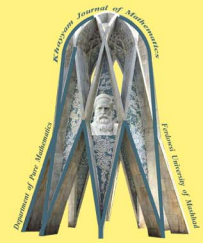
Khayyam J. Math. 11 (2025), no. 2, 336-349
DOI:10.22034/KJM.2025.513627.3491



Khayyam Journal of Mathematics
emis.de/journals/KJM
kjm-math.org

ALGEBRAIC CONSTRUCTION AND ANALYSIS OF DOUBLE CYCLIC CODES OVER $\mathbb{Z}_p \bigoplus u\mathbb{Z}_p$

ZAKARIAE CHEDDOUR[1,*] AND ABDELHAMID TADMORI[1]

Communicated by B. Mashayekhy

Abstract. This study explores the structure and properties of cyclic codes and extends the analysis to double cyclic codes over the ring $\Re = \mathbb{Z}_p \bigoplus u\mathbb{Z}_p$. The objective is to determine the generator polynomials for double cyclic codes. A systematic approach is developed for constructing these generator polynomials using algebraic techniques. Additionally, the research investigates the ranks and minimal covering sets associated with double cyclic codes.

1. Introduction

Cyclic codes [2, 3, 4, 7] are a fundamental class of linear codes that play an essential role in error detection and correction for digital communication and data storage systems [8, 10, 15]. Their inherent algebraic structure enables efficient encoding and decoding algorithms, which has led to their widespread adoption in practical applications.

These codes also intersect with cryptographic systems, where they can be used for secure transmissions or exploited in cryptographic attacks [12, 13, 14, 19]. These codes are characterized by their invariance under cyclic shifts, meaning that if a codeword $(\alpha_0, \alpha_1, \ldots, \alpha_{m-1})$ belongs to a cyclic code $\mathcal{C}$ of length m, then $(\alpha_{m-1}, \alpha_0, \alpha_1, \ldots, \alpha_{m-2})$ is also a codeword, ensuring that the set of codewords forms an ideal in the quotient ring $\Re[t]/(t^m - 1)$, generated by a polynomial $a(t)$ that divides $t^m - 1$, which plays a crucial role in both encoding and decoding processes [15, 20].

Among these codes, Hamming codes [17], defined over $\mathbb{Z}_2$, correct single-bit errors with a minimum Hamming distance of three, Bose–Chaudhuri–Hocquenghem

Date: Received: 23 March 2025; Accepted: 14 August 2025.
* Corresponding author.
2020 *Mathematics Subject Classification.* Primary: 94B05. Secondary: 94B60, 16D10.
Key words and phrases. Linear code, cyclic codes, double cyclic codes.

codes [10, 18] can be designed to correct multiple errors, while Reed-Solomon codes [21], being nonbinary, are optimized for burst error correction and are widely used in digital storage and communication systems.

A natural extension leads to double cyclic codes [1, 6, 5, 9, 11, 16], defined as linear codes of length $m = r + s$ whose coordinates are partitioned into two subsets of respective sizes r and s, each invariant under independent cyclic shifts, meaning that if

$$(\alpha_0, \alpha_1, \ldots, \alpha_{r-1}, \alpha_r, \ldots, \alpha_{m-1})$$

is a codeword of $\mathcal{C}$, then

$$(\alpha_{r-1}, \alpha_0, \alpha_1, \ldots, \alpha_{r-2}, \alpha_{m-1}, \alpha_r, \ldots, \alpha_{m-2})$$

also belongs to $\mathcal{C}$.

Such codes are represented by pairs of polynomials associated with each subset, forming two distinct ideals in the rings $\Re[t]/(t^r - 1)$ and $\Re[t]/(t^s - 1)$, each generated by a polynomial.

This article focuses on double cyclic codes, a specialized subclass of linear codes that extends the concept of cyclic codes. These codes have attracted growing interest in recent years due to their rich algebraic structure and potential applications in the fields of digital communication and data storage.

Borges and Fernandez [9] launched an important line of research by studying the algebraic framework of double cyclic codes $\mathbb{Z}_2$. They provided explicit generator polynomials for these codes and their duals, marking a key step in the structural understanding of this class. This fundamental work has since been extended to broader ring contexts.

Gao et al. [16] analyzed double cyclic codes over $\mathbb{Z}_4$, discovering a classification based on the decomposition of polynomial rings and demonstrating how the structure of the underlying ring influences the parameters and duality of the codes. Building on these developments, Aydogdu and his collaborators have made substantial contributions by exploring double cyclic and skew cyclic codes over various finite rings. For example, Aydogdu [5] studied codes over the unchained ring $\mathbb{Z}_2 + u\mathbb{Z}_2$, presenting new constructions and analyzing their Gray images. Furthermore, Abualrub et al. [1] studied the enumeration and classification of $\mathbb{Z}_p$-double cyclic and quasi-cyclic codes, offering insights into the algebraic structure and counting the number of such codes for given parameters.

2. Preliminaries

In this section, we introduce the essential concepts and notations associated with the ring $\Re = \mathbb{Z}_p \oplus u\mathbb{Z}_p$, where $u^2 = 0$.

These preliminaries provide the necessary background for analyzing cyclic and double-cyclic codes over this ring. Throughout the rest of this paper, we will adhere to the following notations.

- The Hamming weight $\mathrm{H}(s)$ of an element $s \in \Re^m$ is the number of nonzero elements in s.

- Given two vectors $s, t \in \mathfrak{R}^m$, the inner product on $\mathfrak{R}^m$ is defined as

$$\langle s, t\rangle = \sum_{i=1}^{m} s_i t_i.$$

- The dual $\mathcal{C}^{\perp}$ of a linear code $\mathcal{C}$ over $\mathfrak{R}$ is given by

$$\mathcal{C}^{\perp} = \{X \in \mathfrak{R}^m \mid \text{ for all } Y \in \mathcal{C}, \langle Y, X\rangle = 0\},$$

  and a code is self-dual if it is equal to its dual.
- The Lee weight of a codeword $v = (v_1, \ldots, v_m) \in \mathfrak{R}^m$ is defined as $wt(v) = \sum_{i=1}^{m} wt_L(v_i)$, where each component $v_i = x_0^i + x_1^i u \in \mathfrak{R}$ has Lee weight $wt_L(v_i) = \sum_{j=0}^{1} \min\{x_j^i, p - x_j^i\}$.
- We use the notation $\mathbb{Z}_p$ for the ring of integers modulo p, $\mathfrak{R}^m$ to denote an $\mathfrak{R}$-module for $m \in \mathbb{N}$.
- $x \oplus y = x + y \pmod p$ for all $x, y \in \mathfrak{R}$.

