Asia Pac. J. Math. 2026 **13**:106

ON THE STRUCTURE OF CONSTACYCLIC CODES OVER $\mathbb{Z}_4[w]/<w^2-2w>$

JOEL KABORE[1,*], MOUSSA PILABRE[2], IDRISSA KABORE[2]

[1]Department of Mathematics, Université Joseph KI-ZERBO, Burkina Faso

[2]Department of Mathematics, Université Nazi BONI, Burkina Faso

[*]Corresponding author: jokabore@yahoo.fr

Received Jun. 3, 2026

Abstract. In this paper, we investigate constacyclic codes over the ring $\mathfrak{R} := \mathbb{Z}_4[w]/<w^2-2w>$. Minimal spanning sets are provided for cyclic codes over $\mathfrak{R}$ and extended to constacyclic codes using a ring isomorphism. We introduce a new Gray map and show that $\mathbb{Z}_4$-images of constacyclic codes over $\mathfrak{R}$ are permutation equivalent to quasi-cyclic codes.

2020 Mathematics Subject Classification. 13F20; 94B15; 94B60.

Key words and phrases. constacyclic codes; gray map; quasi-cyclic codes.

1. Introduction

Constacyclic codes over rings have attracted significant attention in recent years [6,9–11,16]. Beyond finite fields, the ring of integers modulo 4, denoted by $\mathbb{Z}_4$, is the first ring that has received particular interest in the study of codes. This is due to the observation that certain nonlinear binary codes can be obtained as Gray images of codes defined over $\mathbb{Z}_4$ [7]. Later, cyclic codes and their Gray images have been extensively explored [1,18,20]. This ring belongs to the class of Frobenius rings, which is considered the broadest class of rings suitable for coding theory, as it provides an optimal framework for the study of codes [21].

Local Frobenius rings of order 16 have been classified, and various Gray maps have been provided by Martinez-Moro et al. in [13]. Many studies on linear codes, constacyclic codes, and related structures have been conducted over these rings. Cyclic and constacyclic codes over $\mathbb{Z}_4+u\mathbb{Z}_4$, where $u^2=0$ have been studied in [5, 8, 22] and Gray images of these codes have been explored using various Gray maps. In [17], Ozen et al. determine the structure of cyclic codes and explore Gray images of $(1+2u)$-constacyclic codes over $\mathbb{Z}_4[v]/<v^2-1>$. Later, in [19], Shi et al. extend the study of $(1+2u)$-constacyclic codes over $\mathbb{Z}_4[v]/<v^2-1>$ introducing a new Gray map. In all these works, some new optimal codes have been computed. Recently Aydin et al. investigated cyclic and constacyclic

DOI: 10.28924/APJM/13-106

codes over $\mathbb{Z}_4 + w\mathbb{Z}_4$, where $w^2 = 2$ [2]. Using new introduced Gray maps, these authors constructed new linear codes over $\mathbb{Z}_4$. In this work, we consider the local Frobenius ring $\mathbb{Z}_4 + w\mathbb{Z}_4$, where $w^2 = 2w$. This ring is used in [4,14] for study of linear codes. Self-duality properties and MacWilliams identities have been investigated.

This paper is structured as follows. In Section 2, we recall some basic properties about the ring $\mathbb{Z}_4 + w\mathbb{Z}_4$, where $w^2 = 2w$, constacyclic codes and introduce a new Gray map. In Section 3, we describe generators and provide minimal spanning sets of cyclic codes of odd length over this ring. In Section 4, we explore constacyclic codes using a ring isomorphism. The Gray images of all constacyclic codes are also investigated.

2. Preliminaries

Throughout this paper, $\mathfrak{R}$ denotes the ring $\mathbb{Z}_4[w]/ < w^2 - 2w > := \{a + wb \mid a, b \in \mathbb{Z}_4\}$, where $\mathbb{Z}_4$ is the ring of integers modulo 4. The ring $\mathfrak{R}$ has 5 nontrivial ideals which are $< 2w >, < 2 >, < w >, < 2+w >$ and the maximal ideal $< 2, w >$. The set of units of $\mathfrak{R}$ is given by:

$$U(\mathfrak{R}) = \{a + wb \mid a \text{ is a unit in } \mathbb{Z}_4\} = \{1, 3, 1 + w, 1 + 2w, 1 + 3w, 3 + w, 3 + 2w, 3 + 3w\}.$$

A code $\mathcal{C}$ of length n over $\mathfrak{R}$ is a nonempty subset of R^n. If, in addition, the code is a $\mathfrak{R}$-submodule of $\mathfrak{R}^n$, it is called linear code.

