{\gcd(f_3(x), f_2(x))} + u\frac{x^n-1}{f_1(x)}, v\frac{x^n-1}{f_1(x)} \right\rangle \subseteq \text{Ann}(I)$. The proof of the second statement is obvious by definition. $\square$

Note that $\deg(f^*) = \deg(f)$ for any monic polynomial $f(x)$. In general, for a code C of length n over a non-Frobenius ring R , the equation $|C||C^\perp| = |R|^n$ is not valid. A sufficient condition for this equality to be valid is given in the following theorem.

Theorem 10. *Let $C = \langle f_1(x), uf_2(x) + vq_1(x), vf_3(x) \rangle$ be a cyclic code of odd length n over $R = \mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$, where $\deg(f_1) = r, \deg(f_2) = s, \deg(f_3) = t$ and $f_3 \mid f_2$. Then, we have $|C||C^\perp| = |R|^n$ if and only if C is a code over the Frobenius subring $S = \mathbb{Z}_4 + u\mathbb{Z}_4$ of R .*

Proof. If C is a code of length n over the Frobenius ring $\mathbb{Z}_4 + u\mathbb{Z}_4$ then, by [18], we have $|C||C^\perp| = |\mathbb{Z}_4 + u\mathbb{Z}_4|^n$. Now, let $C = \langle f_1(x), uf_2(x) + vq_1(x), vf_3(x) \rangle$ be a cyclic code of odd length n over the ring $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$. By Lemma 4, $\deg(q_1) < \deg(f_3)$ and by assumption $\deg(f_3) < \deg(f_2)$, $\deg(uf_2 + vq_1) = \deg(f_2)$. Theorem 9, implies that $|C^\perp| = 4^{2r} \cdot 4^{\deg(\gcd(f_2, f_3))}$. As $f_3 \mid f_2$, we have $|C^\perp| = 4^{2r+t}$. Now, suppose that the equation $|C||C^\perp| = |\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4|^n = 4^{3n}$ does hold. Then, $4^{3n-r-s-t} \cdot 4^{2r+t} = 4^{3n}$. This implies that $r = s$. By Lemma 4, $f_2 \mid f_1$, $\deg(f_1) =$

$\deg(f_2)$ and $f_1(x)$, $f_2(x)$ are monic polynomial, it follows that $f_2(x) = f_1(x)$. So, $C = \langle f_1(x)(1+u) + vq_1(x), vf_3(x) \rangle = \langle f_1(x) + vq_1(x), vf_3(x) \rangle$ and C is a code over the ring $\mathbb{Z}_4 + v\mathbb{Z}_4$, which is isomorphic to $\mathbb{Z}_4 + u\mathbb{Z}_4$. Therefore, we can assume that C is a code over the Frobenius ring $\mathbb{Z}_4 + u\mathbb{Z}_4$. $\square$

Theorem 11. (i) Let $C \subseteq (\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4)^n$ is a self-orthogonal code and $n_{U_i}(c)$ denotes the number of units of the i -th type that appear in codeword c . Then, for every $c \in C$, the number $n_{U_i}(c)$ is even for each $i = 1, 2, 3, 4$.

(ii) If C is a self-dual code of length n then, $\langle 2u, 2v \rangle \in C$.

Proof. (i) Suppose that C is self-orthogonal. Then, $\langle c, c \rangle = 0$ for all $c \in C$. By Equation (2.1),

$$\begin{aligned} \langle c, c \rangle &= n_{U_1}(c) + n_{U_2}(c) + n_{U_2}(c)2u + n_{U_3}(c) + n_{U_3}(c)2v \\ &\quad + n_{U_4}(c) + n_{U_4}(c)2u + n_{U_4}(c)2v \\ &= 0. \end{aligned} \tag{3.1}$$

Therefore, $n_{U_2}(c)$, $n_{U_3}(c)$ and $n_{U_4}(c)$ must be even. Thus $n_{U_1}(c) + n_{U_2}(c) + n_{U_3}(c) + n_{U_4}(c)$ must be even. This implies that $n_{U_1}(c)$ is even.

