TWMS J. App. and Eng. Math. V.15, N.3, 2025, pp. 511-525

SKEW-CYCLIC LINEAR CODES OVER THE FINITE RING $\mathcal{R}_p = \mathbb{F}_p[v_1, v_2, \cdots, v_\tau]/\langle v_i^2 = 1, v_iv_j - v_jv_i\rangle$: AN IN-DEPTH EXPLORATION

K. CHATOUH[1*], §

Abstract. This article introduces novel advancements in the realm of linear codes over the ring of integers modulo a prime, denoted as $\mathcal{R}_p = \mathbb{F}_p[v_1, v_2, \cdots, v_\tau]/\langle v_i^2 = 1, v_iv_j - v_jv_i\rangle$, with $\tau \geq 1$, $p = q^s$ and q is an odd prime. Specifically, we present a new Gray map and Gray images tailored for linear codes over $\mathcal{R}_p$, facilitating efficient representation and manipulation of these codes. Building upon this foundation, the study delves into the characterization and properties of skew cyclic codes over $\mathcal{R}_p$, a class of linear codes with intriguing mathematical structures. The investigation of skew cyclic linear code properties reveals new insights into their algebraic properties. This work not only contributes to the theoretical understanding of linear and skew cyclic codes over $\mathcal{R}_p$ but also suggests practical implications for coding theory.

Keywords: Linear codes, Skew cyclic codes, Gray map, Lee weight, Skew cyclic LCD codes.

AMS Subject Classification: 94B05, 11H71.

1. Introduction

In the realm of coding theory, error detection and correction have emerged as crucial techniques for ensuring reliable data transmission in various communication and storage systems. Linear codes, in particular, have been extensively studied for their capacity to detect and correct errors by exploiting algebraic structures, see Refs [1, 2, 5, 7, 13, 17, 18]. Among these, skew cyclic linear codes have garnered significant attention due to their intriguing properties and applications. In this article, we delve into the fascinating world of skew cyclic linear codes, focusing specifically on their construction and properties over the finite ring $\mathcal{R}_p$. Skew cyclic codes extend the concept of cyclic codes, which are known for their efficient encoding and decoding algorithms. The "skew" aspect arises from considering non-commutative ring structures, enabling a broader array of code constructions and applications. These codes have demonstrated their utility in various areas, such as data storage devices, secure communication channels, and fault-tolerant systems. However, their study over non-standard algebraic structures like finite rings introduces novel

[1] 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 ; ORCID: https://orcid.org/0000-0003-4061-1239.
[*] Corresponding author.
§ Manuscript received: September 5, 2023; accepted: February 15, 2024.
TWMS Journal of Applied and Engineering Mathematics, Vol.15, No.3;

challenges and opportunities. The finite ring $\mathcal{R}_p$, serves as a captivating setting for exploring skew cyclic linear codes. Unlike fields, rings may not possess multiplicative inverses for all elements, making the study of codes over rings a more intricate endeavor. Nonetheless, this complexity leads to codes that are better suited to specific scenarios, such as noisy environments where traditional codes may falter.

This article aims to provide a comprehensive overview of skew cyclic linear codes over $\mathcal{R}_p$, encompassing both theoretical foundations and practical implications. We will investigate the construction methods employed to generate these codes, shedding light on the algebraic structures that underpin their formation.

The article is structured into several key sections that delve into various aspects of linear and skew cyclic codes over the ring $\mathcal{R}_p$. In Section 2, the focus is on introducing the concept of Gray map and gray images within the context of linear codes over the ring $\mathcal{R}_p$. This section aims to provide readers with a fundamental understanding of these concepts and their significance in the realm of coding theory. Section 3 builds upon this foundation and delves into a comprehensive exploration of linear codes over $\mathcal{R}_p$, offering insights into their properties, characteristics, and potential applications. Transitioning to Section 4, the discussion shifts towards skew cyclic codes over $\mathcal{R}_p$, presenting readers with an in-depth analysis of these specialized codes. This section not only covers the definition and construction of skew cyclic codes but also delves into certain noteworthy properties that these codes exhibit when defined over the ring $\mathcal{R}_p$. By offering a deeper understanding of these properties, this section contributes to the broader comprehension of the versatility and capabilities of skew cyclic codes. Section 5 marks a significant aspect of the article, focusing specifically on skew cyclic LCD codes over $\mathcal{R}_p$. This section explores the intersection of skew cyclic codes and the LCD property.