For a given unit $\Lambda \in \mathfrak{R}$, we define the Λ-constacyclic shift τ_Λ on $\mathfrak{R}^n$ by:

$$\tau_\Lambda(r_0, ..., r_{n-1}) = (\Lambda r_{n-1}, r_0, ..., r_{n-2}).$$

A linear code which is invariant under the Λ-constacyclic shift τ_Λ is said to be Λ-constacyclic code. For $\Lambda = 1$, Λ-constacyclic codes are called cyclic codes. A Λ-constacyclic code of length n over $\mathfrak{R}$ can be identified with ideals of $\mathfrak{R}[x]/ < x^n - \Lambda >$ by the identification:

$$(r_0, r_1, ..., r_{n-1}) \longmapsto r_0 + r_1 x + ... r_{n-1} x^{n-1}.$$

We define the Gray map on $\mathfrak{R}$ by:

$$\begin{array}{cccc} \psi : & \mathfrak{R} & \longrightarrow & \mathbb{Z}_4^2 \\ & a + bw & \longmapsto & (a + 2b, 3a + 2b) \end{array}$$

and extend it on $\mathfrak{R}^n$ as follows:

$$\begin{array}{cccc} \Psi : & \mathfrak{R}^n & \longrightarrow & \mathbb{Z}_4^{2n} \\ & (r_0, r_1, \cdots, r_{n-1}) & \longmapsto & (a_0 + 2b_0, 3a_0 + 2b_0, \cdots, a_{n-1} + 2b_{n-1}, 3a_{n-1} + 2b_{n-1}) \end{array}$$

where $r_i = a_i + b_i w$, for all $i \in \{0, \cdots, n-1\}$. It is clear that Ψ is $\mathbb{Z}_4$-linear.
The Hamming distance between two vectors $\mathbf{a} = (a_0, \cdots, a_{n-1}),\ \mathbf{b} = (b_0, \cdots, b_{n-1}) \in \mathbb{Z}_4^n$ is defined as $d_H(\mathbf{a}, \mathbf{b}) = w_H(\mathbf{a} - \mathbf{b})$ where $w_H(\mathbf{a}) := |\{i \mid a_i \neq 0\}|$. In the same way, the Lee weight of $a \in \mathbb{Z}_4$ is

defined as $w_L(a) := \max\{|a|, |4-a|\}$ and the Lee distance between two vectors $\mathbf{a} = (a_0, \cdots, a_{n-1})$, $\mathbf{b} = (b_0, \cdots, b_{n-1}) \in \mathbb{Z}_4^n$ is defined as $d_L(\mathbf{a}, \mathbf{b}) = w_L(\mathbf{a} - \mathbf{b})$ where $w_L(\mathbf{a}) = \sum_{i=0}^{n-1} w_L(a_i)$. Now we endow $\mathfrak{R}$ with weights and distances as follows.

Definition 2.1. *The Hamming Gray weight of any element $\boldsymbol{r} \in \mathfrak{R}^n$ is defined as: $Hw_G(\boldsymbol{r}) = w_H(\Psi(\boldsymbol{r}))$, and the Hamming Gray distance between two elements $\boldsymbol{r}, \boldsymbol{s} \in \mathfrak{R}^n$ is given by: $Hd_G(\boldsymbol{r}, \boldsymbol{s}) = Hw_G(\boldsymbol{r} - \boldsymbol{s})$.*
The Lee Gray weight of any element $\boldsymbol{r} \in \mathfrak{R}^n$ is defined as: $Lw_G(\boldsymbol{r}) = w_L(\Psi(\boldsymbol{r}))$, and the Lee Gray distance between two elements $\boldsymbol{r}, \boldsymbol{s} \in \mathfrak{R}^n$ is given by: $Ld_G(\boldsymbol{r}, \boldsymbol{s}) = Lw_G(\boldsymbol{r} - \boldsymbol{s})$.

Since $Hd_G(\mathbf{r}, \mathbf{s}) = Hw_G(\mathbf{r} - \mathbf{s}) = w_H(\Psi(\mathbf{r} - \mathbf{s})) = w_H(\Psi(\mathbf{r}) - \Psi(\mathbf{s})) = d_H(\Psi(\mathbf{r}), \Psi(\mathbf{s}))$, it is obvious that Ψ is a linear distance preserving map from $(\mathfrak{R}^n, Hd_G)$ to $(\mathbb{Z}_4^{2n}, d_H)$. Similarly, Ψ is a linear distance preserving map from $(\mathfrak{R}^n, Ld_G)$ to $(\mathbb{Z}_4^{2n}, d_L)$.
The structure of cyclic codes of any length over $\mathbb{Z}_4$ is well-known [1], and can be summarized as follows.

Proposition 1. *Let $\mathcal{C}$ be a cyclic code of length n over $\mathbb{Z}_4$.*

(1) *If n is odd, then $\mathcal{C} =< g(x) + 2\jmath(x) >$, where $g(x), \jmath(x)$ are monic polynomials over $\mathbb{Z}_4$ such that $\jmath(x) \mid g(x) \mid x^n - 1$.*
(2) *If n is even, then either*
 (a) *$\mathcal{C} =< g(x) + 2p(x) >$, where $g(x) \mid x^n - 1 \mod 2$ and $g(x) + 2p(x) \mid x^n - 1 \mod 4$ or*
 (b) *$\mathcal{C} =< g(x) + 2p(x), 2\jmath(x) >$, where $g(x), \jmath(x)$, and $p(x)$ are polynomials with $g(x) \mid x^n - 1 \mod 2$, $\jmath(x) \mid p(x)(\frac{x^n-1}{g(x)}) \mod 2$ and $\deg \jmath(x) > \deg p(x)$.*

