Palestine Journal of Mathematics

Vol 13(4)(2024) , 1213–1226

LINEAR SKEW CYCLIC CODES OVER THE RING $\mathfrak{R} = (\mathcal{B}[v_1, v_2, v_3]) + \vartheta(\mathcal{B}[v_1, v_2, v_3]) + \vartheta^2(\mathcal{B}[v_1, v_2, v_3]) + \vartheta^3(\mathcal{B}[v_1, v_2, v_3])$

Karima Chatouh

Communicated by Ayman Badawi

MSC 2010 Classifications: Primary 11TXX; Secondary 11T71, 14G50.

Keywords and phrases: Linear codes, Skew cyclic codes, Gray map, Gray images.

The author expresses appreciation to the reviewers and editor for their insightful feedback and valuable suggestions, which contributed to improving the quality of the paper.

Corresponding Author: Karima Chatouh

Abstract This article focuses on the examination of skew cyclic codes over the ring $\mathfrak{R} = (\mathcal{B}[v_1, v_2, v_3]) + \vartheta(\mathcal{B}[v_1, v_2, v_3]) + \vartheta^2(\mathcal{B}[v_1, v_2, v_3]) + \vartheta^3(\mathcal{B}[v_1, v_2, v_3])$, with $\mathcal{B} = \mathbb{Z}_{p^m}$ or $\mathbb{F}_{p^m}$, $v_i^2 = v_i$, and $v_i v_j = v_j v_i$. It explores the generator polynomials associated with these skew cyclic codes over $\mathfrak{R}$ and delves into their structural properties through a decomposition theorem. Furthermore, the paper discusses the generator polynomials of the duals of these skew cyclic codes. Additionally, the investigation covers the idempotent generators of skew cyclic codes over the rings $\mathcal{B}[v_1, v_2, v_3]$ and $\mathfrak{R}$.

1 Introduction

Extensive research has been conducted over the past decade on linear codes over rings, particularly following the groundbreaking findings presented in reference [8], which focused on the examination of linear codes over $\mathbb{Z}_4$. This exploration has catalyzed a surge of interest in examining various types of rings within the context of coding theory, leading to diverse avenues of study and potential applications see [1, 2, 6, 9, 12, 14]. As an extension of this development, our research focuses on studying a particular type of such codes, namely skew cyclic codes over the ring $\mathfrak{R}$.

The concept of skew cyclic codes builds upon cyclic codes but extends to finite rings rather than finite fields. A finite ring is a generalization of a finite field and may not have multiplicative inverses for all elements. Skew cyclic codes were first introduced by Pattanayak and Heliyani in 2016 (see [13, 15, 16, 17]).

Skew-cyclic linear codes represent a significant subclass of linear error-correcting codes in coding theory formed through the utilization of skew polynomial rings over finite fields. In essence, these codes extend the concept of cyclic codes by leveraging non-commutative polynomial multiplication operations. Just as cyclic codes exhibit the property that cyclic shifts of codewords remain within the code, skew cyclic codes maintain this property but with operations defined in skew polynomial rings. This differentiation enables a wider spectrum of algebraic structures to be used in encoding and decoding operations. Skew cyclic linear codes are defined by their capacity to correct errors effectively while preserving the beneficial attributes of cyclic codes, rendering them valuable in numerous communication and data storage applications.

This study mostly delves into various facets of coding theory, emphasizing codes defined over the ring $\mathfrak{R}$. It delves into three main areas of study: linear codes over $\mathfrak{R}$, classes of skew

cyclic linear codes over $\mathfrak{R}$, and codes over $\mathfrak{R}$ possessing dual-containing skew cyclic properties. By studying the properties and structures of these codes, the work aims to contribute to the understanding and advancement of coding theory, particularly within the context of rings and algebraic structures.

The remainder of the paper is structured as follows: Section 2 provides an in-depth exploration of the foundational background and prerequisites required to understand the concepts discussed in this paper. It covers topics such as the Gray map and Gray images of linear codes over $\mathfrak{R}$, which are fundamental for understanding subsequent sections. In Section 3, we introduce the concept of linear codes over $\mathfrak{R}$. The main focus of this section is to analyze a particular linear code over $\mathfrak{R}$. Section 4 is dedicated to the test of various categories of skew cyclic linear codes over $\mathfrak{R}$. Skew cyclic codes constitute a specialized subset of linear codes with unique attributes. This section aims at scrutinizing and comparing different classes within this category. Section 5 focuses on examining codes over the ring $\mathfrak{R}$ possessing dual-containing skew cyclic properties. These are a class of error-correcting codes defined over the ring $\mathfrak{R}$, notable for their specific characteristics linked to their dual codes and their similarities to skew cyclic codes, including their resistance to cyclic permutations of codewords. The concluding Section 6 offers a brief of the essential findings and contributions made within this paper.

2 Foundational Background and Preliminaries

This section introduces the finite ring $\mathfrak{R}$, constructed by combining four distinct subrings: $\mathcal{R}$, $\vartheta\mathcal{R}$, $\vartheta^2\mathcal{R}$, and $\vartheta^3\mathcal{R}$. Here, $\mathcal{R}$ is defined as $\mathcal{B}[v_1, v_2, v_3]$, where $v_i^2 = v_i$, and $v_i v_j = v_j v_i$. The construction's citations include [3, 4, 5, 10], establishing a groundwork of background and preliminary components. These elements form the basis for the ensuing discourse within the framework of this finite ring.

Consider the ring

$$\mathfrak{R} = (\mathcal{B}[v_1, v_2, v_3]) + \vartheta(\mathcal{B}[v_1, v_2, v_3]) + \vartheta^2(\mathcal{B}[v_1, v_2, v_3]) + \vartheta^3(\mathcal{B}[v_1, v_2, v_3]), \tag{2.1}$$

for $\mathcal{B} = \mathbb{Z}_{p^m}$ or $\mathbb{F}_{p^m}$, $v_i^2 = v_i$, and $v_i v_j = v_j v_i$.

Based on [7], let $\mathfrak{R}$ be a commutative ring, and consider the set of orthogonal non-zero idempotents for $0 \leq i \leq 3$. These idempotents are defined as $\delta_i = \dfrac{\vartheta^4 - \vartheta}{\vartheta - \vartheta_i}$, where $gcd(\delta_i, \vartheta - \vartheta_i) = 1$, and there exist polynomials t_i and $r_i \in \mathfrak{R}[\vartheta]$ satisfying $t_i\delta_i + r_i(\vartheta - \vartheta_i) = 1$. Let $\varpi_i = t_i\delta_i$. The following proposition naturally emerges from these conditions.

Proposition 2.1. *Let ϖ_i, for $0 \leq i \leq 3$, represent four elements in the commutative ring $\mathfrak{R}$. These elements ϖ_i satisfy the conditions of being orthogonal non-zero idempotents and also fulfill the Pierce conditions over $\mathfrak{R}$ as follows: $\varpi_0 = t_0\dfrac{\vartheta^4 - \vartheta}{\vartheta - \vartheta_0}$, $\varpi_1 = t_1\dfrac{\vartheta^4 - \vartheta}{\vartheta - \vartheta_1}$, $\varpi_2 = t_2\dfrac{\vartheta^4 - \vartheta}{\vartheta - \vartheta_2}$, and $\varpi_3 = t_3\dfrac{\vartheta^4 - \vartheta}{\vartheta - \vartheta_3}$, where $t_i \in \mathcal{R}$ for $0 \leq i \leq 3$. These expressions demonstrate how each ϖ_i can be constructed using the given polynomial forms, fulfilling the specified conditions.*

Let's examine the subsequent idempotent elements in $\mathcal{R}$, $\zeta_0 = \prod_{i=1}^{2}(1 - v_i), \zeta_1 = v_1\prod_{i=2}^{3}(1 - v_i), \zeta_2 = v_2\prod_{i=1, i\neq 2}^{3}(1 - v_i), \zeta_3 = v_3\prod_{i=1}^{2}(1 - v_i), \zeta_4 = (1 - v_3)\prod_{i=1}^{2} v_i, \zeta_5 = (1 - v_2)\prod_{i=1, i\neq 2}^{3} v_i, \zeta_6 = (1 - v_1)\prod_{i=2}^{3} v_i, \zeta_7 = \prod_{i=1}^{3} v_i$.