Definition 2.1. The ring $\mathfrak{R}$ is defined as $\mathbb{Z}_p \bigoplus u\mathbb{Z}_p$, where u is an indeterminate with the property that $u^2 = 0$. This ring can be viewed as a generalization of the polynomial ring with coefficients in $\mathbb{Z}_p$, truncated at degree 2.

Proposition 2.2. *Let $\mathfrak{R} = \mathbb{Z}_p \bigoplus u\mathbb{Z}_p$. Since u is nilpotent with nilpotent index 2, it follows that $\mathfrak{R}$ is a local principal ideal ring with maximal ideal $u\mathfrak{R}$. Moreover, $\mathfrak{R}/u\mathfrak{R} \cong \mathbb{Z}_p$ is the residue field of $\mathfrak{R}$.*

Proof. The ring $\mathfrak{R}$ is local if it has a unique maximal ideal. The principal ideal generated by u is

$$u\mathfrak{R} = \{uf \mid f \in \mathfrak{R}\}.$$

Since $u^2 = 0$, all elements in $u\mathfrak{R}$ are nilpotent. Thus, $u\mathfrak{R}$ is a proper ideal of $\mathfrak{R}$.

To show that $u\mathfrak{R}$ is maximal, consider the quotient ring $\mathfrak{R}/u\mathfrak{R}$ as follows:

$$\mathfrak{R}/u\mathfrak{R} = \left(\mathbb{Z}_p \bigoplus u\mathbb{Z}_p\right) / u \left(\mathbb{Z}_p \bigoplus u\mathbb{Z}_p\right),$$

since the only surviving term in the quotient is the constant term $\mathbb{Z}_p$.

Thus, $\mathfrak{R}/u\mathfrak{R} \cong \mathbb{Z}_p$, which is the residue field of $\mathfrak{R}$ indicating that $u\mathfrak{R}$ is maximal. Furthermore, since every ideal of a principal ideal ring is generated by a single element and every ideal of $\mathfrak{R}$ is of the form $u^k\mathfrak{R}$, $\mathfrak{R}$ is a principal ideal ring. □

We will now explore the concept of linear codes over the ring $\mathfrak{R}$. More precisely, a linear code $\mathcal{C}$ of length m over $\mathfrak{R}$ is a submodule of $\mathfrak{R}^m$. We can associate linear codes on $\mathfrak{R}$ with linear codes on $\mathbb{Z}_p$ using the following map.

Definition 2.3. Let $A = (\gamma_j)_{j=1}^m \in \mathfrak{R}^m$, where $\gamma_j = x_0^j + x_1^j u \in \mathfrak{R}$ for all $j \in \{1, \ldots, m\}$. Accordingly, the Gray map is characterized in the following manner

$$\begin{aligned} \Phi : \quad & \mathfrak{R}^m \to \mathbb{Z}_p^{2m} \\ & A \to \Phi(A) = \left(x_1^1, \ldots, x_1^m, x_0^1 \oplus x_1^1, \ldots, x_0^m \oplus x_1^m\right). \end{aligned} \tag{2.1}$$

Remark 2.4. We can also extend the above map to $\Re^r \times \Re^s$ for $A = (\gamma_j)_{j=1}^r \in \Re^r, B = (\alpha_j)_{j=1}^s \in \Re^s$ and $m = r + s$ as follows,

$$\begin{aligned} \Phi: \quad & \Re^r \times \Re^s \to \mathbb{Z}_p^{2m} \\ & (A, B) \to \left(x_1^1, \ldots, x_1^r, x_0^1 \oplus x_1^1, \ldots, x_0^r \oplus x_1^r, \right. \\ & \qquad \left. y_1^1, \ldots, y_1^s, y_0^1 \oplus y_1^1, \ldots, y_0^s \oplus y_1^s\right), \end{aligned} \tag{2.2}$$

where $\gamma_j = x_0^j + x_1^j u$ and $\alpha_j = y_0^j + y_1^j u \in \Re$.

Proposition 2.5. *Let Φ be the Gray map defined above and $\mathcal{C}$ be a linear code in $\Re^m$, then, $\Phi(\mathcal{C})$ is a linear code over $\mathbb{Z}_p^{2m}$.*

Proof. Let $\mathcal{C}$ be a linear code in $\Re^m$. We need to show that $\Phi(\mathcal{C})$ is a linear code in $\mathbb{Z}_p^{2m}$.
By definition, $\mathcal{C}$ being a linear code means that $\mathcal{C}$ is closed under addition and scalar multiplication in $\Re^m$.
Specifically, for any $A = (\gamma_j)_{j=1}^m$, $B = (\alpha_j)_{j=1}^m \in \mathcal{C}$ and any $\lambda \in \Re$, we have $A + B \in \mathcal{C}$ and $\lambda A \in \mathcal{C}$.
Put $\gamma_j = x_0^j + x_1^j u$ and $\alpha_j = y_0^j + y_1^j u \in \Re$. Thus, considering the images under Φ,

$$\Phi(A) = \left(x_1^1, \ldots, x_1^m, x_0^1 \oplus x_1^1, \ldots, x_0^m \oplus x_1^m\right),$$

and

$$\Phi(B) = \left(y_1^1, \ldots, y_1^m, y_0^1 \oplus y_1^1, \ldots, y_0^m \oplus y_1^m\right).$$

Since addition in $\Re$ corresponds to bitwise addition modulo p in $\mathbb{Z}_p$

$$\begin{aligned} \Phi(A + B) &= \Phi\left((\gamma_j + \alpha_j)_{j=1}^m\right) \\ &= \Phi\left(((x_0^j \oplus y_0^j) + (x_1^j \oplus y_1^j)u)_{j=1}^m\right) \\ &= \left(x_1^1 \oplus y_1^1, \ldots, x_1^m \oplus y_1^m, x_0^1 \oplus y_0^1 \oplus x_1^1 \oplus y_1^1, \right. \\ &\qquad \left. \ldots, x_0^m \oplus y_0^m \oplus x_1^m \oplus y_1^m\right). \end{aligned}$$