3. Structure of cyclic codes over $\mathfrak{R}$

Let $\phi : \mathfrak{R} \to \mathbb{Z}_4$ be the map defined by $\phi(a + wb) = a + 2b$. It is straightforward to see that ϕ is a ring morphism and can be extended to a morphism of polynomial rings $\varphi : \mathfrak{R}[x]/ < x^n - 1 > \longrightarrow \mathbb{Z}_4[x]/ < x^n - 1 >$ such that

$$\varphi(r_0 + r_1 x + \cdots + r_{n-1}x^{n-1}) = \phi(r_0) + \phi(r_1)x + \cdots + \phi(r_{n-1})x^{n-1}.$$

Let $\mathcal{C}$ be a cyclic code of odd length n over $\mathfrak{R}$. Then $\varphi(\mathcal{C})$ is an ideal of $\mathbb{Z}_4[x]/ < x^n - 1 >$ and from Proposition 1, we get $\varphi(\mathcal{C}) =< h_1(x) >$, where $h_1 = g_1(x) + 2\jmath_1(x)$; and $g_1(x),\ \jmath_1(x)$ are monic polynomials over $\mathbb{Z}_4$ such that $\jmath_1(x) \mid g_1(x) \mid x^n - 1$.
It is clear that

$$\ker \varphi = \{(2 + w)k(x) \in \mathcal{C} \mid k(x) \in \mathbb{Z}_4[x]\}.$$

Let

$$\kappa := \{k(x) \in \mathbb{Z}_4[x]/ < x^n - 1 > \mid (2 + w)k(x) \in \ker \varphi\}.$$

It is obvious that κ is an ideal of $\mathbb{Z}_4[x]/ < x^n - 1 >$, then $\kappa =< h_2 >$, where $h_2 = g_2(x) + 2\jmath_2(x)$; and $g_2(x),\ \jmath_2(x)$ are monic polynomials over $\mathbb{Z}_4$ such that $\jmath_2(x) \mid g_2(x) \mid x^n - 1$. From the above discussion, we deduce the following result.

Theorem 1. *Let $\mathcal{C}$ be a cyclic code of odd length n over $\mathfrak{R}$, then*

$$\mathcal{C} =< h_1(x) + (2+w)\hbar(x), (2+w)h_2(x) >,$$

where $h_1 = g_1(x) + 2\jmath_1(x),\ h_2 = g_2(x) + 2\jmath_2(x)$;and $\hbar_1(x) \in \mathbb{Z}_4[x], g_1, g_2,\ \jmath_1, \jmath_2$ are monic polynomials over $\mathbb{Z}_4$ such that $\jmath_1(x) \mid g_1(x) \mid x^n - 1$ and $\jmath_2(x) \mid g_2(x) \mid x^n - 1$.

When the generator of cyclic codes over $\mathbb{Z}_4[x]$ is regular, we will see that some additional conditions can be added on the structure of cyclic codes over $\mathfrak{R}$.
We recall that two polynomials $g(x), h(x) \in \mathbb{Z}_4[x]$ are said to be associated if $g(x) = \epsilon(x)h(x)$, where $\epsilon(x)$ is a unit in $\mathbb{Z}_4[x]$. It is well-known that a regular polynomial over $\mathbb{Z}_4[x]$ can be associated to a monic polynomial (see [15], Theorem XIII.6), so it is sufficient to work with monic polynomials rather than with regular polynomials. In the sequel, we suppose that generator polynomials of cyclic codes over $\mathbb{Z}_4[x]$, $h_1(x)$ and $h_2(x)$ are monic.

Lemma 1. *Let $\mathcal{C} =< h_1(x) + (2+w)\hbar(x), (2+w)h_2(x) >$ be a cyclic code of length n over $\mathfrak{R}$, then we can assume that $h_2 \mid 2h_1$ and $\deg \hbar < \deg h_2 \leq \deg h_1$.*

Proof. Since $\mathcal{C}$ is cyclic, then $2w(h_1(x) + (2+w)\hbar(x)) = 2wh_1 = (2+w)(2h_1) \in \ker \varphi$. Then $2h_1 \in \kappa$ and $h_2 \mid 2h_1$. Since h_1 and h_2 are monic, then $\deg h_2 \leq \deg h_1$.

Suppose that $\deg \hbar \geq \deg h_2$. By the algorithm division, there exist $q, r \in \mathbb{Z}_4[x]$ such that $\hbar(x) = q(x)h_2(x) + r(x)$, where $\deg r < \deg h_2$. Then

$$\begin{aligned} \mathcal{C} &=< h_1(x) + (2+w)\hbar(x), (2+w)h_2(x) > \\ &=< h_1(x) + (2+w)q(x)h_2(x) + (2+w)r(x), (2+w)h_2(x) > \\ &=< h_1(x) + (2+w)r(x), (2+w)h_2(x) >, \end{aligned}$$

hence we can assume that $\deg \hbar < \deg h_2$. □

Lemma 2. *If $\deg h_1 = \deg h_2$, then $\mathcal{C} =< h_1(x) + (2+w)\hbar(x) >$, where $\deg \hbar(x) < \deg h_1(x)$ and $h_1(x) + (2+w)\hbar(x) \mid x^n - 1$.*

Proof. Suppose that $\deg h_1 = \deg h_2$. Since $h_2 \mid 2h_1$, we get $2h_1 = \beta h_2$, where $\beta \in \mathbb{Z}_4$. Since h_1 and h_2 are monic, we get $\beta = 2$ and $h_1 = \epsilon h_2 + 2q$, where ϵ is a unit in $\mathbb{Z}_4$ and $\deg q \leq \deg h_2$. Since $\mathcal{C}$ is cyclic,

$$\begin{aligned} (2+w)(h_1 + (2+w)\hbar(x)) &= (2+w)h_1 + 2w\hbar(x) \\ &= (2+w)h_2 + 2w(q(x) + \hbar(x)) \in \mathcal{C}. \end{aligned}$$