There exist two primary approaches to define an element c in $\mathfrak{R}$. According to [5], the first

method is:

$$\begin{aligned} c &= \varpi_0\left[a_0+\sum_{i=1}^{4}v_ia_1^i+\sum_{i=1}^{2}\sum_{j=i+1}^{3}v_iv_ja_2^{ij}+\prod_{k=1}^{3}v_ka_7\right] \\ &+ \varpi_1\left[b_0+\sum_{i=1}^{3}v_ib_1^i+\sum_{i=1}^{2}\sum_{j=i+1}^{3}v_iv_jb_2^{ij}+\prod_{k=1}^{3}v_kb_7\right] \\ &+ \varpi_2\left[c_0+\sum_{i=1}^{3}v_ic_1^i+\sum_{i=1}^{2}\sum_{j=i+1}^{3}v_iv_jc_2^{ij}+\prod_{k=1}^{3}v_kc_7\right] \\ &+ \varpi_3\left[d_0+\sum_{i=1}^{3}v_id_1^i+\sum_{i=1}^{2}\sum_{j=i+1}^{3}v_iv_jd_2^{ij}+\prod_{k=1}^{3}v_kd_7\right]. \end{aligned}$$

As for the second approach, we have:

$$\begin{aligned} c &= \zeta_0(\varpi_0a_0+\varpi_1b_0+\varpi_2c_0+\varpi_3d_0)+\sum_{i=1}^{3}\zeta_iv_i(\varpi_1(a_0+a_1^i)+\varpi_2(b_0+b_1^i)+\varpi_3(c_0+c_1^i)) \\ &+ \zeta_7\prod_{i=1}^{3}v_k(\varpi_0(a_0+a_1^i+\ldots+a_7)+\varpi_1(b_0+b_1^i+\ldots+b_7)+\varpi_2(c_0+c_1^i+\ldots+c_7)) \\ &+ \varpi_3(d_0+d_1^i+\ldots+d_7)). \end{aligned}$$

Corollary 2.2. *[10] The product $\varpi_i\zeta_j$ is the idempotents of $\mathfrak{R}$, for $0\leq i\leq 3$ and $0\leq j\leq 7$.*

Each codeword $(c_0,c_1,\ldots,c_{n-1})\in C$ in the code C is represented by a polynomial $c_0+c_1x+\ldots+c_{n-1}x^{n-1}$ in $\mathfrak{R}[x]$. A code C is termed a cyclic code of length n over $\mathfrak{R}$ if it remains invariant under the cyclic shift operator

$$\begin{array}{rccc} \pi & : & \mathfrak{R}^n & \to & \mathfrak{R}^n \\ & & (c_0,c_1,\ldots,c_{n-1}) & \mapsto & \pi(c_0,c_1,\ldots,c_{n-1})=(c_{n-1},c_0,c_1,\ldots,c_{n-2}). \end{array} \tag{2.2}$$

In the polynomial representation, a cyclic code C of length n over $\mathfrak{R}$ can be characterized as an ideal of the ring $\mathfrak{R}[x]/\langle x^n-1\rangle$. For further insights into skew polynomial rings, readers can refer to the comprehensive discussions in references [7, 11].

Let λ be in $Aut(\mathcal{R})$, and $\Theta:\mathfrak{R}\to\mathfrak{R}$ an extension of λ given by

$$\Theta\left(x=x_0+x_1\vartheta+x_2\vartheta^2+x_3\vartheta^3\right)=\lambda(x_0)+\lambda(x_1)\vartheta+\lambda(x_2)\vartheta^2+\lambda(x_3)\vartheta^3. \tag{2.3}$$

For ν be in $Aut(\mathcal{B})$, and $\lambda:\mathcal{R}\to\mathcal{R}$ an extension of ν given by

$$\lambda(r) = \nu(a_0)+\sum_{i=1}^{4}v_i\nu\left(a_1^i\right)+\sum_{i=1}^{2}\sum_{j=i+1}^{3}v_iv_j\nu\left(a_2^{ij}\right)+\prod_{k=1}^{3}v_k\nu(a_7), \tag{2.4}$$

where $\nu:\mathcal{B}\to\mathcal{B}$ is an application defined by

$$\nu(a)=a^{p^t}. \tag{2.5}$$

By utilizing Equations 2.3, 2.4, and 2.5, we can obtain

$$\begin{aligned}\Theta(x) &= \sum_{t=0}^{3}\vartheta^t\left[(a_0)^{p^t}+\sum_{i=1}^{4}v_i\left(a_1^i\right)^{p^t}+\sum_{i=1}^{2}\sum_{j=i+1}^{3}v_iv_j\left(a_2^{ij}\right)^{p^t}+\prod_{k=1}^{3}v_k\left(a_7\right)^{p^t}\right]\\ &+ \sum_{t=0}^{3}\vartheta^t\left[(b_0)^{p^t}+\sum_{i=1}^{4}v_i\left(b_1^i\right)^{p^t}+\sum_{i=1}^{2}\sum_{j=i+1}^{3}v_iv_j\left(b_2^{ij}\right)^{p^t}+\prod_{k=1}^{3}v_k\left(b_7\right)^{p^t}\right]\\ &+ \sum_{t=0}^{3}\vartheta^t\left[(c_0)^{p^t}+\sum_{i=1}^{4}v_i\left(c_1^i\right)^{p^t}+\sum_{i=1}^{2}\sum_{j=i+1}^{3}v_iv_j\left(c_2^{ij}\right)^{p^t}+\prod_{k=1}^{3}v_k\left(c_7\right)^{p^t}\right]\\ &+ \sum_{t=0}^{3}\vartheta^t\left[(d_0)^{p^t}+\sum_{i=1}^{4}v_i\left(d_1^i\right)^{p^t}+\sum_{i=1}^{2}\sum_{j=i+1}^{3}v_iv_j\left(d_2^{ij}\right)^{p^t}+\prod_{k=1}^{3}v_k\left(d_7\right)^{p^t}\right].\end{aligned}$$

Furthermore, the multiplication operation is defined as follows:

$$(ax^i)(bx^j)=a\Theta(b)\,x^{i+j}, \tag{2.6}$$

but this multiplication is not commutative.

Definition 2.3. [7] Let $\mathfrak{R}$ be a ring and Θ be an automorphism of $\mathfrak{R}$. A linear code C of length n over $\mathfrak{R}$ is a skew cyclic code with

$$c=(c_0,c_1,\ldots,c_{n-1})\in C\Rightarrow\tau(c)=(\Theta(c_{n-1}),\Theta(c_0),\ldots,\Theta(c_{n-2}))\in C, \tag{2.7}$$

where $\tau(c)$ is a skew cyclic shift of c.

Proposition 2.4. *[7] Let $Z(\mathfrak{R}[x,\Theta])$ Denote the center of $\mathfrak{R}[x,\Theta]$. Then $x^n-1\in Z(\mathfrak{R}[x,\Theta])$ if and only if the order of the automorphism Θ divides n.*

Theorem 2.5. *[7] Let C be a code of length n over $\mathfrak{R}$ such that the order of the automorphism Θ divides n. Then C is a skew Θ-cyclic code if and only if C is a left ideal $\langle g(x)\rangle\subseteq R^n$, where $g(x)$ is a right divisor of x^n-1 in $\mathfrak{R}[x,\Theta]$.*

2.1 A Gray Map and Gray Images of Linear Code over $\mathfrak{R}$

This section explores the relationship between linear codes, Gray maps, and their applications in $\mathfrak{R}$. We explore the construction and properties of Gray maps tailored to linear codes over this particular algebraic structure, shedding light on their significance in practical coding theory.

Definition 2.6. The Gray map from $\mathfrak{R}$ to $\mathcal{B}^{32}$ is defined by

$$\begin{array}{rccccccc}\Phi=\Phi_2\circ\Phi_1 & : & \mathfrak{R} & \overset{\Phi_1}{\to} & \mathcal{R}^4 & \overset{\Phi_2}{\to} & \mathcal{B}^{32}\\ & & v & \mapsto & \Phi_1(v)=(v_1,v_2,v_3,v_4) & \mapsto & \Phi_2(\Phi_1(v)),\end{array} \tag{2.8}$$

with $\Phi_2(\Phi_1(v))=\Phi_2(v_1,v_2,v_3,v_4)$, where

$$\begin{aligned}\Phi(v) &= \Phi_2(v_1)=(a_0,a_0+a_1^i,\ldots,a_0+a_1^i+\cdots+a_7),\\ &\Phi_2(v_2)=(b_0,b_0+b_1^i,\ldots,b_0+b_1^i+\cdots+b_7),\\ &\Phi_2(v_3)=(c_0,c_0+c_1^i,\ldots,c_0+c_1^i+\cdots+c_7)),\\ &\Phi_2(v_3)=(d_0,d_0+d_1^i,\ldots,c_0+d_1^i+\cdots+d_7)),\end{aligned}$$

the map Φ is bijective. Furthermore this map can be extended into n tuples of $\mathfrak{R}$ naturally as follows:

$$\Phi=\Phi_2\circ\Phi_1 \;:\; \mathfrak{R}^n \overset{\Phi_1}{\to} \mathcal{R}^{4n} \overset{\Phi_2}{\to} \mathcal{B}^{32n} \tag{2.9}$$