In essence, this article seeks to unravel the intricacies of skew cyclic linear codes over the finite ring $\mathcal{R}_p$, offering readers a comprehensive understanding of their construction, properties, and applications. By bridging the gap between abstract algebra and real-world coding scenarios, we hope to illuminate the path toward more efficient and robust error-detection and error-correction strategies in diverse communication and storage systems.

2. Background Information

In this section, we delve into the essential background information that forms the foundation for our subsequent discussions. We begin by introducing the concept of a commutative ring denoted as $\mathcal{R}_p$, a fundamental algebraic structure where addition and multiplication operations adhere to the commutative property. Building upon this, we explore the notion of an inner product defined over the commutative ring $\mathcal{R}_p$, which provides a means to measure the geometric relationship between elements within this algebraic framework. Furthermore, we investigate a crucial construct known as a linear code over $\mathcal{R}_p$. This specialized code utilizes the algebraic properties of the commutative ring to efficiently represent and transmit information. By comprehending these interrelated concepts of the commutative ring $\mathcal{R}_p$, the inner product over it, and the linear code built upon it, we establish the necessary groundwork to delve deeper into the subsequent discussions on advanced applications and analyses. According to [4], we can express $\mathcal{R}_p$ by

$$\mathcal{R}_p = \mathbb{F}_p + \left(\sum_{i=1}^{\tau} v_i\right)\mathbb{F}_p + \left(\sum_{i=1}^{\tau-1} v_i \sum_{j=i+1}^{\tau} v_j\right)\mathbb{F}_p + \ldots + \left(\prod_{k=1}^{\tau} v_k\right)\mathbb{F}_p, \tag{1}$$

with $p = q^s$ and q is an odd prime. The collection $\mathcal{R}_p$ constitutes a commutative ring that encompasses a total of $q^{2^\tau s}$ elements, exhibiting a characteristic of q. An $\mathcal{R}_p$-module of $\mathcal{R}_p^n$ defines a linear code C with a length of n over this ring. Consider $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$, where x and y are arbitrary elements of $\mathcal{R}_p^n$. In this context, the inner product over $\mathcal{R}_p$ is defined as follows, $\langle x, y\rangle_{\mathcal{R}_p} = \sum_{i=1}^{n} x_i y_i$. The dual code $C^\perp$ of C is defined by $C^\perp = \{x \in \mathcal{R}_p^n | \langle x, y\rangle_{\mathcal{R}_p} = 0 \text{ for all } y \in C\}$. If $C \subset C^\perp$, we say the code is self-orthogonal, and if $C = C^\perp$ then, the code C is self-dual. Our proposal involves defining an asymmetric skew cyclic code based on the automorphism θ acting on the ring $\mathcal{R}_p$. This automorphism extends the one discussed in several articles [6, 11, 16].

$$\begin{array}{rccc} \theta & : & \mathcal{R}_p & \rightarrow & \mathcal{R}_p \\ & & c & \mapsto \theta(c), & \end{array} \tag{2}$$

where,

$$c = c_0 + \left(\sum_{i_1=1}^{\tau} v_{i_1}\right) c_1^{i_1} + \left(\sum_{i_1=1}^{\tau-1} v_{i_1} \sum_{i_2=i_1+1}^{\tau} v_{i_2}\right) c_2^{i_1 i_2} + \ldots + \left(\prod_{k=1}^{\tau} v_k\right) c_{2^\tau-1},$$