This implies that $2w(q(x)+\hbar(x)) \in \mathcal{C}$ with $\deg(q(x)+\hbar(x)) < \deg h_2$. Then $q(x)+\hbar(x) = 0$ and $(2+w)(h_1+(2+w)\hbar(x)) = (2+w)h_2$. Hence $\mathcal{C} =< h_1(x)+(2+w)\hbar(x) >$.
Using the division algorithm, we get

$$x^n - 1 = (h_1(x)+(2+w)\hbar(x))\mathbf{q}(x) + \mathbf{r}(x),$$

where $\deg \mathbf{r} \leq \deg h_1$. Then $\mathbf{r}(x) \in \mathcal{C}$, hence $\mathbf{r}(x) = 0$ and $h_1(x)+(2+w)\hbar(x) \mid x^n - 1$. □

Lemma 3. *If h_1 and h_2 are associated polynomials in $\mathbb{Z}_4[x]$, then $\mathcal{C} =< h_1(x)+2wl(x) >$, where l is a binary polynomial and $h_1(x)+2wl(x) \mid x^n - 1$.*

Proof. Suppose that $h_1(x) = \epsilon(x)h_2(x)$, where $\epsilon(x)$ is a unit in $\mathbb{Z}_4[x]$. Since $\mathcal{C}$ is cyclic, then

$$\begin{aligned}(2+w)(h_1(x)+(2+w)\hbar(x)) &= (2+w)h_1(x)+2w\hbar(x)\\ &= \epsilon(x)(2+w)h_2(x)+2w\hbar(x) \in \mathcal{C}.\end{aligned}$$

This implies that $2w\hbar(x) = 2(2+w)\hbar(x) \in \mathcal{C}$ and $2\hbar(x) \in \kappa$. Therefore $h_2(x) \mid 2\hbar(x)$ hence $h_1(x) \mid 2\hbar(x)$. Since $\deg 2\hbar(x) \leq \deg \hbar(x) < \deg h_1$, then $2\hbar(x) = 0$ and $\hbar(x) = 2l(x)$, where $l(x)$ is a binary polynomial. We get $h_1+(2+w)\hbar(x) = h_1+2wl(x)$. Moreover $(2+w)(h_1+2wl(x)) = (2+w)h_1(x) = \epsilon(x)(2+w)h_2(x)$, then $(2+w)h_2(x) \in< h_1(x)+2wl(x) >$ and $\mathcal{C} =< h_1(x)+2wl(x) >$.
Using reasoning similar to that of the proof of the Lemma 2, we obtain that $h_1(x)+2wl(x) \mid x^n - 1$. □

Theorem 2. *Let $\mathcal{C} =< \mathfrak{g}(x) >$ be a cyclic code of odd length n, where $\mathfrak{g} \mid x^n - 1$. Then $\mathcal{C}$ is a free, where its rank is $n - \deg \mathfrak{g}$ and its basis is $\mathcal{B} = \{\mathfrak{g}, x\mathfrak{g}, \cdots, x^{n-\deg \mathfrak{g}-1}\mathfrak{g}\}$.*

Proof. Let $\deg \mathfrak{g} = t$, since $\mathfrak{g}(x) \mid x^n - 1$, there exists $\hat{\mathfrak{g}}(x) \in \mathfrak{R}[x]$ where $\deg \hat{\mathfrak{g}}(x) = n - t$ such that $x^n - 1 = \mathfrak{g}(x)\hat{\mathfrak{g}}(x)$. Let $c(x) = k(x)\mathfrak{g}(x) \in \mathcal{C}$. Suppose that $\deg k(x) \geq n - t$, then by the division algorithm, there exist polynomials $\mathbf{q}(x), \mathbf{r}(x)$ such that $k(x) = \hat{\mathfrak{g}}(x)\mathbf{q}(x)+\mathbf{r}(x)$, where $\deg \mathbf{r}(x) \leq n-t-1$. This implies that

$$c(x) = k(x)\mathfrak{g}(x) = (\hat{\mathfrak{g}}(x)\mathbf{q}(x)+\mathbf{r}(x))\mathfrak{g}(x) = \mathbf{r}(x)\mathfrak{g}(x),$$

then $\mathcal{B}$ spans $\mathcal{C}$. Now, we check that $\mathcal{B}$ is linearly independant.