3 A Linear Code over $\mathfrak{R}$

A code $\mathfrak{C}$ of length n over $\mathfrak{R}$ is considered as an $\mathfrak{R}$-submodule of $(\mathfrak{R})^n$. To represent the dual code of $\mathfrak{C}$, denoted as $\mathfrak{C}^{\perp}$, we use the notation such that, $\mathfrak{C}^{\perp} = \{x \in \mathfrak{R}^n : \langle x, y\rangle = 0, \text{for all } y \in \mathfrak{C}\}$. Next, we proceed to define the codes $\mathcal{C}_0, \mathcal{C}_1, \mathcal{C}_2$, and $\mathcal{C}_3$ as follows:

$$\mathcal{C}_0 = \left\{ x_0 \in (\mathcal{R})^n | \exists x_1, x_2, x_3 \in (\mathcal{R})^n | \sum_{i=0}^{3} \varpi_0 x_i \in \mathfrak{C} \right\},$$

$$\mathcal{C}_1 = \left\{ x_1 \in (\mathcal{R})^n | \exists x_0, x_2, x_3 \in (\mathcal{R})^n | \sum_{i=0}^{3} \varpi_0 x_i \in \mathfrak{C} \right\},$$

$$\mathcal{C}_2 = \left\{ x_2 \in (\mathcal{R})^n | \exists x_0, x_1, x_3 \in (\mathcal{R})^n | \sum_{i=0}^{3} \varpi_0 x_i \in \mathfrak{C} \right\},$$

$$\mathcal{C}_3 = \left\{ x_3 \in (\mathcal{R})^n | \exists x_0, x_1, x_2 \in (\mathcal{R})^n | \sum_{i=0}^{3} \varpi_0 x_i \in \mathfrak{C} \right\}.$$

Proposition 2.1 establishes that a linear code $\mathfrak{C}$ of length n over $\mathfrak{R}$ possesses a distinct and unique decomposition as follows:

Theorem 3.1. *Consider a linear code $\mathfrak{C}$ of length n over $\mathfrak{R}$. In this case, a distinctive and exclusive decomposition can be expressed as follows:*

$$\mathfrak{C} = \bigoplus_{i=0}^{3} \varpi_i \mathcal{C}_i, \tag{3.1}$$

and

$$\mathfrak{C} = \bigoplus_{i=0}^{3} \varpi_i \mathcal{C}_i^{\perp}. \tag{3.2}$$

In addition, one can execute a similar computation to form the codes $\mathcal{C}_0, \mathcal{C}_1, \mathcal{C}_2$, and $\mathcal{C}_3$.

Theorem 3.2. *Suppose $\mathcal{C}_0, \mathcal{C}_1, \mathcal{C}_2$, and $\mathcal{C}_3$ are linear codes of length n over $\mathcal{R}$. In this scenario, each of these codes can be uniquely decomposed as follows:*

$$\mathcal{C}_0 = \bigoplus_{k=0}^{7} \zeta_k C_{0k},\ \mathcal{C}_1 = \bigoplus_{k=1}^{7} \zeta_k C_{1k}, \mathcal{C}_2 = \bigoplus_{k=2}^{7} \zeta_k C_{2k}\ and \mathcal{C}_3 = \bigoplus_{k=3}^{7} \zeta_k C_{3k} \tag{3.3}$$

where, the codes C_{ik}, for $0 \le i \le 3$ and $0 \le k \le 7$ is defined in [10].

According to Theorems 3.1 and 3.2, we can deduce the construction of both a linear code and its orthogonal over $\mathfrak{R} = \mathcal{R} + \vartheta\mathcal{R} + \vartheta^2\mathcal{R} + \vartheta^3\mathcal{R}$ by utilizing the following relationships.

$$\begin{aligned} \mathfrak{C} &= \varpi_0 \left[\bigoplus_{k=0}^{7} \zeta_k C_{0k} \right] \oplus \varpi_1 \left[\bigoplus_{k=0}^{7} \zeta_k C_{1k} \right] \oplus \varpi_2 \left[\bigoplus_{k=0}^{7} \zeta_k C_{2k} \right] \oplus \varpi_3 \left[\bigoplus_{k=0}^{7} \zeta_k C_{3k} \right] \\ &= \bigoplus_{i=0}^{3} \varpi_i \left[\bigoplus_{k=0}^{7} \zeta_k C_{ik} \right], \end{aligned} \tag{3.4}$$

and

$$\begin{aligned} \mathfrak{C}^{\perp} &= \varpi_0 \left[\bigoplus_{k=0}^{7} \zeta_k C_{0k}^{\perp} \right] \oplus \varpi_1 \left[\bigoplus_{k=0}^{7} \zeta_k C_{1k}^{\perp} \right] \oplus \varpi_2 \left[\bigoplus_{k=0}^{7} \zeta_k C_{2k}^{\perp} \right] \oplus \varpi_3 \left[\bigoplus_{k=0}^{7} \zeta_k C_{3k}^{\perp} \right] \\ &= \bigoplus_{i=0}^{3} \varpi_i \left[\bigoplus_{k=0}^{7} \zeta_k C_{ik}^{\perp} \right]. \end{aligned} \tag{3.5}$$

Equation 3.4 presents a theorem that can be articulated as follows:

Theorem 3.3. *Let $\mathfrak{C}$ be a linear code of lenght n over $\mathfrak{R}$. Then*

$$\Phi(\mathfrak{C}) = \left(\bigotimes_{k=0}^{7} C_{0k}\right) \otimes \left(\bigotimes_{k=0}^{7} C_{1k}\right) \otimes \left(\bigotimes_{k=0}^{7} C_{2k}\right) \otimes \left(\bigotimes_{k=0}^{7} C_{3k}\right)$$

and

$$|\mathfrak{C}| = \prod_{i=0}^{3} |\mathcal{C}_i|, \ where\ |\mathcal{C}_i| = \prod_{i=0}^{3} \left(\prod_{k=0}^{7} |C_{ik}|\right).$$

Theorem 3.4. *Let us assume that the generator matrix G_i, with $0 \leq i \leq 3$, represents linear codes $\mathcal{C}_0, \mathcal{C}_1, \mathcal{C}_2$, and $\mathcal{C}_3$ as follows, $G_i = \begin{pmatrix} \zeta_0 G_{i0} \\ \zeta_1 G_{i1} \\ \vdots \\ \zeta_7 G_{i7} \end{pmatrix}$. Now, we need to determine the generator matrix of $\mathfrak{C}$.*

$$G = \begin{pmatrix} \varpi_0 G_0 \\ \varpi_1 G_1 \\ \varpi_2 G_2 \\ \varpi_3 G_3 \end{pmatrix}. \tag{3.6}$$

Proposition 3.5. *Suppose $\mathfrak{C}$ is a linear code of length n over $\mathfrak{R}$ with a generator matrix G. Then the generator matrix of $\Phi(\mathfrak{C})$ can be expressed as follows:*

$$\Phi(G) = \begin{pmatrix} \Phi(G_0) & 0 & 0 & 0 \\ 0 & \Phi(G_1) & 0 & 0 \\ 0 & 0 & \Phi(G_2) & 0 \\ 0 & 0 & 0 & \Phi(G_3) \end{pmatrix}, \tag{3.7}$$

with

$$\Phi(G_i) = \begin{pmatrix} G_{i0} & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & G_{i7} \end{pmatrix}, \ for\ 0 \leq i \leq 3. \tag{3.8}$$

4 A Classes of Skew Cyclic Linear Codes over $\mathfrak{R}$

This section focuses on constructing skew cyclic codes over finite rings using the skew polynomial ring with an automorphism Θ. This concept serves as a generalization of cyclic codes over non-commutative polynomial rings. Our main objective is to identify and analyze skew cyclic codes of length n over the finite ring $\mathfrak{R}$.

Theorem 4.1. *Let $\mathfrak{C} = \bigoplus_{i=0}^{3} \varpi_i \left[\bigoplus_{k=0}^{7} \zeta_k C_{ik}\right]$ be a linear code over $\mathfrak{R}$ of length n where C_{ik}, for $0 \leq i \leq 3$ and $0 \leq k \leq 7$ are linear codes of length n over $\mathcal{B}$. Then $\mathfrak{C}$ is a Θ-skew cyclic code over $\mathfrak{R}$ if and only if C_{ik}, for $0 \leq i \leq 3$ and $0 \leq k \leq 7$ are ν-skew cyclic codes over $\mathcal{B}$.*

Proof. Let $\varepsilon = (\varepsilon^0, \varepsilon^1, \ldots, \varepsilon^{n-1})$ in $\mathfrak{C}$, where

$$\varepsilon^q = \varpi_0 \left(\sum_{k=0}^{7} \zeta_k \varepsilon_{0k}^q\right) + \varpi_1 \left(\sum_{k=0}^{7} \zeta_k \varepsilon_{1k}^q\right) + \varpi_2 \left(\sum_{k=0}^{7} \zeta_k \varepsilon_{2k}^q\right) + \varpi_3 \left(\sum_{k=0}^{7} \zeta_k \varepsilon_{3k}^q\right) \text{ and } \varepsilon_{ik}^q \in \mathcal{B},$$

for $0 \leq i \leq 3$, $0 \leq k \leq 7$ and $0 \leq q \leq n-1$. Then

$$\begin{aligned}
\varepsilon_{00} &= \left(\varepsilon_{00}^{0}, \varepsilon_{00}^{1}, \ldots, \varepsilon_{00}^{n-1}\right) \in C_{00}, \\
&\vdots \\
\varepsilon_{07} &= \left(\varepsilon_{07}^{0}, \varepsilon_{07}^{1}, \ldots, \varepsilon_{07}^{n-1}\right) \in C_{07}, \\
&\vdots \\
\varepsilon_{30} &= \left(\varepsilon_{30}^{0}, \varepsilon_{30}^{1}, \ldots, \varepsilon_{30}^{n-1}\right) \in C_{30}, \\
&\vdots \\
\varepsilon_{37} &= \left(\varepsilon_{37}^{0}, \varepsilon_{37}^{1}, \ldots, \varepsilon_{37}^{n-1}\right) \in C_{37}.
\end{aligned}$$