On the other hand,

$$\begin{aligned} \Phi(A) \oplus \Phi(B) &= \left(x_1^1, \ldots, x_1^m, x_0^1 \oplus x_1^1, \ldots, x_0^m \oplus x_1^m\right) \\ &\qquad \oplus \left(y_1^1, \ldots, y_1^m, y_0^1 \oplus y_1^1, \ldots, y_0^m \oplus y_1^m\right) \\ &= \left(x_1^1 \oplus y_1^1, \ldots, x_1^m \oplus y_1^m, x_0^1 \oplus x_1^1 \oplus y_0^1 \oplus y_1^1, \right. \\ &\qquad \left. \ldots, x_0^m \oplus x_1^m \oplus y_0^m \oplus y_1^m\right). \end{aligned}$$

Thus,

$$\Phi(A + B) = \Phi(A) \oplus \Phi(B).$$

Similarly, for scalar multiplication by $\lambda \in \mathbb{Z}_p^{2m}$, given that scalar multiplication by λ in $\Re$ corresponds to coordinate-wise multiplication in $\mathbb{Z}_p$

$$\Phi(\lambda A) = \lambda \Phi(A).$$

Thus, $\Phi(\mathcal{C})$ is closed under addition and scalar multiplication in $\mathbb{Z}_p^{2m}$, making it a linear code in $\mathbb{Z}_p^{2m}$. □

3. DOUBLE CYCLIC CODES

A double cyclic code is a generalization of a cyclic code, where the set of its coordinates is divided into two parts, and each part is cyclically shifted independently.

Definition 3.1. Let $m = r + s$, where r and s are odd integers. A double cyclic code $\mathcal{C}$, of length m over $\Re$ can be viewed as a pair of cyclic codes of lengths r and s. This means that if

$$c = (\alpha_0, \alpha_1, \ldots, \alpha_{r-1}, \gamma_0, \ldots, \gamma_{s-2}, \gamma_{s-1}) \in \mathcal{C},$$

then

$$(\alpha_{r-1}, \alpha_0, \alpha_1, \ldots, \alpha_{r-2}, \gamma_{s-1}, \gamma_0, \ldots, \gamma_{s-2}) \in \mathcal{C}.$$

Remark 3.2. For any codeword

$$c = (\alpha_0, \alpha_1, \ldots, \alpha_{r-1}, \gamma_0, \ldots, \gamma_{s-2}, \gamma_{s-1})$$

and any $k \in \mathbb{Z}$, we denote the kth shift of c by

$$\begin{aligned} S^k(c) = \big(&\alpha_{\{r-k \pmod r\}}, \alpha_{\{r+1-k \pmod r\}}, \ldots, \alpha_{\{r+(r-1)-k \pmod r\}}, \\ &\gamma_{\{s-k \pmod s\}}, \ldots, \gamma_{\{s+(s-1)-k \pmod s\}}\big). \end{aligned} \tag{3.1}$$

As mentioned previously, the dual code is defined by

$$\mathcal{C}^{\perp} = \{X \in \Re^m \mid \text{ for all } Y \in \mathcal{C}, \langle Y, X\rangle = 0\}.$$

So, here we will give a similar definition to the dual code of a double cyclic code $\mathcal{C}$.

Definition 3.3. The dual code of $\mathcal{C}$ is defined by

$$\mathcal{C}^{\perp} = \{(X_1, X_2) \in \Re^r \times \Re^s \mid \text{ for all } (Y_1, Y_2) \in \mathcal{C}, \langle (Y_1, Y_2), (X_1, X_2)\rangle = 0\}.$$

Since we define a double cyclic code as pairs of cyclic codes of lengths r and s, where $m = r + s$ and r and s are odd integers, we have the following result, which gives us the relationship between the double cyclicity of the code $\mathcal{C}$ and its dual.

Lemma 3.4. *Let $\mathcal{C}$ be an $\Re$-double cyclic code; then so is $\mathcal{C}^{\perp}$.*

Proof. A double cyclic code $\mathcal{C}$ of length $m = r + s$ over $\Re$ can be viewed as a pair of cyclic codes of lengths r and s. To show that $\mathcal{C}^{\perp}$ is also a double cyclic code, we will demonstrate that $\mathcal{C}^{\perp}$ is closed under the same shifting operation defined for $\mathcal{C}$. Then, for any

$$c = (\alpha_0, \alpha_1, \ldots, \alpha_{r-1}, \gamma_0, \ldots, \gamma_{s-2}, \gamma_{s-1}) \in \mathcal{C}$$

and $y \in \mathcal{C}^{\perp}$, we have

$$\langle y, c\rangle = 0.$$

Now, consider the shifted codeword $S^k(c)$ and $S^k(y)$ for $k \in \mathbb{Z}$,

$$\begin{aligned} S^k(c) = \big(&\alpha_{\{r-k \pmod r\}}, \alpha_{\{r+1-k \pmod r\}}, \ldots, \alpha_{\{r+(r-1)-k \pmod r\}}, \\ &\gamma_{\{s-k \pmod s\}}, \ldots, \gamma_{\{s+(s-1)-k \pmod s\}}\big). \end{aligned}$$

Since $S^k(c) \in \mathcal{C}$, we have

$$\langle y, S^k(c)\rangle = 0.$$

Conversely, since y was chosen arbitrarily from $\mathcal{C}^\perp$, it necessarily follows that

$$\langle S^k(y), c\rangle = \langle y, S^{-k}(c)\rangle = 0,$$

for all $c \in \mathcal{C}$, implying that

$$S^k(y) \in \mathcal{C}^\perp.$$

Hence, $\mathcal{C}^\perp$ is closed under the shift S^k for all $k \in \mathbb{Z}$, making $\mathcal{C}^\perp$ a double cyclic code. □

3.1. **Generator polynomials.** This subsection explores the generator polynomials of a double cyclic code $\mathcal{C}$. The focus is on identifying and characterizing these polynomials, which are fundamental to defining the structure and properties of $\mathcal{C}$. This study aims to clarify and better understand the algebraic structure of double cyclic codes.