and

$$\theta(c) = (c_0)^{q^m} + \left(\sum_{i_1=1}^{\tau} v_{i_1}\right)(c_1^{i_1})^{q^m} + \left(\sum_{i_1=1}^{\tau-1} v_{i_1} \sum_{i_2=i_1+1}^{\tau} v_{i_2}\right)(c_2^{i_1 i_2})^{q^m} + \ldots + \left(\prod_{k=1}^{\tau} v_k\right)(c_{2^\tau-1})^{q^m},$$

so that

$$\theta(c) = \theta(c_0) + \left(\sum_{i_1=1}^{\tau} v_{i_1}\right)\theta(c_1^{i_1}) + \left(\sum_{i_1=1}^{\tau-1} v_{i_1} \sum_{i_2=i_1+1}^{\tau} v_{i_2}\right)\theta(c_2^{i_1 i_2}) + \ldots + \left(\prod_{k=1}^{\tau} v_k\right)\theta(c_{2^\tau-1}).$$

The order of this automorphism is given by $|\langle\theta\rangle| = \frac{s}{m}$. With respect to the automorphism θ acting on $\mathcal{R}_p$, the set

$$\mathcal{R}_p[x, \theta] = \{f(x) = \sum_{i=0}^{n} a_i x^i, a_i \in \mathcal{R}_p, \text{ for } 0 \leq i \leq n, \tag{3}$$

form a ring under the usual addition of polynomials and the multiplication, where

$$(ax^i)(bx^j) = a\theta^i(b)x^{i+j}. \tag{4}$$

Definition 2.1. *A linear code C of length n over $\mathcal{R}_p$ is said to be a skew cyclic code with respect to the automorphism θ if and only if for any codeword*

$$c = (c_0, c_1, c_2, \ldots, c_{n-1}) \in C \Rightarrow \sigma(c) = (\theta(c_{n-1}), \theta(c_0), \theta(c_1), \ldots, \theta(c_{n-2})) \in C, \tag{5}$$

where σ is a skew cyclic shift of C.

3. New Gray Map and Gray Images of Linear Codes over $\mathcal{R}_p$

In this section, we delve into a novel avenue of exploration within the realm of linear codes over $\mathcal{R}p$. Specifically, we introduce and discuss the concept of the "Gray map" and its associated "Gray images." These concepts present intriguing possibilities for enhancing the efficiency and versatility of linear codes, offering fresh perspectives on their representation and utilization. We establish the Gray map and Gray images for linear codes over $\mathcal{R}_p$, employing the Lee weight through a defined process

$$\begin{array}{cccc} \phi & : & \mathcal{R}_p & \rightarrow & \mathbb{F}_p^{2^\tau} \\ & & x & \mapsto & \phi(x) = H_{2^\tau} \cdot \mathrm{x}, \end{array} \tag{6}$$

where

$$x = x_0 + \left(\sum_{i_1=1}^{\tau} v_{i_1}\right) x_1^{i_1} + \left(\sum_{i_1=1}^{\tau-1} v_{i_1} \sum_{i_2=i_1+1}^{\tau} v_{i_2}\right) x_2^{i_1 i_2} + \ldots + \left(\prod_{k=1}^{\tau} v_k\right) x_{2^\tau-1}, \tag{7}$$

with $\mathrm{x} = (x_0, x_1^{i_1}, x_2^{i_1 i_2}, \ldots, x_{2^\tau-1})$. Furthermore, H_{2^τ} is a Hadamard matrix that is characterized by the equation

$$H_{2^\tau} = H_2 \otimes H_{2^{\tau-1}}, \tag{8}$$

where H_2 represents one of these matrices.

$$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 1 \\ 1 & 1, \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix},$$
$$\begin{bmatrix} -1 & -1 \\ -1 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 1 \\ -1 & -1 \end{bmatrix}, \begin{bmatrix} -1 & -1 \\ 1 & -1 \end{bmatrix}, \begin{bmatrix} 1 & -1 \\ -1 & -1 \end{bmatrix}.$$