Following Equations 2.3, 2.4 and 2.5, we have

$$\begin{aligned}
\tau(\varepsilon) &= \left(\Theta\left(\sum_{i=0}^{3} \varpi_i x_i^{n-1}\right), \Theta\left(\sum_{i=0}^{3} \varpi_i x_i^{0}\right), \ldots, \Theta\left(\sum_{i=0}^{3} \varpi_i x_i^{n-2}\right)\right) \\
&= \left(\sum_{i=0}^{3} \varpi_i \lambda\left(x_i^{n-1}\right), \sum_{i=0}^{3} \varpi_i \lambda\left(x_i^{0}\right), \ldots, \sum_{i=0}^{3} \varpi_i \lambda\left(x_i^{n-2}\right)\right) \\
&= \varpi_0\left(\lambda\left(x_0^{n-1}\right), \lambda\left(x_0^{0}\right), \ldots, \lambda\left(x_0^{n-2}\right)\right) + \varpi_1\left(\lambda\left(x_1^{n-1}\right), \lambda\left(x_1^{0}\right), \ldots, \lambda\left(x_1^{n-2}\right)\right) \\
&+ \varpi_2\left(\lambda\left(x_2^{n-1}\right), \lambda\left(x_2^{0}\right), \ldots, \lambda\left(x_2^{n-2}\right)\right) + \varpi_3\left(\lambda\left(x_3^{n-1}\right), \lambda\left(x_3^{0}\right), \ldots, \lambda\left(x_3^{n-2}\right)\right) \\
&= \varpi_0\left(\sum_{k=0}^{7} \zeta_k \nu(\varepsilon_{0k}^{n-1}), \ldots, \sum_{k=0}^{7} \zeta_k \nu(\varepsilon_{0k}^{n-2})\right) + \varpi_1\left(\sum_{k=0}^{7} \zeta_k \nu(\varepsilon_{1k}^{n-1}), \ldots, \sum_{k=0}^{7} \zeta_k \nu(\varepsilon_{1k}^{n-2})\right) \\
&+ \varpi_2\left(\sum_{k=0}^{7} \zeta_k \nu(\varepsilon_{2k}^{n-1}), \ldots, \sum_{k=0}^{7} \zeta_k \nu(\varepsilon_{2k}^{n-2})\right) + \varpi_3\left(\sum_{k=0}^{7} \zeta_k \nu(\varepsilon_{3k}^{n-1}), \ldots, \sum_{k=0}^{7} \zeta_k \nu(\varepsilon_{3k}^{n-2})\right) \\
&= \varpi_0\left[\zeta_0\left(\nu(\varepsilon_{00}^{n-1}), \nu(\varepsilon_{00}^{0}), \ldots, \nu(\varepsilon_{00}^{n-2})\right) + \ldots + \zeta_7\left(\nu(\varepsilon_{07}^{n-1}), \nu(\varepsilon_{07}^{0}), \ldots, \nu(\varepsilon_{07}^{n-2})\right)\right] \\
&+ \varpi_1\left[\zeta_0\left(\nu(\varepsilon_{10}^{n-1}), \nu(\varepsilon_{10}^{0}), \ldots, \nu(\varepsilon_{10}^{n-2})\right) + \ldots + \zeta_7\left(\nu(\varepsilon_{17}^{n-1}), \nu(\varepsilon_{17}^{0}), \ldots, \nu(\varepsilon_{17}^{n-2})\right)\right] \\
&+ \varpi_2\left[\zeta_0\left(\nu(\varepsilon_{20}^{n-1}), \nu(\varepsilon_{20}^{0}), \ldots, \nu(\varepsilon_{20}^{n-2})\right) + \ldots + \zeta_7\left(\nu(\varepsilon_{27}^{n-1}), \nu(\varepsilon_{27}^{0}), \ldots, \nu(\varepsilon_{27}^{n-2})\right)\right] \\
&+ \varpi_3\left[\zeta_0\left(\nu(\varepsilon_{30}^{n-1}), \nu(\varepsilon_{30}^{0}), \ldots, \nu(\varepsilon_{30}^{n-2})\right) + \ldots + \zeta_7\left(\nu(\varepsilon_{37}^{n-1}), \nu(\varepsilon_{37}^{0}), \ldots, \nu(\varepsilon_{37}^{n-2})\right)\right] \\
&= \varpi_0\zeta_0\nu(\varepsilon_{00}) + \ldots + \varpi_0\zeta_0\nu(\varepsilon_{07}) + \ldots + \varpi_3\zeta_0\nu(\varepsilon_{30}) + \ldots + \varpi_3\zeta_7\nu(\varepsilon_{37}) \in \mathfrak{C}.
\end{aligned}$$

So that, $\nu(\varepsilon_{ik}) \in C_{ik}$, for $0 \leq i \leq 3$ and $0 \leq k \leq 7$ implying C_{ik} are ν-skew cyclic codes of length n over $\mathcal{B}$. Similarly for the second inclusion. □

The statement suggests that when the length of the code, denoted by n, satisfies the condition of being a multiple of the order of Θ, i.e., $n = \varsigma \cdot \mathrm{ord}(\Theta)$, then it becomes possible to construct the dual code for any skew cyclic code over the field $\mathfrak{C}$. This condition likely has some mathematical significance or simplifies the construction of the dual codes in the context of skew cyclic codes.

Proposition 4.2. *If $\mathfrak{C}$ is a skew cyclic code over $\mathfrak{R}$ and $ord(\Theta)$ divides n, then its dual code $\mathfrak{C}^{\perp}$ is also a skew cyclic code over $\mathfrak{R}$.*

Proof. Let $\mathfrak{C}$ be a skew Θ-cyclic code of length n over $\mathfrak{R}$. We are given two vectors in this code: $\varepsilon = (\varepsilon^0, \varepsilon^1, \ldots, \varepsilon^{n-1})$ and $\eta = ((\eta^0, \eta^1, \ldots, \eta^{n-2})$, where $\eta \in \mathfrak{C}^{\perp}$. To prove that $\mathfrak{C}^{\perp}$ is a skew Θ-cyclic code of length n over $\mathfrak{R}$, it suffices to demonstrate that the vector $\tau(\eta) =$

$(\Theta(\eta^{n-1}), \Theta(\eta^0), \ldots, \Theta(\eta^{n-1}))$ is also a valid element of $\mathfrak{C}^{\perp}$. In other words, if we apply the skew cyclic shift Θ to each component of vector η and arrange them accordingly, this resulting vector $\tau(\eta)$ also satisfies the property of being orthogonal to all elements of $\mathfrak{C}$, we can conclude that $\mathfrak{C}^{\perp}$ is indeed a skew Θ-cyclic code of length n over $\mathfrak{R}$. Consider

$$\varepsilon \cdot \tau(\eta) = \sum_{i=0}^{n-1} \varepsilon^i \Theta(\eta^i). \tag{4.1}$$

When $\mathfrak{C}$ is a skew Θ-cyclic code, we have $\tau^{n-1}(\varepsilon) \in \mathfrak{C}$, where

$$\tau^{n-1}(\varepsilon) = (\Theta^{n-1}(\varepsilon^0), \Theta^{n-1}(\varepsilon^1), \ldots, \Theta^{n-1}(\varepsilon^{n-1})) \in \mathfrak{C}.$$

Then $\tau^{n-1}(\varepsilon) \cdot \eta = 0$, where

$$\tau^{n-1}(\varepsilon) \cdot \eta = \sum_{i=0}^{n-1} \Theta^{n-1}(\varepsilon^i)\eta^i = 0. \tag{4.2}$$

Since $ord(\Theta)|n$, $\Theta^n = Id$, so that

$$\Theta\left(\sum_{i=0}^{n-1} \Theta^{n-1}(\varepsilon^i)\eta^i\right) = \Theta(0) = 0. \tag{4.3}$$

Which involves,

$$\varepsilon \cdot \tau(\eta) = \sum_{i=0}^{n-1} \varepsilon^i \Theta(\eta^i) = 0. \tag{4.4}$$

We result, $\tau(\eta) \in \mathfrak{C}^{\perp}$, implies $\mathfrak{C}^{\perp}$ is a skew Θ-cyclic code of length n over $\mathfrak{R}$. □

Hence, the subsequent outcome is as follows.

Corollary 4.3. *Let* $\mathfrak{C} = \bigoplus_{i=0}^{3} \varpi_i \left[\bigoplus_{k=0}^{7} \zeta_k C_{ik}\right]$ *be a linear code over* $\mathfrak{R}$ *of length* n *such that* n *is a multiple of* $ord(\Theta)$. *Then the dual code* $\mathfrak{C} = \bigoplus_{i=0}^{3} \varpi_i \left[\bigoplus_{k=0}^{7} \zeta_k C_{ik}^{\perp}\right]$ *is a skew* Θ*-cyclic code of length* n *over* $\mathfrak{R}$, *and* $C_{0k}, C_{1k}, C_{2k}, C_{3k}$, *for* $0 \leq k \leq 7$ *are* ν*-skew cyclic codes over* $\mathcal{A}$.