Lemma 3.5. *Let $\mathcal{C}$ be an $\Re$-double cyclic code. Thus,*

$$\Pi : \Re^r \times \Re^s \to \Re[t]/\left(t^r - 1\right) \times \Re[t]/\left(t^s - 1\right)$$

is a bijective function, where any element

$$c = (\alpha_0, \alpha_1, \ldots, \alpha_{r-1}, \alpha_r, \alpha_{r+1}, \ldots, \alpha_{m-1}) \in \mathcal{C} \subseteq \Re^r \times \Re^s$$

can be identified with an element of $\Re[t]/\left(t^r - 1\right) \times \Re[t]/\left(t^s - 1\right)$ as follows:

$$\begin{aligned}\Pi(c) &= \left(\alpha_0 + \alpha_1 t + \cdots + \alpha_{r-1}t^{r-1}, \alpha_r + \alpha_{r+1}t + \cdots + \alpha_{m-1}t^{s-1}\right)\\ &= (u(t), v(t)).\end{aligned}$$

Corollary 3.6. *The ring $\Re[t]/\left(t^r - 1\right) \times \Re[t]/\left(t^s - 1\right)$ is an $\Re[t]$-module.*

Furthermore, any $\Re$-double cyclic code $\mathcal{C}$ is an $\Re[t]$-sub-module of $\Re[t]/\left(t^r - 1\right) \times \Re[t]/\left(t^s - 1\right)$.

Proof. We have that Π is a bijective function. Moreover,

$$\begin{aligned}* : \Re[t] \times \Re[t]/\left(t^r - 1\right) \times \Re[t]/\left(t^s - 1\right) &\longrightarrow \Re[t]/\left(t^r - 1\right) \times \Re[t]/\left(t^s - 1\right)\\ (\lambda(t), u(t), v(t)) &\longrightarrow \lambda(t) * (u(t), v(t)) = (\lambda(t)u(t), \lambda(t)v(t))\end{aligned}$$

is well-defined. □

The following theorem provides a fundamental result that characterizes the generator polynomials of double cyclic codes.

Theorem 3.7. *Let $\mathcal{C}$ be an $\Re$-double cyclic code of length $m = r + s$. Then*

$$\mathcal{C} = \left\langle \left(\aleph_1(t), 0\right), \left(h(t), \aleph_2(t)\right)\right\rangle,$$

where $\aleph_1 = \sigma_1(t) + u\gamma(t)$ and $\aleph_2 = \sigma_2(t) + u\alpha(t)$ and we have

1. *$\gamma(t)|\sigma_1(t)|t^r - 1$ and $\alpha(t)\,|\sigma_2(t)|\,t^s - 1$ over $\Re$.*
2. *$h(t)$ is a polynomial over $\Re$ with $\deg h(t) < \deg \aleph_1$.*
3. *$\aleph_1$, $\aleph_2$ and $h(t)$ are unique.*
4. *$\aleph_1(t) \,\Big|\, \left(\frac{t^s-1}{\alpha(t)}\right) h(t)$.*

Proof. Let $\mathcal{C}$ be an $\Re$-double cyclic code. We have from Lemma 3.5 that Π is a one-to-one correspondence map, so consider the following commutative diagrams:

$$\begin{array}{ccc} \Re^r \times \Re^s & \xrightarrow{\Pi} & \Re[t]/(t^r-1) \times \Re[t]/(t^s-1) \\ \downarrow & & \downarrow \\ \mathcal{C} & \xrightarrow{\Psi_1} & \Re[t]/(t^r-1) \end{array}$$

and

$$\begin{array}{ccc} \Re^r \times \Re^s & \xrightarrow{\Pi} & \Re[t]/(t^r-1) \times \Re[t]/(t^s-1) \\ \downarrow & & \downarrow \\ \mathcal{C} & \xrightarrow{\Psi_2} & \Re[t]/(t^s-1) \end{array},$$

where

$$\Psi_1(\mu_1(t), \mu_2(t)) = \mu_1(t), \ \ \Psi_2(\mu_1(t), \mu_2(t)) = \mu_2(t).$$

Since $\mathcal{C}$, $\Re[t]/(t^r-1)$ and $\Re[t]/(t^s-1)$ are $\Re[t]$-modules, we have that Ψ_1 and Ψ_2 are $\Re$-module homomorphisms. Thus,

$$\mathcal{C}/\ker(\Psi_1) \cong \mathrm{Im}(\Psi_1) \quad \textit{and} \quad \mathcal{C}/\ker(\Psi_2) \cong \mathrm{Im}(\Psi_2).$$

(1) On the other hand, $\mathrm{Im}(\Psi_i)$ and $\ker(\Psi_i)$ are sub-modules respectively of $\Re[t]/(t^s-1)$ and $\mathcal{C}$.

Furthermore, $\mathrm{Im}(\Psi_1)$ and $\mathrm{Im}(\Psi_2)$ are cyclic codes respectively over $\Re[t]/(t^r-1)$ and $\Re[t]/(t^s-1)$, and it follows from [3] that we have

$$\mathrm{Im}(\Psi_1) = \langle \sigma_1(t) + u\gamma(t) \rangle \quad \textit{and} \quad \mathrm{Im}(\Psi_2) = \langle \sigma_2(t) + u\alpha(t) \rangle,$$

where $\sigma_i(t)$, $\alpha(t)$ and $\gamma(t)$ are polynomials in $\Re[t]$ satisfying

$$\gamma(t)\,|\sigma_1(t)|\,t^r - 1 \quad \textit{and} \quad \alpha(t)\,|\sigma_2(t)|\,t^s - 1.$$

On the other hand, $\ker(\Psi_2) = \mathrm{Im}(\Psi_1) \times \{0\}$, where

$$\ker(\Psi_2) = \{(\mu(t), 0) \in \mathcal{C} \mid \mu(t) \in \Re[t]/(t^r-1)\}.$$

Consequently,

$$\ker(\Psi_2) = \langle \sigma_1(t) + u\gamma(t), 0 \rangle.$$

Since we have

$$\mathcal{C}/\ker(\Psi_2) \cong \mathrm{Im}(\Psi_2) = \langle \sigma_2(t) + u\alpha(t) \rangle,$$

it follows that

$$\mathcal{C} = \langle (\aleph_1(t), 0), (h(t), \aleph_2(t)) \rangle,$$

where

$$\aleph_1 = \sigma_1(t) + u\gamma(t) \ \textit{and} \ \aleph_2 = \sigma_2(t) + u\alpha(t),$$

for polynomial $h(t) \in \Re[t]/(t^r-1)$ and, $\aleph_1$ and $\aleph_2$, respectively, over $\Re[t]/(t^r-1)$ and $\Re[t]/(t^s-1)$.