This application can be extended to $\mathcal{R}_p^n$, yielding

$$\begin{array}{cccc} \Phi & : & \mathcal{R}_p^n & \rightarrow & \mathbb{F}_p^{2^\tau n} \\ & & x = (x_1, x_2, \ldots, x_n) & \mapsto & \Phi(x), \end{array} \tag{9}$$

with

$$x_t = (x_0)_t + \left(\sum_{i_1=1}^{\tau} v_{i_1}\right) (x_1^{i_1})_t + \left(\sum_{i_1=1}^{\tau-1} v_{i_1} \sum_{i_2=i_1+1}^{\tau} v_{i_2}\right) (x_2^{i_1 i_2})_t + \ldots + \left(\prod_{k=1}^{\tau} v_k\right) (x_{2^\tau-1})_t,$$

for $0 \leq t \leq n$.

When considering any two elements x and y belonging to $\mathcal{R}_p$, the Lee distance between them is defined as $d_{Lee}(x, y) = w_{Lee}(x - y)$. Given the definition of the Gray map, it becomes evident that we can discern the following outcomes.

Theorem 3.1. *The Gray map is an isometry from ($\mathcal{R}_p^n$, Lee distance) to ($\mathbb{F}_p^{2^\tau n}$, Hamming distance).*

Proof. Upon examining the definition of the Gray map, it becomes evident that Φ operates as a linear map. Simultaneously, it also functions as a map that preserves distances. □

Lemma 3.1. *If C is a linear code of length n over $\mathcal{R}_p$, with minimum Lee distance d_{Lee}, then $\Phi(C)$ is $[2^\tau n; k; d_{Ham}]_p$-linear codes over $\mathbb{F}_p$.*

Theorem 3.2. *If C is self orthogonal, then $\Phi(C)$ is self orthogonal.*

Proof. Consider two elements, denoted as x and y, belonging to a self-orthogonal code C. Under this assumption, it follows that $x \cdot y = 0$, where

$$x = x_0 + \left(\sum_{i_1=1}^{\tau} v_{i_1}\right) x_1^{i_1} + \left(\sum_{i_1=1}^{\tau-1} v_{i_1} \sum_{i_2=i_1+1}^{\tau} v_{i_2}\right) x_2^{i_1 i_2} + \ldots + \left(\prod_{k=1}^{\tau} v_k\right) x_{2^\tau-1},$$

and

$$y = y_0 + \left(\sum_{i_1=1}^{\tau} v_{i_1}\right) y_1^{i_1} + \left(\sum_{i_1=1}^{\tau-1} v_{i_1} \sum_{i_2=i_1+1}^{\tau} v_{i_2}\right) y_2^{i_1 i_2} + \ldots + \left(\prod_{k=1}^{\tau} v_k\right) y_{2^\tau - 1},$$

we have

$$\begin{aligned} 0 &= x_0 y_0 + x_1^{i_1} y_1^{i_1} + x_2^{i_1 i_2} y_2^{i_1 i_2} + \ldots + x_{2^\tau-1} y_{2^\tau-1}, \\ 0 &= \left(x_0 y_1^{i_1} + x_1^{i_1} y_0\right) + \ldots + \left(x_{2^\tau-2}^{i_1 i_2 \ldots i_{2^\tau-2}} y_{2^\tau-1} + x_{2^\tau-1} y_{2^\tau-2}^{i_1 i_2 \ldots i_{2^\tau-2}}\right), \\ &\vdots \\ 0 &= (x_0 y_{2^\tau-1} + x_{2^\tau-1} y_0) + \ldots + \left(x_1^{i_1} y_{2^\tau-2}^{i_1 i_2 \ldots i_{2^\tau-2}} + x_{2^\tau-2}^{i_1 i_2 \ldots i_{2^\tau-2}} y_1^{i_1}\right). \end{aligned}$$