(ii) If C is self-dual then, $\langle c, c \rangle = 0$ for all $c \in C$. The Equation (3.1), shows that the number of units in c , must be even. Since

$$a \cdot (2u) = \begin{cases} 0 & a \in m \\ 2u & a \in U(R) \end{cases}$$

Now, if we denote the all $2u$ -vector of length n by $2u$ then, $\langle c, 2u \rangle = n_U(c) \cdot (2u) = 0$, because $n_U(c)$ is even. Hence, $2u \in C^\perp = C$. Similarly, we can show that $2v \in C$. Therefore, $\langle 2u, 2v \rangle \in C$. $\square$

4. Gray map and $\mathbb{Z}_4$ -images of cyclic codes

Since codes over $\mathbb{Z}_4$ have a significant role in coding theory, designs, cryptography and DNA computing, it is of interest to researchers to find linear codes over $\mathbb{Z}_4$ with better parameters. One way of finding such codes has been considering codes over an extension of $\mathbb{Z}_4$ and using a Gray-like map to obtain codes over $\mathbb{Z}_4$. There are a number of papers in the literature that present new linear codes over $\mathbb{Z}_4$ by this approach and there is a database of best known $\mathbb{Z}_4$ -codes [4, 5]. To obtain codes over $\mathbb{Z}_4$ from codes over $R = \mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$, we introduce two Gray-like maps ψ and ϕ from the ring R to $\mathbb{Z}_4^3$ and $\mathbb{Z}_4^6$, respectively. Let A be an element of $GL_3(\mathbb{Z}_4)$, i.e., an invertible matrix of order 3 over $\mathbb{Z}_4$. A map $\psi : R \rightarrow \mathbb{Z}_4^3$ for any element $r = a + bu + dv \in R$ is defined as $\psi(a + bu + dv) = (a, b, d)A$. For simplicity, $(a, b, d)A$

is written as rA . The map ψ can naturally be extended as

$$\psi : R^n \rightarrow \mathbb{Z}_4^{3n},$$

$$(c_0, c_1, c_2, \dots, c_{n-1}) \mapsto (c_0A, c_1A, c_2A, \dots, c_{n-1}A).$$

Let C be a code of length n over R . The Lee weight of $c = (c_0, c_1, \dots, c_{n-1}) \in C$ is defined as the rational sum of Lee weight of all coordinates in c . The minimum Lee weight of C is the minimum Lee weight of all codewords in C . For any codewords $c, c' \in C$, the Lee distance of c and c' is defined as the Lee weight of $c - c'$. Also, the minimum Lee distance of C is the smallest nonzero Lee weight among all codewords.

Definition 3. The map ψ is a Gray map from R^n to $\mathbb{Z}_4^{3n}$ corresponding to the invertible matrix A . The Lee weight of any $a+bu+dv \in R$ is defined as $w_L(a+bu+dv) = w_L((a, b, d)A)$.

Since A is an invertible matrix over $\mathbb{Z}_4$, the map ψ is an $\mathbb{Z}_4$ -isomorphism. Therefore, the following theorem is obvious from the definition of Gray map and Lee weight:

Theorem 12. The Gray map ψ is a $\mathbb{Z}_4$ -linear bijection map from $((\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4)^n, \text{Lee distance})$ to $(\mathbb{Z}_4^{3n}, \text{Lee distance})$.

We give an example to show that Gray map ψ does not preserve self duality of linear codes.

Example 2. Let $A = \begin{pmatrix} 2 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & 2 \end{pmatrix}$ be a matrix of $GL_3(\mathbb{Z}_4)$. Let

$$C = \langle 2 + u + v \rangle = \{0, 2 + u + v, 2u + 2v, 2u, 2v, 2 + u + 3v, 2 + 3u + v, 2 + 3u + 3v\}$$

be a cyclic code of length 1 over the ring $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$. Since $(2+u+v)(2+u+v) = 0$, $2+u+v \in C^\perp$. We show that $\psi(2+u+v) \notin \psi(C)^\perp$. We aim to show that $\psi(2+u+v)\psi(2+u+v) \neq 0$. Clearly, $\psi(2+u+v) = (2, 1, 1)A = [-1, -1, 0]^\perp$ and thus $\psi(2+u+v).\psi(2+u+v) = 2 \neq 0$.

We define another Gray map $\phi : \mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 \rightarrow \mathbb{Z}_4^6$ as

$$\phi(a + bu + dv) = (b, d, b + d + a, b + 2d + 2a, b + 3d + a, d + 2b).$$

This map ϕ can be extended to $(\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4)^n$ component-wise. Clearly, the Gray map ϕ is an injective, $\mathbb{Z}_4$ -linear from $((\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4)^n, \text{Lee weight})$ to $(\mathbb{Z}_4^{6n}, \text{Lee weight})$.