(2) Suppose $\deg(h(t)) \geq \deg(\aleph_1(t))$ with $\deg(h(t)) - \deg(\aleph_1(t)) = k$. Consider the code

$$\begin{aligned}\mathcal{C}' &= \big((\aleph_1(t),0),(h(t),\aleph_2(t)) + t^k * (\aleph_1(t),0)\big)\\ &= \big((\aleph_1(t),0),\big(h(t)+t^k\aleph_1(t),\aleph_2(t)\big)\big).\end{aligned}$$

It is clear that $\mathcal{C}' \subseteq \mathcal{C}$. Indeed we also have

$$(h(t),\aleph_2(t)) = \big(h(t)+t^k\aleph_1(t),\aleph_2(t)\big) - t^k * (\aleph_1(t),0).$$

Therefore $\mathcal{C} \subseteq \mathcal{C}'$, and hence $\mathcal{C} = \mathcal{C}'$.

(3) Since $\langle \aleph_1 \rangle$ and $\langle \aleph_2 \rangle$ are cyclic codes this proves that the polynomials $\sigma_i(t)$, $\gamma(t)$ and $\alpha(t)$ are unique, it remains to be proven that the polynomial $h(t)$ is unique. Suppose that

$$\begin{aligned}\mathcal{C} &= \langle (\aleph_1(t),0),(h_1(t),\aleph_2(t))\rangle\\ &= \langle (\aleph_1(t),0),(h_2(t),\aleph_2(t))\rangle.\end{aligned}$$

Then, $(h_1(t)-h_2(t),0) \in \ker(\Psi_2) = \langle \sigma_1(t)+u\gamma(t),0\rangle$. This implies that

$$h_1(t) - h_2(t) = (\sigma_1(t)+u\gamma(t))\,\mu(t),$$

for some polynomial $\mu(t) \in \Re[t]$. From the second statement of this theorem, we have

$$\deg(h_1(t)-h_2(t)) \leq \deg h_1(t) < \deg(\sigma_1(t)+u\gamma(t)).$$

Then $\mu(t) = 0$, and we have $h_1(t) = h_2(t)$.

(4) To prove $\aleph_1(t) \,\Big|\, \left(\frac{t^s-1}{\alpha(t)}\right) h(t)$, we need to prove that

$$\left(\frac{t^s-1}{\alpha(t)}h(t),0\right) \in \ker(\Psi_2) = \langle \aleph_1(t),0\rangle.$$

Consider $\frac{t^s-1}{\alpha(t)} * (h(t),\aleph_2(t)) = \left(\frac{t^s-1}{\alpha(t)} * h(t), \frac{t^s-1}{\alpha} * \aleph_2(t)\right)$. Then

$$\Psi_2\left(\frac{t^s-1}{\alpha(t)} * h(t), \frac{t^s-1}{\alpha(t)} * \aleph_2(t)\right) = \Psi_2\left(\frac{t^s-1}{\alpha(t)}h(t),0\right) = 0.$$

Consequently,

$$\left(\frac{t^s-1}{\alpha(t)}h(t),0\right) \in \ker(\Psi_2),$$

and it follows that $\aleph_1(t) \,\Big|\, \left(\frac{t^s-1}{\alpha(t)}\right) h(t)$.

□

Corollary 3.8. *Let $\mathcal{C}$ be a $\Re$-double cyclic code. So, if $(h(t),\aleph_2(t)) \in \mathcal{C}$, then*

$$\left(\frac{t^s-1}{\alpha(t)}h(t),0\right) \in \mathcal{C}.$$

Moreover, if $\mathcal{C} = \langle h(t),\aleph_2(t)\rangle$, then it follows that $(t^r-1) \,\Big|\, \frac{t^s-1}{\alpha(t)}h(t)$.

4. Ranks and minimal spanning sets for double cyclic codes over $\Re$

In this section, we will study the rank of double cyclic codes, that is, the dimension of the vector space generated by the codewords.

Furthermore, a minimal code set $\mathcal{C}$ is a collection of codewords that serves as the basis of the code, with the number of elements in this set corresponding to the rank of the code.

The following theorem presents a spanning set for double cyclic codes of the form $\mathcal{C} = \langle (\aleph_1(t), 0), (h(t), \aleph_2(t)) \rangle$ viewed as $\Re$-sub-modules.

Theorem 4.1. *Let $\mathcal{C}$ be an $\Re$-double cyclic code of length $m = r + s$, such that*

$$\mathcal{C} = \langle (\aleph_1(t), 0), (h(t), \aleph_2(t)) \rangle,$$

where

- $\aleph_1 = \sigma_1(t) + u\gamma(t)$ *and* $\aleph_2 = \sigma_2(t) + u\alpha(t)$.
- $deg(\sigma_i) = e_i$.
- $\aleph_1 | t^r - 1$ *and* $\aleph_2 | t^s - 1$.

Then,

$$S = \left(\bigcup_{k=0}^{max\{r-e_1, s-e_2\}-1} \langle (t^k \aleph_1(t), 0) \rangle \right) \cup \left(\bigcup_{k=0}^{s-e_2-1} \langle (t^k h(t), t^k \aleph_2(t)) \rangle \right)$$

forms a spanning set for $\mathcal{C}$ as an $\Re$-module.

Proof. Suppose

$$t^r - 1 = \aleph_1(t) f_1(t) \text{ and } t^s - 1 = \aleph_2(t) f_2(t) \text{ over } \Re[t].$$

Let $\alpha(t) \in \mathcal{C}$. Then

$$\alpha(t) = \mu_1(t) * (\aleph_1(t), 0) + \mu_2(t) * (h(t), \aleph_2(t)),$$

where $\mu_1(t)$ and $\mu_2(t) \in \Re[t]$.