At this phase, we have obtained the generator polynomials for a skew Θ-cyclic code over the ring $\mathfrak{R}$, utilizing the direct sum decomposition technique. In this process, the code decomposes into smaller modules, and each of these modules contributes to the generation of the skew Θ-cyclic code. Consequently, with the help of the direct sum decomposition, we are now equipped with the essential generator polynomials that enable us to represent and analyze the skew Θ-cyclic code effectively.

Theorem 4.4. *Let* $\mathfrak{C} = \bigoplus_{i=0}^{3} \varpi_i \left[\bigoplus_{k=0}^{7} \zeta_k C_{ik}\right]$ *be a skew* Θ*-cyclic code of length* n *over* $\mathfrak{R}$ *and* $t_{ik}(x)$ *be a monic generator polynomial of the skew* ν*-cyclic code* C_{ik}, *for* $0 \leq i \leq 3$ *and* $0 \leq k \leq 7$. *Then*

1. $\mathfrak{C} = \langle \varpi_0\zeta_0 t_{00}(x), \varpi_0\zeta_1 t_{01}(x), \ldots, \varpi_3\zeta_7 t_{37}(x)\rangle$.
2. *A polynomial* $t(x) \in \mathfrak{R}[x, \Theta]$ *can be found such that* $\mathfrak{C} = \langle t(x)\rangle$, *where*

$$t(x) = \sum_{i=0}^{3}\sum_{k=0}^{7} \varpi_i\zeta_k t_{ik}(x),$$

and $t(x)$ *is a divisor of* $x^n - 1$ *on the right.*

Proof. 1. Based on Theorem 4.1, it is established that the sets C_{ik} represent skew ν-cyclic codes of length n over $\mathcal{B}$ for $0 \leq i \leq 3$ and $0 \leq k \leq 7$. Hence, each C_{ik} can be expressed as $\langle t_{ik}(x)\rangle$. On the other hand, the code $\mathfrak{C}$ can be written as $\varpi_0\left(\bigoplus_{k=0}^{7}\zeta_k C_{0k}\right)\oplus \varpi_1\left(\bigoplus_{k=0}^{7}\zeta_k C_{1k}\right)\oplus \varpi_2\left(\bigoplus_{k=0}^{7}\zeta_k C_{2k}\right)\oplus \varpi_3\left(\bigoplus_{k=0}^{7}\zeta_k C_{3k}\right)$, so that

$$\mathfrak{C} \subseteq \langle \varpi_0\zeta_0 t_{00}(x), \varpi_0\zeta_1 t_{01}(x), \ldots, \varpi_3\zeta_7 t_{37}(x)\rangle\,. \tag{4.5}$$

Regarding the second inclusion, we possess the following details and information:

$$\sum_{i=0}^{3}\sum_{k=0}^{7}\varpi_i\zeta_k t_{ij}(x)s_{ik}(x) \in \langle \varpi_0\zeta_0 t_{00}(x), \varpi_0\zeta_1 t_{01}(x), \ldots, \varpi_3\zeta_7 t_{37}(x)\rangle\,,$$

where $s_{ik}(x) \in \mathfrak{R}[x,\Theta]/\langle x^n-1\rangle$. Then there exists, $r_{ik}(x) \in \mathfrak{R}[x,\Theta]/\langle x^n-1\rangle$ such that $\varpi_i\zeta_k s_{ik}(x) = \varpi_i\zeta_k r_{ik}(x)$, for $0 \leq i \leq 3$ and $0 \leq k \leq 7$. Hence,

$$\mathfrak{C} \supseteq \langle \varpi_0\zeta_0 t_{00}(x), \varpi_0\zeta_1 t_{01}(x), \ldots, \varpi_3\zeta_7 t_{37}(x)\rangle\,. \tag{4.6}$$

Subsequent to considering Equations 4.5 and 4.6, the resulting outcome is as follows:

$$\mathfrak{C} = \langle \varpi_0\zeta_0 t_{00}(x), \varpi_0\zeta_1 t_{01}(x), \ldots, \varpi_3\zeta_7 t_{37}(x)\rangle\,.$$

2. If $t_{ik}(x)$ be a generator polynomial of C_{ik}, for $0 \leq i \leq 3$ and $0 \leq k \leq 7$. Then using Part (1), we have the result.

   For the second half, assume that $t_{ik}(x)$, for $0 \leq i \leq 3$ and $0 \leq k \leq 7$ be a monic generator polynomial of C_{ik}, then $t_{ik}(x)$ divides x^n-1 on the right such that

$$\begin{aligned}
x^n-1 &= s_{ik}(x)t_{ik}(x), s_{ik}(x) \in C_{ik}, for\ 0 \leq i \leq 3\ and\ 0 \leq k \leq 7\\
&= \sum_{i=0}^{3}\sum_{k=0}^{7}\varpi_i\zeta_k\left(x^n-1\right)\\
&= \varpi_0\zeta_0\left(x^n-1\right)+\varpi_0\zeta_1\left(x^n-1\right)+\ldots+\varpi_3\zeta_7\left(x^n-1\right)\\
&= \varpi_0\zeta_0 s_{00}(x)t_{00}(x)+\varpi_0\zeta_1 s_{01}(x)t_{01}(x)+\ldots+\varpi_3\zeta_7 s_{37}(x)t_{37}(x)\\
&= \sum_{i=0}^{3}\sum_{k=0}^{7}\varpi_i\zeta_k s_{ik}(x)t_{ik}(x)\\
&= s(x)t(x).
\end{aligned}$$

   Hence, $t(x)$ divides x^n-1 on the right.

□

Example 4.5. Consider $\mathcal{A} = \mathbb{Z}_{16}$, according to the definition of the automorphism Θ, we have

$$\Theta(r) = \varpi_0\left(\sum_{k=0}^{7}\zeta_k r_{0k}^2\right)+\varpi_1\left(\sum_{k=0}^{7}\zeta_k r_{1k}^2\right)+\varpi_2\left(\sum_{k=0}^{7}\zeta_k r_{2k}^2\right)+\varpi_3\left(\sum_{k=0}^{7}\zeta_k r_{3k}^2\right). \tag{4.7}$$

Let $n = 12$ then $ord(\Theta) = 2$ divides n.

$x^{12}-1 = \left(x^2+1\right)(x+1)(x+15)\left(x^2+x+1\right)\left(x^2+15x+1\right)\left(x^4+15x+1\right) \in \mathbb{Z}_{16}[x,\nu]$.

Take, for $1 \leq k \leq 7$

$$\begin{aligned}
t_{0k}(x) &= \left(x^2+x+1\right),\\
t_{1k}(x) &= (x+1),\\
t_{2k}(x) &= (x+15),\\
t_{3k}(x) &= \left(x^4+15x+1\right).
\end{aligned}$$

Then, for $1 \leq k \leq 7$

$$\begin{aligned} C_{0k} &= \langle x^2+x+1 \rangle, \\ C_{1k} &= \langle x+1 \rangle, \\ C_{2k} &= \langle x+15 \rangle, \\ C_{3k} &= \langle x^4+15x+1 \rangle \end{aligned}$$

are skew cyclic codes over $\mathbb{Z}_{16}$. Thus

$$\mathfrak{C} = \langle h_1(x), h_2(x), h_3(x), h_4(x) \rangle,$$

with

$$\begin{aligned} h_0(x) &= \langle \varpi_0\zeta_0\left(x^2+x+1\right), \varpi_0\zeta_1\left(x^2+x+1\right), \ldots, \varpi_0\zeta_7\left(x^2+x+1\right)\rangle, \\ h_1(x) &= \langle \varpi_1\zeta_0\left(x+1\right), \varpi_1\zeta_1\left(x+1\right), \ldots, \varpi_1\zeta_7\left(x+1\right)\rangle, \\ h_2(x) &= \langle \varpi_2\zeta_0\left(x+15\right), \varpi_2\zeta_1\left(x+15\right), \ldots, \varpi_2\zeta_7\left(x+15\right)\rangle, \\ h_3(x) &= \langle \varpi_3\zeta_0\left(x^4+15x+1\right), \varpi_3\zeta_1\left(x^4+15x+1\right), \ldots, \varpi_3\zeta_7\left(x^4+15x+1\right)\rangle. \end{aligned}$$

Example 4.6. Given the set $\mathcal{A} = \mathbb{F}_{64}$, in accordance with the definition of the automorphism Θ, we find that

$$\begin{aligned} x^{12}-1 &= (x+1)^2(x+\alpha+1)^2(x+\alpha^2+1)^2(x+\alpha^3+\alpha^2+\alpha)^2(x+\alpha^3+\alpha^2+\alpha+1)^2 \\ &\quad (x+\alpha^4+1)^2(x+\alpha^4+\alpha)^2(x+\alpha^5+\alpha^4+\alpha+1)^2(x+\alpha^5+\alpha^4+\alpha^2+\alpha)^2. \end{aligned}$$