Conversely, $\Phi(x) \cdot \Phi(y) = \langle H_{2^\tau} \cdot \mathrm{x}, H_{2^\tau} \cdot \mathrm{y}\rangle$. With reference to the earlier derived equations, it becomes evident that $\Phi(x) \cdot \Phi(y) = 0$, indicating that the code $\Phi(C)$ exhibits self-orthogonality. □

4. Linear Codes over $\mathcal{R}_p$

In this section, we embark on an in-depth journey into the intricacies of linear codes over $\mathcal{R}_p$. By elucidating the theoretical foundations and practical implications of linear codes over $\mathcal{R}_p$, we aim to provide a comprehensive understanding of this crucial coding paradigm. Through this exploration, we shed light on the advantages, challenges, and novel applications associated with linear codes over $\mathcal{R}_p$. Referring to [12], when considering an element denoted as c belonging to $\mathcal{R}_p$, it becomes possible to represent it in the following format

$$c = \langle \varpi, \vartheta \rangle_{\mathcal{R}_p}, \tag{10}$$

where

$$\varpi = \begin{bmatrix} \varpi_0 \\ \varpi_1 \\ \vdots \\ \varpi_{2^\tau-1} \end{bmatrix} \text{ and } \vartheta = H_{2^\tau} \cdot \begin{bmatrix} c_0 \\ c_1^{i_1} \\ \vdots \\ c_{2^\tau-1} \end{bmatrix},$$

we obtain

$$\begin{aligned} c = \varpi_0 (c_0 + c_1^{i_1} + c_2^{i_1 i_2} + \ldots + c_{2^\tau-1}) \\ +\varpi_1 (c_0 + c_1^{i_1} - c_2^{i_1 i_2} + \ldots - c_{2^\tau-1}) \\ \vdots \\ +\varpi_{2^\tau-1} (c_0 + c_1^{i_1} - c_2^{i_1 i_2} - \ldots - c_{2^\tau-1}), \end{aligned} \tag{11}$$

with

$$\begin{bmatrix} \varpi_0 \\ \varpi_1 \\ \vdots \\ \varpi_{2^\tau-1} \end{bmatrix} = \frac{1}{2^\tau} H_{2^\tau} \begin{bmatrix} 1 \\ v_1 \\ \vdots \\ \left(\prod_{k=1}^{\tau} v_k\right) \end{bmatrix}. \tag{12}$$

Example 4.1. *In the case of τ being equal to 4, we select*

$$H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

The orthogonal non-zero idempotents of a commutative ring $\mathcal{R}_p = \mathbb{F}_p + v_1\mathbb{F}_p + v_2\mathbb{F}_p + v_3\mathbb{F}_p + v_4\mathbb{F}_p + v_1v_2\mathbb{F}_p + v_1v_3\mathbb{F}_p + v_1v_4\mathbb{F}_p + v_2v_3\mathbb{F}_p + v_2v_4\mathbb{F}_p + v_3v_4\mathbb{F}_p + v_1v_2v_3\mathbb{F}_p + v_1v_2v_4\mathbb{F}_p + v_1v_3v_4\mathbb{F}_p + v_2v_3v_4\mathbb{F}_p + v_1v_2v_3v_4\mathbb{F}_p$ *are*

$$\begin{pmatrix} \varpi_0 \\ \varpi_1 \\ \varpi_2 \\ \varpi_3 \\ \varpi_4 \\ \varpi_5 \\ \varpi_6 \\ \varpi_7 \\ \varpi_8 \\ \varpi_9 \\ \varpi_{10} \\ \varpi_{11} \\ \varpi_{12} \\ \varpi_{13} \\ \varpi_{14} \\ \varpi_{15} \end{pmatrix} = \frac{1}{16} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_1v_2 \\ v_1v_3 \\ v_1v_4 \\ v_2v_3 \\ v_2v_4 \\ v_1v_2v_3 \\ v_1v_2v_4 \\ v_1v_3v_4 \\ v_2v_3v_4 \\ v_1v_2v_3v_4 \end{bmatrix},$$