If $\deg(\mu_1(t)) \leq r - e_1 - 1$, then

$$\mu_1(t) * (\aleph_1(t), 0) \in \langle \left(\aleph_1(t), t\aleph_1(t), \ldots, t^{r-e_1-1} \aleph_1(t) \right), 0 \rangle.$$

Otherwise there exist two polynomials $u_1(t), v_1(t)$ such that

$$\mu_1(t) = \left(\frac{t^r - 1}{\aleph_1(t)} \right) u_1(t) + v_1(t),$$

where $v_1(t) = 0$ or $\deg(v_1(t)) \leq r - e_1 - 1$.
Now,

$$\begin{aligned} \mu_1(t) * (\aleph_1(t), 0) &= \left(\frac{t^r - 1}{\aleph_1(t)} \right) u_1(t) * (\aleph_1(t), 0) + v_1(t) * (\aleph_1(t), 0) \\ &= (v_1(t) \aleph_1(t), 0). \end{aligned}$$

Since $\deg(v_1(t)) \leq r - e_1 - 1$, then

$$\mu_1(t) * (\aleph_1(t), 0) \in \langle \left(\aleph_1(t), t\aleph_1(t), \ldots, t^{r-e_1-1} \aleph_1(t) \right), 0 \rangle.$$

If $\deg(\mu_2(t)) \leq s - e_2 - 1$, then

$$\mu_2(t) * (h(t), \aleph_2(t)) \in$$
$$\langle \left(h(t), th(t), \ldots, t^{s-e_2-1}h(t)\right), \left(\aleph_2(t), t\aleph_2(t), \ldots, t^{s-e_2-1}\aleph_2(t)\right)\rangle.$$

Otherwise, there exist two polynomials $u_2(t), v_2(t)$ such that

$$\mu_2(t) = \left(\frac{t^s - 1}{\aleph_2(t)}\right) u_2(t) + v_2(t),$$

where $v_2(t) = 0$ or $\deg(v_2(t)) \leq s - e_2 - 1$.

Now,

$$\begin{aligned}\mu_2(t) * (h(t), \aleph_2(t)) &= \left(\left(\frac{t^s - 1}{\aleph_2(t)}\right) u_2(t) + v_2(t)\right) * (h(t), \aleph_2(t)) \\ &= \left(\frac{t^s - 1}{\aleph_2(t)}\right) u_2(t) * (h(t), 0) + v_2(t) * (h(t), \aleph_2(t)) \\ &= f_2(t)u_2(t) * (h(t), 0) + v_2(t) * (h(t), \aleph_2(t)).\end{aligned}$$

Since $\deg(v_2(t)) \leq s - e_2 - 1$, then

$$v_2(t) * (h(t), \aleph_2(t)) \in$$
$$\langle \left(h(t), th(t), \ldots, t^{s-e_2-1}h(t)\right), \left(\aleph_2(t), t\aleph_2(t), \ldots, t^{s-e_2-1}\aleph_2(t)\right)\rangle.$$

If $\deg(u_2(t)) \leq e_1 - e_2 - 1$, then

$$f_2(t)u_2(t) * (h(t), 0) \in \langle \left(f_2(t)h(t), tf_2(t)h(t), \ldots, t^{s-e_2-1}f_2(t)h(t)\right), 0\rangle.$$

On the other hand, $\aleph_1(t) \Big| \left(\frac{t^s-1}{\alpha(t)}\right) h(t)$; then

$$\left(\frac{t^s - 1}{\alpha(t)}\right) h(t) \in \langle \aleph_1(t)\rangle.$$

Moreover,

$$\left(\frac{t^s - 1}{\aleph_2(t)}\right) u_2(t)h(t) = \left(\frac{t^s - 1}{\alpha(t)}\right) h(t) \left(\frac{\alpha(t)}{\aleph_2(t)}\right) u_2(t).$$

If $\deg(u_2(t)) \leq e_1 - e_2 - 1$, then

$$\left(\frac{t^s - 1}{\alpha(t)}\right) u_2 * (h(t), 0) \in \langle \left(\aleph_1(t), t\aleph_1(t), \ldots, t^{e_1-e_2-1}\aleph_1(t)\right), 0\rangle.$$

Otherwise, we have

$$u_2(t) = \frac{t^s - 1}{f_2(t)\alpha(t)} u_3(t) + v_3(t)$$

with $u_3(t), v_3(t) \in \Re[t]$ and $0 \leq \deg(v_3(t)) \leq e_1 - e_2 - 1$.

Therefore,

$$\begin{aligned}\left(\frac{t^s-1}{\aleph_2(t)}\right) u_2(t)*(h(t),0) &\\ &= \left(\frac{t^s-1}{\aleph_2(t)}\right)\frac{t^s-1}{f_2(t)\alpha(t)}u_3(t)h(t) + \left(\frac{t^s-1}{\aleph_2(t)}\right)v_3(t)h(t)\\ &= \left(\frac{t^s-1}{\alpha(t)}\right)h(t)u_3(t) + \left(\frac{t^s-1}{\alpha(t)}\right)h(t)\left(\frac{\alpha}{\aleph_2(t)}\right)v_3(t).\end{aligned}$$

Since $\deg(v_3(t)) \leq e_1 - e_2 - 1$, and $\aleph_1(t) \,\Big|\, \left(\frac{t^s-1}{\alpha(t)}\right)h(t)$, it follows that

$$\left(\frac{t^s-1}{\alpha(t)}\right)h(t)u_3(t) \in \langle \aleph_1(t), t\aleph_1(t), \ldots, t^{s-e_2-1}\aleph_1(t)\rangle$$

and

$$\begin{aligned}\left(\frac{t^s-1}{\alpha(t)}\right)h(t)\left(\frac{\alpha(t)}{\aleph_2(t)}\right)v_3(t) \in &\langle \aleph_1(t), t\aleph_1(t), \ldots, t^{e_1-e_2-1}\aleph_1(t)\rangle\\ &\subseteq \langle \aleph_1(t), t\aleph_1(t), \ldots, t^{s-e_2-1}\aleph_1(t)\rangle.\end{aligned}$$

Therefore, S is a spanning set for the double cyclic code $\mathcal{C}$. □

In the next theorem, we present a minimal spanning set for the double cyclic code

$$\mathcal{C} = \langle (\aleph_1(t), 0), (h(t), \aleph_2(t))\rangle,$$

where $\sigma_1 | t^r - 1$ and $\sigma_2 | t^s - 1$.

Theorem 4.2. *Let $\mathcal{C}$ be an $\mathfrak{R}$-double cyclic code of length $m = r + s$, such that*

$$\mathcal{C} = \langle (\aleph_1(t), 0), (h(t), \aleph_2(t))\rangle,$$

where

- $\aleph_1 = \sigma_1(t) + u\gamma(t)$ *and* $\aleph_2 = \sigma_2(t) + u\alpha(t)$.
- $deg(\sigma_i) = e_i$, $deg(\gamma) = k$ *and* $deg(\alpha) = l$.
- $\sigma_1 | t^r - 1$ *and* $\sigma_2 | t^s - 1$.