The codes denoted as $\mathcal{C}_i = \langle \mathcal{J}_i(x) \rangle$, for $0 \leq i \leq 3$ are generated through the following process

$$\begin{aligned} \mathcal{J}_0 &= \langle \zeta_0\left(x+1\right), \zeta_1\left(x+\alpha+1\right), \zeta_2\left(x+\alpha^2+1\right), \zeta_3\left(x+\alpha^3+\alpha^2+\alpha\right), \\ &\quad \zeta_4\left(x+\alpha^3+\alpha^2+\alpha+1\right), \zeta_5\left(x+\alpha^4+1\right), \zeta_6\left(x+\alpha^4+\alpha\right), \\ &\quad \zeta_7\left(x+\alpha^5+\alpha^4+\alpha+1\right)\rangle, \\ \mathcal{J}_1 &= \langle \zeta_0\left(x+\alpha+1\right), \zeta_1\left(x+\alpha^2+1\right), \zeta_2\left(x+\alpha^3+\alpha^2+\alpha\right), \zeta_3\left(x+\alpha^3+\alpha^2+\alpha+1\right), \\ &\quad \zeta_4\left(x+\alpha^4+1\right), \zeta_5\left(x+\alpha^4+\alpha\right), \zeta_6\left(x+\alpha^5+\alpha^4+\alpha+1\right), \\ &\quad \zeta_7\left(x+\alpha^5+\alpha^4+\alpha^2+\alpha\right)\rangle, \\ \mathcal{J}_2 &= \langle \zeta_0\left(x+\alpha^2+1\right), \zeta_1\left(x+\alpha^3+\alpha^2+\alpha\right), \zeta_2\left(x+\alpha^3+\alpha^2+\alpha+1\right), \zeta_3\left(x+\alpha^4+1\right), \\ &\quad \zeta_4\left(x+\alpha^4+\alpha\right), \zeta_5\left(x+\alpha^5+\alpha^4+\alpha+1\right), \zeta_6\left(x+\alpha^5+\alpha^4+\alpha^2+\alpha\right), \zeta_7\left(x+1\right)\rangle, \\ \mathcal{J}_3 &= \langle \zeta_0\left(x+\alpha^3+\alpha^2+\alpha\right), \zeta_1\left(x+\alpha^3+\alpha^2+\alpha+1\right), \zeta_2\left(x+\alpha^4+1\right), \zeta_3\left(x+\alpha^4+\alpha\right), \\ &\quad \zeta_4\left(x+\alpha^5+\alpha^4+\alpha+1\right), \zeta_5\left(x+\alpha^5+\alpha^4+\alpha^2+\alpha\right), \zeta_6\left(x+1\right), \zeta_7\left(x+\alpha+1\right)\rangle \end{aligned}$$

are skew cyclic codes over $\mathbb{F}_{64}[v_1, v_2, v_3]$. Thus, the code $\mathfrak{C} = \langle \varpi_0\mathcal{J}_0, \varpi_1\mathcal{J}_1, \varpi_2\mathcal{J}_2, \varpi_3\mathcal{J}_3 \rangle$.

Example 4.7. When considering the set $\mathcal{A} = \mathbb{F}_{256}$ and referring to the definition of the automorphism Θ, we observe that

$$\Theta(r) = \varpi_0\left(\sum_{k=0}^{7}\zeta_k r_{0k}^8\right) + \varpi_1\left(\sum_{k=0}^{7}\zeta_k r_{1k}^8\right) + \varpi_2\left(\sum_{k=0}^{7}\zeta_k r_{2k}^8\right) + \varpi_3\left(\sum_{k=0}^{7}\zeta_k r_{3k}^8\right). \quad (4.8)$$

Let $n = 200$ then $ord(\Theta) = 8$ divides n.

$$\begin{aligned} x^{200}-1 &= (x+1)^8(x+\alpha^3+\alpha)^8(x+\alpha^6+\alpha^2)^8(x+\alpha^7+\alpha^4+\alpha)^8 \\ &\quad (x+\alpha^7+\alpha^6+\alpha^4+\alpha^3+\alpha^2+1)^8(x^5+\alpha^3+\alpha)^8(x^5+\alpha^6+\alpha^2)^8 \\ &\quad (x^5+\alpha^7+\alpha^4+\alpha)^8(x^5+\alpha^7+\alpha^6+\alpha^4+\alpha^3+\alpha^2+1)^8. \end{aligned}$$

The codes represented as $\mathcal{C}_i = \langle \mathcal{J}_i(x) \rangle$, where $0 \leq i \leq 3$, are created using the following procedure

$$\begin{aligned}
\mathcal{J}_0 &= \langle \zeta_0(x^5+\alpha^7+\alpha^6+\alpha^4+\alpha^3+\alpha^2+1), \zeta_1(x^5+\alpha^7+\alpha^6+\alpha^4+\alpha^3+\alpha^2+1), \ldots, \\
&\quad \zeta_7(x^5+\alpha^7+\alpha^6+\alpha^4+\alpha^3+\alpha^2+1), \\
\mathcal{J}_1 &= \langle \zeta_0(x^5+\alpha^7+\alpha^4+\alpha), \zeta_1(x^5+\alpha^7+\alpha^4+\alpha), \ldots, \zeta_7(x^5+\alpha^7+\alpha^4+\alpha) \rangle, \\
\mathcal{J}_2 &= \langle \zeta_0(x+\alpha^7+\alpha^6+\alpha^4+\alpha^3+\alpha^2+1)^8, \zeta_1(x+\alpha^7+\alpha^6+\alpha^4+\alpha^3+\alpha^2+1)^8, \ldots, \\
&\quad \zeta_7(x+\alpha^7+\alpha^6+\alpha^4+\alpha^3+\alpha^2+1)^8 \rangle, \\
\mathcal{J}_3 &= \langle \zeta_0(x+\alpha^7+\alpha^4+\alpha)^8, \zeta_1(x+\alpha^7+\alpha^4+\alpha)^8, \ldots, \zeta_7(x+\alpha^7+\alpha^4+\alpha)^8 \rangle
\end{aligned}$$

are skew cyclic codes over $\mathbb{F}_{256}[v_1, v_2, v_3]$. Therefore, the code $\mathfrak{C} = \langle \varpi_0 \mathcal{J}_0, \varpi_1 \mathcal{J}_1, \varpi_2 \mathcal{J}_2, \varpi_3 \mathcal{J}_3 \rangle$.

Example 4.8. When examining the set $\mathcal{A} = \mathbb{F}_{1024}$ and taking into account the definition of the automorphism Θ, we can note that

$$\Theta(r) = \varpi_0 \left(\sum_{k=0}^{7} \zeta_k r_{0k}^{10} \right) + \varpi_1 \left(\sum_{k=0}^{7} \zeta_k r_{1k}^{10} \right) + \varpi_2 \left(\sum_{k=0}^{7} \zeta_k r_{2k}^{10} \right) + \varpi_3 \left(\sum_{k=0}^{7} \zeta_k r_{3k}^{10} \right). \quad (4.9)$$

Let $n = 1000$ then $ord(\Theta) = 10$ divides n.

$$\begin{aligned}
x^{1000}-1 &= (x+1)^8(x^2+\alpha x+1)^8(x^2+\alpha^2 x+1)^8(x^2+(\alpha^3+\alpha)x+1)^8(x^2+\alpha^4 x+1)^8 \\
&\quad (x^2+(\alpha^5+\alpha^3+\alpha)x+1)^8(x^2+(\alpha^5+\alpha^3+\alpha+1)x+1)^8(x^2+\alpha^8 x+1)^8 \\
&\quad (x^2+(\alpha^7+\alpha^5+\alpha)x+1)^8(x^2+(\alpha^8+\alpha^7+\alpha^5+\alpha^3+\alpha^2)x+1)^8 \\
&\quad (x^2+(\alpha^9+\alpha^7+\alpha^5+\alpha)x+1)^8(x^2+(\alpha^9+\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha^2)x+1)^8 \\
&\quad (x^{10}+\alpha x^5+1)^8(x^{10}+\alpha^2 x^5+1)^8(x^{10}+(\alpha^3+\alpha)x^5+1)^8(x^{10}+\alpha^4 x^5+1)^8 \\
&\quad (x^{10}+(\alpha^6+\alpha^2)*x^5+1)^8(x^{10}+(\alpha^7+\alpha^5+\alpha)x^5+1)^8(x^{10}+\alpha^8 x^5+1)^8 \\
&\quad (x^{10}+(\alpha^8+\alpha^7+\alpha^5+\alpha^3+\alpha^2)x^5+1)^8(x^{10}+(\alpha^9+\alpha^7+\alpha^5+\alpha)x^5+1)^8 \\
&\quad (x^{10}+(\alpha^9+\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha^2)x^5+1)^8(x^2+(\alpha^6+\alpha^2)x+1)^8.
\end{aligned}$$