Let $\lambda_0, \lambda_1, \cdots, \lambda_{n-t-1} \in \mathfrak{R}$ such that

$$\lambda_0\mathfrak{g}(x) + \lambda_1 x\mathfrak{g}(x) + \cdots + \lambda_{n-t-1}x^{n-t-1}\mathfrak{g}(x) = 0.$$

Since $\mathfrak{g}(x) \mid x^n - 1$, then the constant term of $\mathfrak{g}(x)$ denoted by g_0 is a unit. By comparing coefficients of the above equation, we get: $g_0\lambda_0 = 0$, thus $\lambda_0 = 0$ and

$$\lambda_1 x\mathfrak{g}(x) + \cdots + \lambda_{n-t-1}x^{n-t-1}\mathfrak{g}(x) = x(\lambda_1\mathfrak{g}(x) + \cdots + \lambda_{n-t-1}x^{n-t-2}\mathfrak{g}(x)) = 0.$$

This implies that $\lambda_1\mathfrak{g}(x)+\cdots+\lambda_{n-t-1}x^{n-t-2}\mathfrak{g}(x) = 0$ Similarly, we get $\lambda_i = 0$, $\forall\, i \in \{0, 1, \cdots, n-t-1\}$. Therefore $\mathcal{B}$ is linearly independant, hence it forms a basis of $\mathcal{C}$. □

Theorem 3. *Let $\mathcal{C} =< h_1(x) + (2+w)\hbar(x), (2+w)h_2(x) >$ be a cyclic code of length n over $\mathfrak{R}$, where $t_1 = \deg h_1 > t_2 = \deg h_2$. Then the rank of $\mathcal{C}$ is $n - t_2$ and a minimal spanning set of $\mathcal{C}$ is given by*

$$\begin{aligned}\mathcal{B} = \ & \{h_1(x) + (2+w)\hbar(x), x(h_1(x) + (2+w)\hbar(x)), \cdots, x^{n-t_1-1}(h_1(x) + (2+w)\hbar(x)), \\ & (2+w)h_2(x), x(2+w)h_2(x), \cdots, x^{t_1-t_2-1}(2+w)h_2(x)\}.\end{aligned}$$

Proof. It is obvious that

$$\begin{aligned}& \{h_1(x) + (2+w)\hbar(x), x(h_1(x) + (2+w)\hbar(x)), \cdots, x^{n-t_1-1}(h_1(x) + (2+w)\hbar(x)), \\ & (2+w)h_2(x), x(2+w)h_2(x), \cdots, x^{n-t_2-1}(2+w)h_2(x)\}\end{aligned}$$

is a generating set for $\mathcal{C}$. Using the division algorithm, we get $\forall i \geq 0$,

$$x^{t_1-t_2+i}(2+w)h_2 = (h_1 + (2+w)\hbar(x))\mathbf{q}(x) + \mathbf{r}(x),$$

where $\deg \mathbf{r} < t_1$. Since $\mathcal{C}$ is cyclic, then $\mathbf{r} \in \mathcal{C}$ and can be represented as

$$\mathbf{r}(x) = l_1(x)(h_1(x) + (2+w)\hbar(x)) + l_2(x)(2+w)h_2(x).$$

Then $l_1 = 0$ and $\mathbf{r}(x) = l_2(2+w)h_2$. Since h_2 is monic, we get $\deg \mathbf{r} = \deg l_2 + \deg h_2$ and $\deg l_2 < t_1 - t_2$. Therefore $x^{t_1-t_2+i}(2+w)h_2 \in$ span$(\mathcal{B})$.

Now we show that $\mathcal{B}$ is modular independant and independant.

Let $\lambda_0, \lambda_1, \cdots, \lambda_{n-t_1-1}, \gamma_0, \gamma_1, \cdots, \gamma_{t_1-t_2-1} \in \mathfrak{R}$ such that

$$\sum_{i=0}^{n-t_1-1} \lambda_i x^i (h_1 + (2+w)\hbar(x)) + \sum_{i=0}^{t_1-t_2-1} \gamma_i x^i (2+w)h_2 = 0.$$

Let $h_1 + (2+w)\hbar = x^{t_1} + a_{t_1-1}x^{t_1-1} + \cdots + a_0$ and $h_2 = x^{t_2} + b_{t_2-1}x^{t_2-1} + \cdots + b_0$. Comparing the coefficients of x^{n-1}, we get $\lambda_{n-t_1-1} = 0$. Comparing the coefficients of x^{n-2}, we get $\lambda_{n-t_1-1}a_{t_1-2} + \lambda_{n-t_1-2} = 0$, then $\lambda_{n-t_1-2} = 0$. By continuing this process with the coefficients of $x^{n-3}, \cdots, x^{t_1}$, we get $\lambda_j = 0, \ \forall\, j \in \{0, \cdots, n - t_1 - 1\}$. Then, we obtain

$$\sum_{i=0}^{t_1-t_2-1} \gamma_i x^i (2+w)h_2 = 0.$$

Comparing the coefficients of x^{t_1-1}, we get $(2+w)\gamma_{t_1-t_2-1} = 0$, this implies that $\gamma_{t_1-t_2-1} \in \{0, w, 2w, 2+2w\} \subset \mathfrak{m}$, where $\mathfrak{m}$ is the maximal ideal of $\mathfrak{R}$. Comparing the coefficients of x^{t_1-2}, we get $\gamma_{t_1-t_2-1}(2+w)b_{t_2-1} + \gamma_{t_1-t_2-2}(2+w) = 0$. This implies that $\gamma_{t_1-t_2-2}(2+w) = 0$, hence $\gamma_{t_1-t_2-2} \in \{0, w, 2w, 2+2w\}$. By continuing this process with the coefficients of $x^{t_1-3}, \cdots, x, x^0$, we get $\gamma_j \in \{0, w, 2w, 2+2w\}, \ \forall\, j \in \{0, \cdots, t_1 - t_2 - 1\}$. Then $\mathcal{B}$ is modular independant. Moreover, since $\gamma_i \in \{0, w, 2w, 2+2w\}, \ \forall\, i \in \{0, \cdots, t_1 - t_2 - 1\}$, $\lambda_i = 0, \ \forall\, i \in \{0, \cdots, n - t_1 - 1\}$, and