we obtain

$$\begin{aligned}
\varpi_0 &= \frac{1}{16}(1 + v_1 + v_2 + v_3 + v_4 + v_1v_2 + v_1v_3 + v_1v_4 + v_2v_3 + v_2v_4 + v_3v_4 + v_1v_2v_3 + v_1v_2v_4 + v_1v_3v_4 + v_2v_3v_4 + v_1v_2v_3v_4), \\
\varpi_1 &= \frac{1}{16}(1 - v_1 + v_2 - v_3 + v_4 - v_1v_2 + v_1v_3 - v_1v_4 + v_2v_3 - v_2v_4 + v_3v_4 - v_1v_2v_3 + v_1v_2v_4 - v_1v_3v_4 + v_2v_3v_4 - v_1v_2v_3v_4), \\
\varpi_2 &= \frac{1}{16}(1 + v_1 - v_2 - v_3 + v_4 + v_1v_2 - v_1v_3 - v_1v_4 + v_2v_3 + v_2v_4 - v_3v_4 - v_1v_2v_3 + v_1v_2v_4 + v_1v_3v_4 - v_2v_3v_4 - v_1v_2v_3v_4), \\
\varpi_3 &= \frac{1}{16}(1 - v_1 - v_2 + v_3 + v_4 - v_1v_2 - v_1v_3 + v_1v_4 + v_2v_3 - v_2v_4 - v_3v_4 + v_1v_2v_3 + v_1v_2v_4 - v_1v_3v_4 - v_2v_3v_4 + v_1v_2v_3v_4), \\
\varpi_4 &= \frac{1}{16}(1 + v_1 + v_2 + v_3 - v_4 - v_1v_2 - v_1v_3 - v_1v_4 + v_2v_3 + v_2v_4 + v_3v_4 + v_1v_2v_3 - v_1v_2v_4 - v_1v_3v_4 - v_2v_3v_4 - v_1v_2v_3v_4), \\
\varpi_5 &= \frac{1}{16}(1 - v_1 + v_2 - v_3 - v_4 + v_1v_2 - v_1v_3 + v_1v_4 + v_2v_3 - v_2v_4 + v_3v_4 - v_1v_2v_3 - v_1v_2v_4 + v_1v_3v_4 - v_2v_3v_4 + v_1v_2v_3v_4), \\
\varpi_6 &= \frac{1}{16}(1 + v_1 - v_2 - v_3 - v_4 - v_1v_2 + v_1v_3 + v_1v_4 + v_2v_3 + v_2v_4 - v_3v_4 - v_1v_2v_3 - v_1v_2v_4 - v_1v_3v_4 + v_2v_3v_4 + v_1v_2v_3v_4), \\
\varpi_7 &= \frac{1}{16}(1 - v_1 - v_2 + v_3 - v_4 + v_1v_2 + v_1v_3 - v_1v_4 + v_2v_3 - v_2v_4 - v_3v_4 + v_1v_2v_3 - v_1v_2v_4 + v_1v_3v_4 + v_2v_3v_4 - v_1v_2v_3v_4), \\
\varpi_8 &= \frac{1}{16}(1 + v_1 + v_2 + v_3 + v_4 + v_1v_2 + v_1v_3 + v_1v_4 - v_2v_3 - v_2v_4 - v_3v_4 - v_1v_2v_3 - v_1v_2v_4 - v_1v_3v_4 - v_2v_3v_4 - v_1v_2v_3v_4), \\
\varpi_9 &= \frac{1}{16}(1 - v_1 + v_2 - v_3 + v_4 - v_1v_2 + v_1v_3 - v_1v_4 - v_2v_3 + v_2v_4 - v_3v_4 + v_1v_2v_3 - v_1v_2v_4 + v_1v_3v_4 - v_2v_3v_4 + v_1v_2v_3v_4), \\
\varpi_{10} &= \frac{1}{16}(1 + v_1 - v_2 - v_3 + v_4 + v_1v_2 - v_1v_3 - v_1v_4 - v_2v_3 - v_2v_4 + v_3v_4 + v_1v_2v_3 - v_1v_2v_4 - v_1v_3v_4 + v_2v_3v_4 + v_1v_2v_3v_4), \\
\varpi_{11} &= \frac{1}{16}(1 - v_1 - v_2 + v_3 + v_4 - v_1v_2 - v_1v_3 + v_1v_4 - v_2v_3 + v_2v_4 + v_3v_4 - v_1v_2v_3 - v_1v_2v_4 + v_1v_3v_4 + v_2v_3v_4 - v_1v_2v_3v_4), \\
\varpi_{12} &= \frac{1}{16}(1 + v_1 + v_2 + v_3 - v_4 - v_1v_2 - v_1v_3 - v_1v_4 - v_2v_3 - v_2v_4 - v_3v_4 - v_1v_2v_3 + v_1v_2v_4 + v_1v_3v_4 + v_2v_3v_4 + v_1v_2v_3v_4), \\
\varpi_{13} &= \frac{1}{16}(1 - v_1 + v_2 - v_3 - v_4 + v_1v_2 - v_1v_3 + v_1v_4 - v_2v_3 + v_2v_4 - v_3v_4 + v_1v_2v_3 + v_1v_2v_4 - v_1v_3v_4 + v_2v_3v_4 - v_1v_2v_3v_4), \\
\varpi_{14} &= \frac{1}{16}(1 + v_1 - v_2 - v_3 - v_4 - v_1v_2 + v_1v_3 + v_1v_4 - v_2v_3 - v_2v_4 + v_3v_4 + v_1v_2v_3 + v_1v_2v_4 + v_1v_3v_4 - v_2v_3v_4 - v_1v_2v_3v_4), \\
\varpi_{15} &= \frac{1}{16}(1 - v_1 - v_2 + v_3 - v_4 + v_1v_2 + v_1v_3 - v_1v_4 - v_2v_3 + v_2v_4 + v_3v_4 - v_1v_2v_3 + v_1v_2v_4 - v_1v_3v_4 - v_2v_3v_4 + v_1v_2v_3v_4).
\end{aligned}$$