Then,

$$\begin{aligned}S =&\langle \left(t^k\aleph_1(t), 0\right)_{k=0}^{r-e_1-1}\rangle \cup \langle \left(t^k h(t), t^k\aleph_2(t)\right)_{k=0}^{s-e_2-1}\rangle\\ &\cup \langle \left(t^k u f_1(t)\,(\gamma(t), 0)\right)_{k=0}^{e_1-k-1}\rangle \cup \langle \left(t^k f_2(t) * (h(t), \alpha(t)u)\right)_{k=0}^{e_2-l-1}\rangle,\end{aligned}$$

forms a minimal spanning set for $\mathcal{C}$ as an $\mathfrak{R}$-module. Moreover, $\mathcal{C}$ has $4^{r+s-e_1-e_2}2^{e_1+e_2-k-l}$ codewords.

Proof. We have from Theorem 3.7 that

$$t^r - 1 = \gamma(t)f_1(t) \text{ and } t^s - 1 = \alpha(t)f_2(t) \text{ over } \mathfrak{R}[t].$$

It should be noted that this demonstration uses a technique similar to the method employed in the previous argument.

So, let $\alpha(t) \in \mathcal{C},$. Then

$$\alpha(t) = \mu_1(t) * (\aleph_1(t), 0) + \mu_2(t) * (h(t), \aleph_2(t)),$$

where $\mu_1(t)$ and $\mu_2(t) \in \Re[t]$.

If $\deg(\mu_1(t)) \leq r - e_1 - 1$, then

$$\mu_1(t) * (\aleph_1(t), 0) \in \langle \left(\aleph_1(t), t\aleph_1(t), \ldots, t^{r-e_1-1}\aleph_1(t)\right), 0\rangle;$$

see the previous Theorem 4.1.

Otherwise, there exist two polynomials $D_1(t), B_1(t) \in \Re[t]$ such that

$$\mu_1(t) = f_1(t)D_1(t) + B_1(t) \; and \; 0 \leq \deg\left(B_1(t)\right) < r - e_1 - 1.$$

It follows from here that

$$\begin{aligned}\mu(t) * (\aleph_1(t), 0) &= (f_1(t)D_1(t) + B_1(t)) * (\aleph_1(t), 0) \\ &= D_1(t)uf_1(t) * (\gamma(t), 0) + B_1(t) * (\aleph_1(t), 0).\end{aligned}$$

If $\deg\left(D_1(t)\right) \leq e_1 - k - 1$, then we get that

$$D_1(t)uf_1(t) * (\gamma(t), 0) \in \langle t^k uf_1(t) * (\gamma(t), 0)\rangle_{k=0}^{e_1-k-1}.$$

Otherwise, we have

$$D_1(t) = \frac{t^r - 1}{f_1(t)\gamma(t)}D_2(t) + B_2(t),$$

where $D_2(t)$ and $B_2(t)$ are polynomials in $\Re[t]$ with

$$0 \leq \deg\left(B_2(t)\right) \leq e_1 - k - 1.$$

Therefore,

$$\begin{aligned}D_1(t)uf_1(t) * (\gamma(t), 0) &= \left(\frac{t^r - 1}{f_1(t)\gamma(t)}D_2(t) + B_2(t)\right) uf_1(t) * (\gamma(t), 0) \\ &= B_2(t) * uf_1(t) * (\gamma(t), 0) \\ &\in \langle t^k uf_1(t) * (\gamma(t), 0)\rangle_{k=0}^{e_1-k-1}.\end{aligned}$$

So, we have shown that

$$\mu(t) * (\aleph_1(t), 0) \in \langle t^k \left(\aleph_1, 0\right)\rangle_{k=0}^{e_1-k-1} \cup \in \langle t^k uf_1(t) * (\gamma(t), 0)\rangle_{k=0}^{e_1-k-1}.$$

If $\deg(\mu_2(t)) \leq s - e_2 - 1$, then

$$\mu_2(t) * (h(t), \aleph_2(t)) \in \langle t^k \left(h(t), \aleph_2(t)\right)\rangle_{k=0}^{s-e_2-1},$$

see the previous Theorem 4.1.

Otherwise there exist two polynomials $M_1(t), N_1(t) \in \Re[t]$ such that

$$\mu_2(t) = f_2(t)M_1(t) + N_1(t) \; and \; 0 \leq \deg\left(N_1(t)\right) < s - e_2 - 1.$$

It follows from here that

$$\begin{aligned}\mu_2(t) * (h(t), \aleph_2(t)) &= (f_2(t)M_1(t) + N_1(t)) * (h(t), \aleph_2(t)) \\ &= M_1(t)f(2) * (h(t), \alpha(t)u) + N_1(t) * (h(t), \aleph_2(t)).\end{aligned}$$

Since $0 \leq \deg\left(N_1(t)\right) < s - e_2 - 1$, then

$$N_1(t) * (h(t), \aleph_2(t)) \in \langle t^k \left(h(t), \aleph_2\right)\rangle_{k=0}^{s-e_2-1}.$$

If $\deg\left(M_1(t)\right) \leq e_2 - l - 1$, then we get that

$$M_1(t)f(2) * (h(t), \alpha(t)u) \in \langle t^k f_2(t) * (h(t), \alpha(t)u)\rangle_{k=0}^{e_2-l-1}.$$

Otherwise, we have

$$M_1(t) = \frac{t^s - 1}{f_2(t)\alpha(t)} M_2(t) + N_2(t),$$

where $M_2(t)$ and $N_2(t)$ are polynomials in $\Re[t]$ with

$$0 \leq \deg\left(N_2(t)\right) \leq e_2 - l - 1.$$

Therefore,

$$\begin{aligned} M_1(t) f_2(t) * (h(t), \alpha(t)u) &= \left(\frac{t^s - 1}{f_2(t)\alpha(t)} M_2(t) + N_2(t) \right) f_2(t) * (h(t), \alpha(t)u) \\ &= \left(\frac{t^s - 1}{f_2(t)\alpha(t)} M_2(t) \right) * (f_2(t)h(t), f_2(t)\alpha(t)u) \\ &\qquad + N_2(t) f_2(t) * (h(t), \alpha(t)u) \\ &= M_2(t) * \left(\frac{t^s - 1}{\alpha(t)} h(t), 0 \right) \\ &\qquad + N_2(t) f_2(t) * (h(t), \alpha(t)u)\,. \end{aligned}$$

Since $0 \leq \deg\left(N_2(t)\right) < e_2 - l - 1$, then

$$N_2(t) f_2(t) * (h(t), \alpha(t)u) \in \langle t^k f_2(t) * (h(t), \alpha(t)u) \rangle_{k=0}^{e_2 - l - 1}.$$

From Theorem 3.7 we have $\aleph_1(t) \,\Big|\, \left(\frac{t^s - 1}{\alpha(t)}\right) h(t)$.