$$\sum_{i=0}^{n-t_1-1} \lambda_i x^i (h_1 + (2+w)\hbar(x)) + \sum_{i=0}^{t_1-t_2-1} \gamma_i x^i (2+w)h_2 = 0,$$

we deduce that $\lambda_i x^i(h_1 + (2+w)\hbar(x)) = 0$ and $\gamma_j x^j(2+w)h_2 = 0$, for all $i \in \{0, \cdots, n-t_1-1\}$, and $j \in \{0, \cdots, t_1 - t_2 - 1\}$; then $\mathcal{B}$ is independant. □

4. Constacyclic codes and gray images

Let $\mathfrak{L}$ be the ring homomorphism defined by

$$\begin{array}{rccc} \mathfrak{L}: & \frac{\mathfrak{R}[x]}{<x^n-1>} & \longrightarrow & \frac{\mathfrak{R}[x]}{<x^n-\Lambda>} \\ & \mathbf{r}(x) & \longmapsto & \mathbf{r}(\Lambda x). \end{array}$$

Let $\mathbf{r}_1(x), \mathbf{r}_2(x) \in \mathfrak{R}[x]/ < x^n - 1 >$ such that $\mathbf{r}_1(x) = \mathbf{r}_2(x) + < x^n - 1 >$. Since $\lambda^2 = 1$ and n is odd, we have

$$\begin{aligned} \mathfrak{L}(\mathbf{r}_1(x)) &= \mathbf{r}_1(\Lambda x) = \mathbf{r}_2(\Lambda x) + < (\Lambda x)^n - 1 > \\ &= \mathbf{r}_2(\Lambda x) + < (\Lambda x)^n - 1 > \\ &= \mathbf{r}_2(\Lambda x) + < \Lambda x^n - 1 > \\ &= \mathbf{r}_2(\Lambda x) + < \Lambda^{-1}(x^n - \Lambda) > \\ &= \mathbf{r}_2(\Lambda x) + < x^n - \Lambda > . \end{aligned}$$

Consequently, we deduce the following result.

Lemma 4. *Any constacyclic code of odd length n over $\mathfrak{R}$ is equivalent to a cyclic code of length n over $\mathfrak{R}$.*

With vector representation, the ring isomorphism $\mathfrak{L}$ is equivalent to

$$\begin{array}{rccc} \mathfrak{L}: & \mathfrak{R}^n & \longrightarrow & \mathfrak{R}^n \\ & (r_0, \cdots, r_{n-1}) & \longmapsto & (r_0, \lambda r_1, \cdots, \lambda r_{n-2}, r_{n_1}). \end{array}$$

By the above lemma, the following result is obvious.

Theorem 4. *Let $\mathcal{C}$ be a Λ-constacyclic code of odd length n over $\mathfrak{R}$, then*

$$\mathcal{C} =< h_1(\Lambda x) + (2+w)\hbar(\Lambda x), (2+w)h_2(\Lambda x) >,$$

where $h_1 = g_1(x) + 2\jmath_1(x)$, $h_2 = g_2(x) + 2\jmath_2(x)$; and $\hbar_1(x) \in \mathbb{Z}_4[x]$, g_1, $\jmath_1$, g_2, $\jmath_2$ are monic polynomials over $\mathbb{Z}_4$ such that $\jmath_1(x) \mid g_1(x) \mid x^n - 1$ and $\jmath_2(x) \mid g_2(x) \mid x^n - 1$.

A code $\mathfrak{C}$ of length $2n$ over $\mathbb{Z}_4$ is called a 2-quasi-cyclic code if

$$\tau_2(c) = (a_{n-1}, b_{n-1}, a_0, b_0, \cdots, a_{n-2}, b_{n-2}) \in \mathfrak{C}$$

whenever

$$c = (a_0, b_0, a_1, b_1, \cdots, a_{n-1}, b_{n-1}) \in \mathfrak{C}, \ \forall\, c \in \mathfrak{C}.$$

The following results characterize Gray images of constacyclic codes over $\mathfrak{R}$.

Theorem 5. *Let $\mathcal{C}$ be a Λ-constacyclic code of length n over $\mathfrak{R}$. Then $\Psi(\mathcal{C})$ is*

- *a 2-quasi-cyclic code of length $2n$ over $\mathbb{Z}_4$ if $\Lambda \in \{1, 1+2w, 3+w, 3+3w\}$ or*

- *a permutation equilavent to a 2-quasi-cyclic code of length $2n$ if $\Lambda \in \{3, 3+2w, 1+w, 1+3w\}$.*

Proof. Let $\mathcal{C}$ be a Λ- constacyclic code of length n over $\mathfrak{R}$ and $c = (c_0, \cdots, c_{n-1}) \in \mathcal{C}$, where $c_i = a_i + b_i w$ for all $i \in \{0, \cdots, n-1\}$.