Theorem 13. Let C be a self-orthogonal cyclic code over $R = \mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$. Then, $\phi(C)$ is self-orthogonal.

Proof. Suppose that C is a self-orthogonal cyclic code over R of length n . Also, let $\mathbf{c}_1 = a_1 + b_1u + d_1v$, $\mathbf{c}_2 = a_2 + b_2u + d_2v \in C$, where $a_i, b_i, d_i \in \mathbb{Z}_4$ for $i = 1, 2$. Since C is self-orthogonal, $\langle \mathbf{c}_1, \mathbf{c}_1 \rangle = 0$. This implies that $a_1 \cdot a_2 = a_1b_2 + a_2b_1 = a_1d_2 + a_2d_1 = 0$. It is sufficient to show that $\langle \phi(\mathbf{c}_1), \phi(\mathbf{c}_2) \rangle = 0$. But $\langle \phi(\mathbf{c}_1), \phi(\mathbf{c}_2) \rangle$ equals to:

$$\begin{aligned} & b_1b_2 + d_1d_2 + (b_1b_2 + d_1d_2 + b_1d_2 + b_2d_1) + (b_1b_2 + 2b_1d_2 + 2d_1b_2) \\ & + (b_1b_2 + d_1d_2 + 3b_1d_2 + 3b_2d_1) + (d_1d_2 + 2d_1b_2 + 2d_2b_1) = 0. \end{aligned}$$

Therefore, $\phi(C) \subseteq \phi(C)^\perp$. □

Note that in general the Gray image of a self-dual code over R under ϕ is not a self dual code over $\mathbb{Z}_4$.

Example 3. Let $C = \langle u, v \rangle = \{0, u, 2u, 3u, v, 2v, 3v, u + v, u + 2v, u + 3v, 2u + v, 2u + 2v, 2u + 3v, 3u + v, 3u + 2v, 3u + 3v\}$ be a cyclic code of length 1 over R . Clearly, C is a self-dual code. The Gray image of C under ϕ is $\phi(C) = \{000000, 101112, 202220, 303332, 011231, 022022, 033213, 112303, 220202, 332101, 123303, 130321, 213011, 231033, 310123, 321310\}$. Since $231211 \in \phi(C)^\perp$, $\phi(C) \subsetneq \phi(C)^\perp$.

Definition 4. Let τ be the cyclic shift over R^n and $m = tn$. The quasi-shift operator $\sigma^{(t)}$ is given by

$$\sigma^{(t)}(a_1 | a_2 | \cdots | a_t) = (\tau(a_1) | \tau(a_2) | \cdots | \tau(a_t)),$$

where $a_i \in \mathbb{Z}_4^n$ for $i = 1, 2, \dots, t$ and " $|$ " denotes the usual vector concatenation. A quasi-cyclic code of index t and length tn over $\mathbb{Z}_4$ is a subset $\mathbb{Z}_4^{tn}$ such that $\sigma^{(t)}(C) = C$.

Theorem 14. A linear code C of length n over $R = \mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$ is a cyclic code if and only if $\phi(C)$ is a quasi-cyclic code of index 6 and length $6n$ over $\mathbb{Z}_4$.

Proof. Let ϕ be the Gray map and $\sigma^{(t)}$ be the quasi-cyclic shift on R^n . We show that $\sigma^{(6t)}(\phi(C)) = \phi(\tau(C))$, where τ is the cyclic shift on R^n . Let $\mathbf{c} = (c_0, c_1, \dots, c_{n-2}, c_{n-1}) \in C$, where $c_i = a_i + b_iu + d_iv$, for $i = 0, 1, \dots, n-1$. Then,