Therefore, $\frac{t^s - 1}{\alpha(t)} h(t) = \aleph_1(t) g(t)$, where $g(t) \in \Re[t]$. So,

$$M_2(t) * \left(\frac{t^s - 1}{\alpha(t)} h(t), 0 \right) \in \left(\langle t^k * (\aleph_1, 0) \rangle_{k=0}^{r - e_1 - 1} \right) \cup \left(\langle t^k u f_1(t) * (\gamma(t), 0) \rangle_{k=0}^{e_1 - k - 1} \right).$$

Consequently, the set S is an overlay for $\mathcal{C}$.

Furthermore, S is a minimal set. This means that none of the elements of S are linearly dependent on the others.

Therefore, the code $\mathcal{C}$ contains

$$2^{2(r+s-e_1-e_2)} 2^{e_1+e_2-k-l} = 4^{r+s-e_1-e_2} 2^{e_1+e_2-k-l}$$

codewords. □

Conclusion

This study examined the algebraic structure and fundamental characteristics of double cyclic codes defined over the ring $\Re = \mathbb{Z}_p \oplus u\mathbb{Z}_p$, with $u^2 = 0$.

The discussion began with an exploration of cyclic codes, and then extended the analysis to their double-cyclic counterparts.

At the heart of the analysis is the derivation of generator polynomials using algebraic methods.

In addition, the article addresses the determination of code ranks and the identification of minimal covering sets.

Acknowledgement. The authors are thankful to the anonymous referees for

their helpful comments.

References

1. T. Abualrub, I. Aydogdu, E. Yildiz, and K. Khashyarmanesh, *On the number of $\mathbb{Z}_p$-double cyclic codes and quasi cyclic codes*, J. Algebra Appl. **23** (2024), no. 13, 2450215.
2. T. Abualrub and R. Oehmke, *On the generators of $\mathbb{Z}_4$ cyclic codes of length 2^e*, IEEE Trans. Inf. Theory **49** (2003), no. 9, 2126–2133.
3. T. Abualrub and I. Siap, *Cyclic codes over the rings $\mathbb{Z}_2 + u\mathbb{Z}_2$ and $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2$*, Des. Codes Cryptogr. **42** (2007), no. 3, 273–287.
4. M. Al Ashker and M. Hamoudeh, *Cyclic codes over $\mathbb{Z}_2+u\mathbb{Z}_2+\cdots+u^{k-1}\mathbb{Z}_2$*, Turk. J. Math. **35** (2011), no. 4, Article 14.
5. I. Aydogdu, *On double cyclic codes over $\mathbb{Z}_2+u\mathbb{Z}_2$*, AIMS Math. **9** (2024), no. 5, 11076–11091.
6. I. Aydogdu, R. M. Hesari, and K. Samei, *Double skew cyclic codes over $\mathbb{F}_q$*, Comput. Appl. Math. **41** (2022), no. 3, 126.
7. T. Blackford, *Cyclic codes over $\mathbb{Z}_4$ of oddly even length*, Discrete Appl. Math. **128** (2003), no. 1, 27–46.
8. R. E. Blahut, *Algebraic Codes for Data Transmission*, Cambridge Univ. Press, 2003.
9. J. Borges, C. Fernández-Córdoba, and R. Ten-Valls, *$\mathbb{Z}_2$-double cyclic codes*, Des. Codes Cryptogr. **86** (2018), no. 3, 463–479.
10. R. C. Bose and D. K. Ray-Chaudhuri, *On a class of error correcting binary group codes*, Inf. Control **3** (1960), no. 1, 68–79.
11. Z. Cheddour, *Double cyclic codes over $\aleph = \bigoplus_{i=0}^{n} \zeta^i\mathbb{Z}_2$, with $\zeta^n = 0$*, Cryptography and Communications (2025).
12. Z. Cheddour, A. Chillali, and A. Mouhib, *Elliptic curve and k-Fibonacci-like sequence*, Sci. Afr. **19** (2023) e01734..
13. Z. Cheddour, A. Chillali, and A. Mouhib, *Elliptic curves over a finite ring*, Ann. Univ. Craiova Math. Comput. Sci. Ser. **50** (2023), no. 2, 313–324.
14. Z. Cheddour, A. Chillali, and A. Mouhib, *Generalized Fibonacci sequences for elliptic curve cryptography*, Mathematics **11** (2023), no. 22, 4693.
15. P. K. Das and L. K. Vashisht, *Error Locating Codes By Using Blockwise-Tensor Product of Blockwise Detecting/Correcting Codes*, Khayyam J. Math. **2**, (2016), no. 1, 6–17.
16. J. Gao, M. Shi, T. Wu, and F.-W. Fu, *On double cyclic codes over $\mathbb{Z}_4$*, Finite Fields Appl. **39** (2016), 233–250.
17. R. W. Hamming, *Error detecting and error correcting codes*, Bell Syst. Tech. J. **29** (1950), no. 2, 147–160.
18. A. Hocquenghem, *Codes correcteurs d'erreurs*, Chiffres **2** (1959), 147–156.
19. H. Imai and M. Hagiwara, *Error-correcting codes and cryptography*, Appl. Algebra Eng. Commun. Comput. **19** (2008), 213–228.
20. W. W. Peterson and E. J. Weldon, *Error-correcting codes*, 2nd ed., MIT Press, 1972.
21. I. S. Reed and G. Solomon, *Polynomial codes over certain finite fields*, J. Soc. Ind. Appl. Math. **8** (1960), no. 2, 300–304.

[1] Department of Mathematics, University Abdelmalek Essaadi, Faculty of Sciences and Technology Al Hoceima, BP 34. Ajdir 32003 Al Hoceima, Morocco.
Email address: Z.cheddour@uae.ac.ma
Email address: A.tadmori@uae.ac.ma