It is easy to check that $\Psi(\Lambda(a_i + b_i w)) = (a_i + 2b_i, 3a_i + 2b_i)$ if $\Lambda \in \{1, 1+2w, 3+w, 3+3w\}$ and $\Psi(\Lambda(a_i + b_i w)) = (3a_i + 2b_i, a_i + 2b_i)$ if $\Lambda \in \{3, 3+2w, 1+w, 1+3w\}$. We first consider $\Lambda \in \{1, 1+2w, 3+w, 3+3w\}$. We have

$$\begin{aligned}\Psi(\tau_\Lambda(c)) &= \Psi(\lambda c_{n-1}, c_0, \cdots, c_{n-2})\\ &= (a_{n-1} + 2b_{n-1}, 3a_{n-1} + 2b_{n-1}, a_0 + 2b_0, 3a_0 + 2b_0,\\ &\quad \cdots, a_{n-2} + 2b_{n-2}, 3a_{n-2} + 2b_{n-2})\end{aligned}$$

and

$$\begin{aligned}\tau_2(\Psi(c)) &= \tau_2(a_0 + 2b_0, 3a_0 + 2b_0, \cdots, a_{n-1} + 2b_{n-1}, 3a_{n-1} + 2b_{n-1})\\ &= (a_{n-1} + 2b_{n-1}, 3a_{n-1} + 2b_{n-1}, a_0 + 2b_0, 3a_0 + 2b_0,\\ &\quad \cdots, a_{n-2} + 2b_{n-2}, 3a_{n-2} + 2b_{n-2}).\end{aligned}$$

Hence $\Psi(\tau_\Lambda(c)) = \tau_2(\Psi(c))$. Since $\mathcal{C}$ is a Λ-constacyclic code, then $\Psi(\tau_\Lambda(\mathcal{C})) = \Psi(\mathcal{C}) = \tau_2(\Psi(\mathcal{C}))$.

Similarly, we get $\Psi(\tau_\Lambda(c)) = \sigma_n(\tau_2(\Psi(c)))$ if $\Lambda \in \{3, 3+2w, 1+w, 1+3w\}$, where σ_n is the permutation on $\mathbb{Z}_4^{2n}$ defined by $\sigma_n(\upsilon_0, \cdots, \upsilon_{2n-1}) = (\upsilon_{\sigma(0)}, \cdots, \upsilon_{\sigma(2n-1)})$, with the permutation $\sigma = (0\ 1)$ of $\{0, 1, \cdots, 2n-1\}$. $\square$

Theorem 6. *Let $\mathcal{C}$ be a cyclic code of length n and $\mathfrak{L}(\mathcal{C})$ be the corresponding Λ-constacyclic code using the ring isomorphism $\mathfrak{L}$.*

(1) *If $\Lambda \in \{1, 1+2w, 3+w, 3+3w\}$, then $\Psi(\mathfrak{L}(\mathcal{C})) = \Psi(\mathcal{C})$.*

(2) *If $\Lambda \in \{3, 3+2w, 1+w, 1+3w\}$, then $\Psi(\mathfrak{L}(\mathcal{C})) = \pi_n(\Psi(\mathcal{C}))$, where π_n is the permutation on $\mathbb{Z}_4^{2n}$ defined by $\pi_n(\upsilon_0, \cdots, \upsilon_{2n-1}) = (\upsilon_{\pi(0)}, \cdots, \upsilon_{\pi(n-1)})$, with the permutation $\pi = (2\ 3)(6\ 7)\cdots(4n+2\ 4n+3)\cdots(2n-4\ 2n-3)$ of $\{0, 1, \cdots, 2n-1\}$.*

Proof. Let $c \in \mathcal{C}$ and $\Lambda \in \{1, 1+2w, 3+w, 3+3w\}$. We have

$$\begin{aligned}\Psi(\mathfrak{L}(c)) &= \Psi(c_0, \Lambda c_1, \cdots, \Lambda c_{n-2}, c_{n_1})\\ &= (a_0 + 2b_0, 3a_0 + 2b_0, \cdots, a_{n-1} + 2b_{n-1}, 3a_{n-1} + 2b_{n-1})\\ &= \Psi(c);\end{aligned}$$

where $c_i = a_i + b_i w$ for all $i \in \{0, 1, \cdots, n-1\}$.

If $\Lambda \in \{3, 3+2w, 1+w, 1+3w\}$, we have

$$\begin{aligned}\Psi(\mathfrak{L}(c)) &= \Psi(c_0, \Lambda c_1, \cdots, \Lambda c_{n-2}, c_{n-1})\\ &= (a_0 + 2b_0, 3a_0 + 2b_0, 3a_1 + 2b_1, a_1 + 2b_1,\\ &\quad \cdots, a_{n-1} + 2b_{n-1}, 3a_{n-1} + 2b_{n-1})\\ &= \pi_n(\Psi(c)),\end{aligned}$$

where $c_i = a_i + b_i w$ for all $i \in \{0, 1, \cdots, n-1\}$.

□

5. Conclusion

This paper has explored the structure of constacyclic codes over the ring $\mathfrak{R} := \mathbb{Z}_4[w]/ < w^2 - 2w >$. We have determined generators and minimal spanning sets for cyclic codes and have deduced the structure of constacyclic codes using a ring isomorphism. We have defined a new Gray map and have shown that the Gray images of constacyclic codes of length n over $\mathfrak{R}$ are permutation equivalent to 2-quasi-cyclic codes of length $2n$ over $\mathbb{Z}_4$.