The codes, denoted as $\mathcal{C}_i = \langle \mathcal{J}_i(x) \rangle$ with $0 \leq i \leq 3$, are generated through the subsequent process

$$\begin{aligned}
\mathcal{J}_0 &= \langle \zeta_0(x+1), \zeta_1(x^2+\alpha x+1), \zeta_2(x^2+\alpha^2 x+1), \zeta_3(x^2+(\alpha^3+\alpha)x+1), \\
&\quad \zeta_4(x^2+\alpha^4 x+1), \zeta_5(x^2+(\alpha^5+\alpha^3+\alpha)x+1), \zeta_6(x^2+(\alpha^5+\alpha^3+\alpha+1)x+1), \\
&\quad \zeta_7(x^2+(\alpha^6+\alpha^2)x+1) \rangle, \\
\mathcal{J}_1 &= \langle \zeta_0(x^2+(\alpha^7+\alpha^5+\alpha)x+1), \zeta_1(x^2+\alpha^8 x+1), \zeta_2(x^{10}+(\alpha^6+\alpha^2)*x^5+1), \\
&\quad \zeta_3(x^2+(\alpha^9+\alpha^7+\alpha^5+\alpha)x+1), \zeta_4(x^2+(\alpha^9+\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha^2)x+1), \\
&\quad \zeta_5(x^{10}+\alpha x^5+1), \zeta_6(x^{10}+\alpha^2 x^5+1), \zeta_7(x^2+(\alpha^8+\alpha^7+\alpha^5+\alpha^3+\alpha^2)x+1) \rangle, \\
\mathcal{J}_2 &= \langle \zeta_0(x^{10}+(\alpha^7+\alpha^5+\alpha)x^5+1), \zeta_1(x^{10}+(\alpha^7+\alpha^5+\alpha)x^5+1), \zeta_2(x^{10}+\alpha^8 x^5+1), \\
&\quad \zeta_3(x^{10}+(\alpha^6+\alpha^2)*x^5+1), \zeta_4(x^{10}+(\alpha^8+\alpha^7+\alpha^5+\alpha^3+\alpha^2)x^5+1), \\
&\quad \zeta_5(x^{10}+(\alpha^7+\alpha^5+\alpha)x^5+1), \zeta_6(x^{10}+(\alpha^7+\alpha^5+\alpha)x^5+1), \\
&\quad \zeta_7(x^{10}+(\alpha^9+\alpha^7+\alpha^5+\alpha)x^5+1) \rangle, \\
\mathcal{J}_3 &= \langle \zeta_0(x^{10}+(\alpha^9+\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha^2)x^5+1), \zeta_1(x^{10}+(\alpha^9+\alpha^7+\alpha^6+\alpha^5+\alpha^4 \\
&\quad +\alpha^2)x^5+1), \ldots, \zeta_7(x^{10}+(\alpha^9+\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha^2)x^5+1) \rangle
\end{aligned}$$

are skew cyclic codes over $\mathbb{F}_{1024}[v_1, v_2, v_3]$. Therefore, the code $\mathfrak{C} = \langle \varpi_0 \mathcal{J}_0, \varpi_1 \mathcal{J}_1, \varpi_2 \mathcal{J}_2, \varpi_3 \mathcal{J}_3 \rangle$.

The following proposition can be taken into consideration as a direct result of Theorem 4.4:

Proposition 4.9. *Assume that $t_{ij}(x)$ are monic generator polynomials of the skew ν-cyclic codes C_{ij}, for $0 \leq i \leq 3$ and $0 \leq j \leq 7$. If $\mathfrak{C}$ be a skew Θ-cyclic code of length n over $\mathfrak{R}$, such that $ord(\Theta)|n$. Then,*

1. $\mathfrak{C}^{\perp} = \langle \varrho_0\rho_0 s^*_{00}(x), \varrho_0\rho_1 s^*_{01}(x), \ldots, \varrho_3\rho_7 s^*_{37}(x)\rangle$.
2. $\mathfrak{C}^{\perp} = \langle \overline{s}(x)\rangle$, *where* $\overline{s}(x) = \sum_{i=0}^{3}\sum_{i=0}^{7} \varrho_i\rho_j s^*_{ij}(x)$, *whith $s^*_{ij}(x)$ are defined as follows,* $x^n - 1 = s_{ij}(x)t_{ij}(x)$, $s_{ij}(x), t_{ij}(x) \in \mathcal{A}[x,\nu]$. *Assume that* $t_{ij}(x) = a_0 + a_1x + \ldots + a_lx^l$ *and* $s_{ij}(x) = b_0 + b_1x + \ldots + b_{n-l}x^{n-l}$, *then the dual of the skew ν-cyclic code C_{ij} is generated by $s^*_{ij}(x)$ such that,* $s^*_{ij}(x) = b_{n-l} + \nu(b_{n-l-1})x + \ldots + \nu(b_0)x^{n-l}$.

5 Codes over $\mathfrak{R}$ with Dual-Containing Skew Cyclic Properties

Dual-containing skew cyclic codes over $\mathfrak{R}$ are a fascinating and mathematically rich area of coding theory. These codes are a subset of linear block codes defined over the ring $\mathfrak{R}$, where $\mathfrak{R}$ represents a general non-commutative ring, extending the concept of skew polynomial rings. Unlike traditional cyclic codes, which are defined over fields, dual-containing skew cyclic codes offer unique properties and advantages in terms of error correction and code construction.

In these codes, the duality property plays a crucial role. The dual code of a given skew cyclic code is also a skew cyclic code. This duality concept allows for the creation of efficient and versatile error-correcting codes that find applications in various communication and information storage systems.

Corollary 5.1. *Let $C_{ik} = \langle t_{ik}(x)\rangle$, for $0 \leq i \leq 3$ and $0 \leq k \leq 7$ be a skew Θ-cyclic code of length n over $\mathcal{B}$ such that n is the multiple of $ord(\Theta)$. Then C_{ik} contains its dual if and only if $x^n - 1$ is divisible by $s^*_{ik}(x)s_{ik}(x)$ on the right, for $0 \leq i \leq 3$ and $0 \leq k \leq 7$.*

Proof. Let $C_{ik} = \langle t_{ik}(x)\rangle$ contain its dual code. Since $s_{ik}(x) \in C^{\perp}_{ik} \subseteq C_{ik} = \langle t_{ik}(x)\rangle$, where $0 \leq i \leq 3$ and $0 \leq k \leq 7$, there exists a polynomial $m_{ik}(x)$ such that $s^*_{ik}(x) = m_{ik}(x)t_{ik}(x)$, for $0 \leq i \leq 3$ and $0 \leq k \leq 7$. Consequently,

$$s^*_{ik}(x)s_{ik}(x) = m_{ik}(x)t_{ik}(x)s_{ik}(x) = m_{ik}(x)s_{ik}(x)t_{ik}(x) = m_{ik}\left(x^n - 1\right). \tag{5.1}$$

Given that the order of the automorphism Θ is a divisor of n,

$$x^n - 1 = t_{ik}(x)s_{ik}(x) = s_{ik}(x)t_{ik}(x) \in Z(\mathcal{B}[x,\Theta]).$$

Therefore, the product $s^*_{ik}(x)s_{ik}(x)$ is divisible by $x^n - 1$ on the right.

On the contrary, suppose $s^*_{ik}(x)s_{ik}(x)$ is divisible by $x^n - 1$ on the right. In this case, there exists a polynomial $m(x)$ such that $s^*_{ik}(x)s_{ik}(x) = m(x)(x^n - 1)$. Now, consider $q(x) \in C^{\perp}_{ik} = \langle s^*_{ik}(x)\rangle$. Hence, we can express $q(x)$ as $q(x) = \vartheta(x)\, s^*_{ik}(x)$. If we multiply both sides by $s_{ik}(x)$, we obtain

$$\begin{aligned} q(x)s_{ik}(x) &= \vartheta(x)\, s^*_{ik}(x)s_{ik}(x) \\ &= \vartheta(x)\, m(x)(x^n - 1) \\ &= \vartheta(x)\, m(x)s_{ik}(x)t_{ik}(x) \\ &= \vartheta(x)\, m(x)t_{ik}(x)s_{ik}(x). \end{aligned}$$

So, $[q(x)s_{ik}(x) - \vartheta(x)\, m(x)t_{ik}(x)s_{ik}(x)] = 0$. Since $s_{ik}(x)$ is a non-zero polynomial, we conclude that

$$[q(x) - \vartheta(x)\, m(x)t_{ik}(x)] = 0,$$

this suggests that $q(x) = \vartheta(x)\, m(x)t_{ik}(x)$, confirming that $q(x) \in C_{ik} = \langle t_{ik}(x)\rangle$, for $0 \leq i \leq 3$ and $0 \leq k \leq 7$. Consequently, $C^{\perp}_{ik} \subseteq C_{ik}$. □