$$\begin{aligned} \sigma^{(6t)}(\phi(\mathbf{c})) &= \sigma^{(6t)}(b_0, b_1, \dots, b_{n-2}, b_{n-1}, d_0, d_1, \dots, d_{n-2}, d_{n-1}, b_0 + d_0 + a_0, b_1 + d_1 + a_1, \dots, b_{n-2} + d_{n-2} + a_{n-2}, \\ & b_{n-1} + d_{n-1} + a_{n-1}, b_0 + 2d_0 + 2a_0, b_1 + 2d_1 + 2a_1, \dots, b_{n-1} + 2d_{n-1} + 2a_{n-1}, b_0 + 3d_0 + a_0, b_1 + 3d_1 + a_1, \dots, \\ & b_{n-2} + 3d_{n-2} + a_{n-2}, b_{n-1} + 3d_{n-1} + a_{n-1}, d_0 + 2b_0, d_1 + 2b_1, \dots, d_{n-2} + 2b_{n-2}, d_{n-1} + 2b_{n-1}) \\ &= (b_{n-1}, b_0, b_1, \dots, b_{n-2}, d_{n-1}, d_0, d_1, \dots, d_{n-2}, b_{n-1} + d_{n-1} + a_{n-1}, b_0 + d_0 + a_0, b_1 + d_1 + a_1, \dots, b_{n-2} + d_{n-2} \\ & + a_{n-2}, b_{n-1} + 2d_{n-1} + 2a_{n-1}, b_0 + 2d_0 + 2a_0, b_1 + 2d_1 + 2a_1, \dots, b_{n-2} + 2d_{n-2} + 2a_{n-2}, b_{n-1} + 3d_{n-1} + a_{n-1}, \\ & b_0 + 3d_0 + a_0, b_1 + 3d_1 + a_1, \dots, b_{n-2} + 3d_{n-2} + a_{n-2}, d_{n-1} + 2b_{n-1}, d_0 + 2b_0, \dots, d_{n-2} + 2b_{n-2}). \end{aligned}$$

On the other hand

$$\begin{aligned} \phi(\tau(\mathbf{c})) &= \phi(c_{n-1}, c_0, c_1, \dots, c_{n-2}) = (b_{n-1}, b_0, b_1, \dots, b_{n-2}, d_{n-1}, d_0, d_1, \dots, d_{n-2}, b_{n-1} + d_{n-1} + a_{n-1}, \\ & b_0 + d_0 + a_0, b_1 + d_1 + a_1, \dots, b_{n-2} + d_{n-2} + a_{n-2}, b_{n-1} + 2d_{n-1} + 2a_{n-1}, b_0 + 2d_0 + 2a_0, b_1 + 2d_1 + 2a_1, \\ & \dots, b_{n-2} + 2d_{n-2} + 2a_{n-2}, b_{n-1} + 3d_{n-1} + a_{n-1}, b_0 + 3d_0 + a_0, b_1 + 3d_1 + a_1, \dots, b_{n-2} + 3d_{n-2} + a_{n-2}, \\ & d_{n-1} + 2b_{n-1}, d_0 + 2b_0, d_1 + 2b_1, \dots, d_{n-2} + 2b_{n-2}). \end{aligned}$$

Now, let C be a cyclic code of length n over R . Then, $\tau(C) = C$ and $\phi(\tau(C)) = \phi(C)$. This implies that $\sigma^{(6t)}(\phi(C)) = \phi(C)$, which means that $\phi(C)$ is a linear quasi-cyclic code of length $6n$ and index 6 over $\mathbb{Z}_4$. $\square$

5. Computational Results

Recall that by Theorem 2, the ring $R_n = (\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4)_n$ is not a principal ideal ring, but Theorem 7 shows that each ideal of R_n can be generated by two elements. We carried out computer searches for cyclic codes of odd length n over R in the special case given in Theorem 7 in which generators are of the form $f_1(x) + uf_2(x) + vq_1(x)$, where f_1, f_2, q_1 are polynomials over $\mathbb{Z}_4$ and f_1 is a generator of a cyclic code of length n over $\mathbb{Z}_4$. We also considered $\mathbb{Z}_4$ images of these codes under Gray map ψ . We have found a number of new linear codes over $\mathbb{Z}_4$ with respect to Lee weight and Euclidean weight. The tables below contain some of these codes for length $n = 5$. The length of the $\mathbb{Z}_4$ -images are therefore 15. Each generator is determined by three polynomials over $\mathbb{Z}_4$. We list the coefficients of the polynomials in descending order and, for example, the polynomial $x^3 + 2x^2 + x - 1$ is represented by 1213. For a constant polynomial, we only write the constant term without trailing 0's. We considered the Lee weight and the Euclidean weight for the $\mathbb{Z}_4$ -images.