Conflicts of Interest. The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

[1] T. Abualrub, I. Siap, Reversible Cyclic Codes over $\mathbb{Z}_4$, Australas. J. Comb. 38 (2007), 195–205.

[2] N. Aydin, Y. Cengellenmis, A. Dertli, On Some Constacyclic Codes over $\mathbb{Z}_4[u]/ < u^2 - 1 >$, Their $\mathbb{Z}_4$-Images and New Codes, Des. Codes Cryptogr. 86 (2018), 1249–1255. https://doi.org/10.1007/s10623-017-0392-y.

[3] N. Aydin, Y. Cengellenmis, A. Dertli, Cyclic and Constacyclic Codes over $\mathbb{Z}_4 + w\mathbb{Z}_4$, Bull. Korean Math. Soc. 61 (2024), 1447–1457. https://doi.org/10.4134/BKMS.b210265.

[4] R.K. Bandi, M. Bhaintwal, Self-dual Codes over $\mathbb{Z}_4 + w\mathbb{Z}_4$, Discrete Math. Algorithms Appl. 7 (2015), 1550014. https://doi.org/10.1142/S1793830915500147.

[5] R.K. Bandi, M. Bhaintwal, A Note on Cyclic Codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$, Discrete Math. Algorithms Appl. 8 (2016), 1650017. https://doi.org/10.1142/S1793830916500178.

[6] A. Batoul, K. Guenda, T.A. Gulliver, Some Constacyclic Codes Over Finite Chain Rings, Adv. Math. Commun. 10 (2016), 683–694. https://doi.org/10.3934/amc.2016034.

[7] A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, P. Sole, The $\mathbb{Z}_4$-Linearity of Kerdock, Preparata, Goethals, and Related Codes, IEEE Trans. Inf. Theory 40 (1994), 301–319. https://doi.org/10.1109/18.312154.

[8] Y. Cengellenmis, A. Dertli, N. Aydın, Some Constacyclic Codes over $\mathbb{Z}_4[u]/ < u^2 >$, New Gray Maps, and New Quaternary Codes, Algebr. Colloq. 25 (2018), 369–376. https://doi.org/10.1142/s1005386718000263.

[9] M. Charkani, J. Kabore, Primitive Idempotents and Constacyclic Codes Over Finite Chain Rings, Gulf J. Math. 8 (2020), 55–67. https://doi.org/10.56947/gjom.v8i2.434.

[10] H.Q. Dinh, S.R. Lopez-Permouth, Cyclic and Negacyclic Codes Over Finite Chain Rings, IEEE Trans. Inf. Theory 50 (2004), 1728–1744. https://doi.org/10.1109/tit.2004.831789.

[11] S.T. Dougherty, Algebraic Coding Theory Over Finite Commutative Rings, Springer, 2017. https://doi.org/10.1007/978-3-319-59806-2.

[12] S.T. Dougherty, A. Kaya, E. Saltürk, Cyclic Codes Over Local Frobenius Rings of Order 16, Adv. Math. Commun. 11 (2017), 99–114. https://doi.org/10.3934/amc.2017005.

[13] E. Martínez-Moro, S. Szabo, On Codes Over Local Frobenius Non-Chain Rings of Order 16, Contemp. Math. 634 (2015), 227–241. https://doi.org/10.1090/conm/634/12702.

[14] E.M. Moro, S. Szabo, B. Yildiz, Linear Codes over $\frac{\mathbb{Z}_4[x]}{<x^2+2x>}$, Int. J. Inf. Coding Theory 3 (2015), 78–96. https://doi.org/10.1504/IJICOT.2015.068698.

[15] B.R. McDonald, Finite Rings with Identity, Marcel Dekker, 1974.

[16] G.H. Norton, A. Sălăgean, On the Structure of Linear and Cyclic Codes Over a Finite Chain Ring, Appl. Algebr. Eng. Commun. Comput. 10 (2000), 489–506. https://doi.org/10.1007/pl00012382.

[17] M. Özen, F.Z. Uzekmek, N. Aydin, N.T. Özzaim, Cyclic and Some Constacyclic Codes over the Ring $\mathbb{Z}_4[u]/ < u^2 - 1 >$, Finite Fields Appl. 38 (2016), 27–39.

[18] V.S. Pless, Qian Zhongqiang, Cyclic Codes and Quadratic Residue Codes Over $\mathbb{Z}_4$, IEEE Trans. Inf. Theory 42 (1996), 1594–1600. https://doi.org/10.1109/18.532906.

[19] M. Shi, L. Qian, L. Sok, N. Aydin, P. Solé, On Constacyclic Codes over $\mathbb{Z}_4[u]/ < u^2 - 1 >$ and Their Gray Images, Finite Fields Appl. 45 (2017), 86–95. https://doi.org/10.1016/j.ffa.2016.11.016.

[20] J. Wolfmann, Binary Images of Cyclic Codes over $\mathbb{Z}_4$, IEEE Trans. Inf. Theory 47 (2001), 1773–1779.

[21] J.A. Wood, Duality for Modules over Finite Rings and Applications to Coding Theory, Am. J. Math. 121 (1999), 555–575. https://doi.org/10.1353/ajm.1999.0024.

[22] B. Yildiz, N. Aydin, Cyclic Codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$ and $\mathbb{Z}_4$ Images, Int. J. Inf. Coding Theory 2 (2014), 226–237.