Example 5.2. To illustrate, when we factorize the polynomial $x^{21} - 1$ over the field $\mathbb{F}_{49}$, we obtain

$$x^{21} - 1 = (x+3)^7(x+5)^7(x+6)^7.$$

Let $t_{ik}(x) = (x+3)$, the codes $C_{ik} = \langle x+3 \rangle$ are skew cyclic codes over $\mathbb{F}_{49}$, for $0 \leq i \leq 3$ and $0 \leq k \leq 7$. Consider $s_{ik}(x) = x^{20} + 4x^{19} + 2x^{18} + x^{17} + 4x^{16} + 2x^{15} + x^{14} + 4x^{13} + 2x^{12} + x^{11} + 4x^{10} + 2x^9 + x^8 + 4x^7 + 2x^6 + x^5 + 4x^4 + 2x^3 + x^2 + 4x + 2$. Then

$$\begin{aligned} x^{21} - 1 &= (x+3)(x^{20} + 4x^{19} + 2x^{18} + x^{17} + 4x^{16} + 2x^{15} + x^{14} + 4x^{13} + 2x^{12} + x^{11} \\ &\quad + 4x^{10} + 2x^9 + x^8 + 4x^7 + 2x^6 + x^5 + 4x^4 + 2x^3 + x^2 + 4x + 2). \end{aligned}$$

Theorem 5.3. *Consider the skew Θ-cyclic code $\mathfrak{C}$ over the ring $\mathfrak{R}$ of length n, where n is a multiple of $ord(\Theta)$. This code is defined as $\mathfrak{C} = \bigoplus_{i=0}^{3} \varpi_i \left[\bigoplus_{k=0}^{7} \zeta_k C_{ik} \right]$. For this code $\mathfrak{C}$, the condition $\mathfrak{C}^{\perp} \subseteq \mathfrak{C}$ holds if and only if the product $s_{ik}^{*}(x)s_{ik}(x)$, for $0 \leq i \leq 3$ and $0 \leq k \leq 7$, is a right divisor of $x^n - 1$.*

Proof. Let $s_{ik}^{*}(x)s_{ik}(x)$ be such that it can be divided by $x^n - 1$ on the right, where $0 \leq i \leq 3$ and $0 \leq k \leq 7$. According to Corollary 5.1, we can establish that $C_{ik}^{\perp}$ is a subset of C_{ik} for all i and k in the specified ranges. Implies that

$$\bigoplus_{i=0}^{3} \varpi_i \left[\bigoplus_{k=0}^{7} \zeta_k C_{ik}^{\perp} \right] \subseteq \bigoplus_{i=0}^{3} \varpi_i \left[\bigoplus_{k=0}^{7} \zeta_k C_{ik} \right].$$

As a result, we can conclude that $\mathfrak{C}^{\perp}$ is a subset of $\mathfrak{C}$.

Conversely, if $\mathfrak{C}^{\perp}$ is a subset of $\mathfrak{C}$, then it follows that

$$\bigoplus_{i=0}^{3} \varpi_i \left[\bigoplus_{k=0}^{7} \zeta_k C_{ik}^{\perp} \right] \subseteq \bigoplus_{i=0}^{3} \varpi_i \left[\bigoplus_{k=0}^{7} \zeta_k C_{ik} \right].$$

When we consider this equation modulo $\varpi_i \zeta_k$, we can deduce that $C_{ik}^{\perp}$ is a subset of C_{ik} for all i and k in the specified ranges. Consequently, we can affirm that $s_{ik}^{*}(x)s_{ik}(x)$ is divisible by $x^n - 1$ on the right, where $0 \leq i \leq 3$ and $0 \leq k \leq 7$. □

The corollary presented below is a straightforward result derived from the preceding theorem.

Corollary 5.4. *Consider a skew Θ-cyclic code $\mathfrak{C}$ of length n over $\mathfrak{R}$. This code is defined as $\mathfrak{C} = \langle \varpi_0\zeta_0 t_{00}(x), \varpi_0\zeta_1 t_{01}(x), \ldots, \varpi_3\zeta_7 t_{37}(x) \rangle$, where n is a multiple of $ord(\Theta)$. The condition $\mathfrak{C}^{\perp} \subseteq \mathfrak{C}$ holds if and only if, for all $0 \leq i \leq 3$ and $0 \leq k \leq 7$, the dual code $C_{ik}^{\perp}$ is a subset of the code C_{ik}.*

6 Conclusion

In this research paper, we delve deep into the properties and applications of skew cyclic codes over the ring $\mathfrak{R}$, offering a thorough analysis that contributes significantly to the field of coding theory. Our study commences with a detailed exposition of the foundational framework of linear codes over $\mathfrak{R}$, followed by an intricate examination of the distinctive structural attributes delineating skew cyclic codes over the same algebraic structure. Furthermore, an exhaustive classification of the various skew cyclic codes over the ring $\mathfrak{R}$ is presented, furnishing a meticulous and comprehensive overview of their diversity and characteristics. By addressing these facets, the manuscript endeavors to enhance comprehension regarding the attributes and utilizations of skew cyclic codes over the ring $\mathfrak{R}$, thereby enriching the field of algebraic coding theory.

References

[1] M. M. AL-Ashker and A. Q. Mahmoud Abu-Jazar, Skew constacyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$, Palestine Journal of Mathematics **5(2)**, 96-103, (2016).

[2] R. AL-Shorbassi and M. M. Al-Ashker, Skew $(\mu_1 + u\mu_2 + v\mu_3 + w\mu_4 + uv\mu_5 + vw\mu_6 + uw\mu_7 + uvw\mu_8)$ Constacyclic Codes over $F_q[u,v,w] / \langle u^2 - 1, v^2 - 1, w^2 - 1, uv - vu, vw - wv, uw - wu \rangle$, Palestine Journal of Mathematics, **12(4)**, 331-339, (2023).

[3] A. Bustomi, P. Santika and D. Suprijanto, Linear codes over the ring $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + w\mathbb{Z}_4 + uv\mathbb{Z}_4 + uw\mathbb{Z}_4 + vw\mathbb{Z}_4 + uvw\mathbb{Z}_4$. Arxiv.org/abs/1904.11117v1[cs.IT].

[4] K. Chatouh K. Guenda, T. A. Gulliver and L. Noui, Simplex and MacDonald codes over R_q, J. Appl. Math. Comput, **55(1-2)**, 455-478, (2017).

[5] K. Chatouh K. Guenda and T. A. Gulliver, New Classes of Codes Over $R_{q,p,m} = \mathbb{Z}_{p^m}[u_1, u_2, \cdots, u_q]/\langle u_i^2 = 0, u_i u_j = u_j u_i \rangle$ and Their Applications. Computational and Applied Mathematics, **39(3)**, 1-39, (2020).

[6] K. Chatouh, Some codes over $\mathcal{R} = \mathcal{R}_1\mathcal{R}_2\mathcal{R}_3$ and their applications in secret sharing schemes. Afr. Mat. **35**, 1 (2024)

[7] H. Q. Dinh, T. Bag, A. K. Upadhyay,R. Bandi and R. Tansuchat, A class of skew cyclic codes and application in quantum codes construction. Discrete Mathematics, **344(2)**, 112-189, (2021).

[8] Hammons A.R., Kumar V., Calderbank A.R., Sloane N.J.A., Solé P.: The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes. IEEE Trans. Inform. Theory **40**, 301-319 (1994).

[9] N. ur Rehman, M. Azmi and G. Mohammad, Reversible cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + \ldots + u^{k-1}\mathbb{F}_2$, Palestine Journal of Mathematics, **12(2)**, 395-407, (2023).

[10] M. Malki and K. Chatouh, Construction of linear codes over $\mathcal{R} = \sum_{s=0}^{4} v_5^s \mathcal{A}_4$. Mathematical Modeling and Computing, **10(1)**, 147-158, (2023).

[11] B. R. Mcdonald, Finite rings with identity. Marcel Dekker Incorporated, **28**, 1974.

[12] Melakhessou, A., Chatouh, K. & Guenda, K. DNA multi-secret sharing schemes based on linear codes over $\mathbb{Z}_4 \times R$. J. Appl. Math. Comput. **69**, 4833-4853 (2023)

[13] R. Mohammadi, S. Rahimi and H. Mousavi, On skew cyclic codes over a finite ring. Iranian J. Math. Sci. Inf. **14(1)**, 135-145, (2019).

[14] M. Reza Alimoradi, Decoding of cyclic codes over a class of finite rings, Palestine Journal of Mathematics, **12(2)**, 321-328, (2023).

[15] D. B. Ranya and B. Aicha, Skew Constacyclic and LCD Codes over $\mathbb{F}_q + v\mathbb{F}_q$. ArXiv:1902.08557v1 [cs.IT] 22 Feb 2019.

[16] M. Shi, T. Yao, A. Alahmadi and P. Solé, Skew cyclic codes over $F_q + vF_q + v^2F_q$, IEICE Transactions on Fundamentals of Electronics, communications and computer science, E98-A, 1 August, 1845-1848, 2015.

[17] M. Shi and P. Solé, Skew cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q + \ldots + v^{m-1}\mathbb{F}_q$, Proceedings International Workshop on the Arithmetic of Finite Fields, 2015.

Author information

Karima Chatouh, Laboratoire D´applications des Mathématiques à L´informatique et à L´électronique. Faculty of Economic, Commercial and Management Sciences University of Batna 1, Batna, Algeria.
E-mail: karima.chatouh@univ-batna.dz

Received: 2023-12-08
Accepted: 2024-05-22