The Gray map ψ from $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$ to $\mathbb{Z}_4^3$ is defined as $\psi(a + bu + dv) = (a, b, d)A$ and

$$\phi(a + bu + dv) = (b, d, b + d + a, b + 2d + 2a, b + 3d + a, d + 2b),$$

where A is an element of $GL_3(\mathbb{Z}_4)$. For each choice of the matrix A , we get a different map ψ_A . In our search, we used three different maps. One of them is the matrix given in Example 2. We used two other matrices given by

$$B = \begin{pmatrix} 1 & 2 & 0 \\ -1 & -1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } C = \begin{pmatrix} 1 & 2 & 0 \\ -1 & -1 & -1 \\ 2 & 0 & 1 \end{pmatrix}.$$

Example 4. In the table below, we list some new linear codes over $\mathbb{Z}_4$ with respect to the Lee weight obtained from cyclic codes of length 5 over the ring $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$ under the image of ψ_A for a few different matrices A . The last column shows the parameters of the images of these cyclic codes under the map ψ_A and the minimum weight is the minimum Lee weight.

$f_1(x)$	$f_2(x)$	$q_1(x)$	Matrix	$\mathbb{Z}_4$ -Parameters (Lee weight)
00011	1	22231	A	$[15, 4^{13}2^1, 2]$
2	11113	22221	A	$[15, 4^12^9, 2]$
22222	00001	20010	B	$[15, 4^52^1, 8]$
22222	33333	33333	C	$[15, 4^12^1, 10]$
1	11111	13111	C	$[15, 4^12^9, 6]$
00011	0	13102	C	$[15, 4^92^1, 4]$

Example 5. In the table below, we list some new linear codes over $\mathbb{Z}_4$ with respect to the Euclidean weight obtained from cyclic codes of length 5 over the ring $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$ under the image of ψ_A for a few different matrices A . The last column shows the parameters of the images of these cyclic codes under the map ψ_A and the minimum weight is the minimum Euclidean weight.

$f_1(x)$	$f_2(x)$	$q_1(x)$	Matrix	$\mathbb{Z}_4$ -Parameters (Euclidean weight)
22222	0	22002	A	$[15, 4^0 2^3, 20]$
22222	2	02221	A	$[15, 4^0 2^6, 20]$
22222	2	12300	A	$[15, 4^0 2^7, 16]$
00022	11111	23030	A	$[15, 4^1 2^{12}, 8]$
00022	00011	02312	A	$[15, 4^4 2^5, 8]$
33333	2	22020	B	$[15, 4^3 2^4, 5]$
22222	00011	13313	B	$[15, 4^4 2^3, 10]$
22222	1	13102	B	$[15, 4^5 2^1, 10]$
2	00022	20202	C	$[15, 4^0 2^{10}, 12]$
2	0	10302	C	$[15, 4^0 2^{14}, 8]$
22222	11311	22200	C	$[15, 4^1 2^4, 15]$
00022	11311	33133	C	$[15, 4^1 2^8, 14]$
00022	00130	20000	C	$[15, 4^4 2^1, 14]$
2	00011	20312	C	$[15, 4^4 2^6, 8]$
22222	1	33211	C	$[15, 4^5 2^0, 13]$
33333	1	11212	C	$[15, 4^6 2^0, 9]$
3	0	13211	C	$[15, 4^{10} 2^5, 3]$

6. Conclusion

In this paper, we consider the non-Frobenius ring $R = \mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$, where $u^2 = v^2 = uv = vu = 0$ and study the cyclic codes of odd length over R . We have construct a unique set of generators for cyclic codes of odd length over R . Also, we showed that any non-principal ideal of $R[x]/\langle x^n - 1 \rangle$ is generated by certain two polynomials in $R[x]/\langle x^n - 1 \rangle$. In addition we study the rank, the dual and minimal spanning set for codes over this ring. Finally, we introduce two Gray maps, ψ and ϕ , and obtain some new linear codes with respect to the Lee weight (Euclidean weight) from cyclic codes of length 5 over R under the Gray map ψ . However, the images of these codes under the Gray map ϕ do not yield good codes over $\mathbb{Z}_4$. It would be an interesting research problem to consider the study of cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$ of even lengths and the study of cyclic codes of an arbitrary length n over ring $\mathbb{Z}_{2^m} + u\mathbb{Z}_{2^m} + v\mathbb{Z}_{2^m}$, where $m \geq 3$.

Acknowledgements: The authors wish to express their appreciation to the anonymous reviewers for their detailed comments and thoughtful recommendations, which greatly improved the manuscript.

Conflicts of Interest: The authors declare that they have 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] *Database of $\mathbb{Z}_4$ codes*, <http://quantumcodes.info/Z4/>.
- [2] T. Abualrub and I. Siap, *Reversible cyclic codes over $\mathbb{Z}_4$* , Australas. J. Combin. **38** (2007), 195–205.
- [3] T.A. Abualrub and R.H. Oehmke, *Cyclic codes of length 2^e over $\mathbb{Z}_4$* , Discrete Appl. Math. **128** (2003), no. 1, 3–9.
[https://doi.org/10.1016/S0166-218X\(02\)00432-8](https://doi.org/10.1016/S0166-218X(02)00432-8).
- [4] N. Aydin and T. Asamov, *A database of $\mathbb{Z}_4$ -codes*, J. Combin. Info. System Sci. **34** (2009), no. 1-4, 1–12.
- [5] N. Aydin, Y. Lu, and V. Onta, *An updated database of $\mathbb{Z}_4$ codes and an open problem about quasi-cyclic Codes*, Codes, Cryptology and Information Security (C2SI 2023) (S. El-Hajji, S. Mesnager, and E.M. Souidi, eds.), Lecture Notes in Computer Science, vol. 13874, Springer, 2023.
- [6] B. Çalıskan, N. Aydin, and P. Liu, *Skew cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$* , Cryptogr. Commun. **15** (2023), no. 4, 845–858.
<https://doi.org/10.1007/s12095-023-00645-3>.
- [7] H.S. Choi and B. Kim, *Various structure of cyclic codes over the non-frobenius ring $F_p[u, v]/\langle u^2, v^2, uv, vu \rangle$* , Adv. Math. Commun. **18** (2024), no. 2, 304–327.
<https://doi.org/10.3934/amc.2023030>.
- [8] S.T. Dougherty, J. Kim, H. Kulosman, and H. Liu, *Self-dual codes over commutative Frobenius rings*, Finite Fields Appl. **16** (2010), no. 1, 14–26.
<https://doi.org/10.1016/j.ffa.2009.11.004>.
- [9] S.T. Dougherty and H. Liu, *Independence of vectors in codes over rings*, Des. Codes Cryptogr. **51** (2009), 55–68.
<https://doi.org/10.1007/s10623-008-9243-1>.
- [10] M. Greferath and S.E. Schmidt, *Finite-ring combinatorics and Macwilliams equivalence theorem*, J. Combin. Theory Ser. A **92** (2000), no. 1, 17–28.
<https://doi.org/10.1006/jcta.1999.3033>.
- [11] A.R. Hammons, P.V. Kumar, A.R. Calderbank, 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.
<https://doi.org/10.1109/18.312154>.
- [12] W.C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, New York, 2003.
- [13] H. Islam and O. Prakash, *A study of cyclic and constacyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$* , Int. J. Inf. Coding Theory **5** (2018), no. 2, 155–168.
<https://doi.org/10.1504/IJICOT.2018.095017>.
- [14] B.R. McDonald, *Finite Rings with Identity*, Marcel Dekker, New York, 1974.
- [15] M. Özen, N.T. Özzaim, and N. Aydin, *Cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4 + u^2\mathbb{Z}_4$* , Turkish J. Math. **41** (2017), 1235–1247.
<https://doi.org/10.3906/mat-1602-35>.

- [16] K. Samie and M.R. Alimoradi, *Cyclic codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2$* , Comput. Appl. Math. **37** (2018), no. 3, 2489–2502.
- [17] M. Shi, L. Qian, L. Sok, N. Aydin, and P. Solé, *On constacyclic codes over $\mathbb{Z}_4[u]/\langle u^2 - 1 \rangle$ and their gray images*, Finite Fields Appl. **45** (2017), 86–95.
<https://doi.org/10.1016/j.ffa.2016.11.016>.
- [18] J. Wood, *Duality for modules over finite rings and applications to coding theory*, Amer. J. Math. **121** (1999), no. 3, 555–575.
- [19] 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.
<https://doi.org/10.1016/j.ffa.2013.12.007>.