Consider a linear code denoted as C, with a length n, defined over $\mathcal{R}_p$. Additionally, let C_i represent linear codes of length n over $\mathbb{F}_p$, for $0 \leq i \leq 2^\tau - 1$.

Then, $C_0 = \{c_0 + (\sum\limits_{i_1=1}^{\tau} c_1^{i_1}) + (\sum\limits_{i_1=1}^{\tau-1} \sum\limits_{i_2=i_1+1}^{\tau} c_2^{i_1 i_2}) + \ldots + c_{2^\tau-1}, \exists c_0, c_1^{i_1}, c_2^{i_1 i_2}, \ldots, c_{2^\tau-1} \in \mathbb{F}_p, \forall c \in C\}$,

$C_1 = \{c_0 + (-1)^{i_1}(\sum\limits_{i_1=1}^{\tau} c_1^{i_1}) + (-1)^{i_2}(\sum\limits_{i_1=1}^{\tau-1} \sum\limits_{i_2=i_1+1}^{\tau} c_2^{i_1 i_2}) + \ldots - c_{2^\tau-1}, \exists c_0, c_1^{i_1}, c_2^{i_1 i_2}, \ldots, c_{2^\tau-1} \in \mathbb{F}_p, \forall c \in C\}$,

$\vdots$

$C_{2^\tau-1} = \{c_0+(\sum_{i_1=1}^{\tau} c_1^{i_1})-(\sum_{i_1=1}^{\tau-1}\sum_{i_2=i_1+1}^{\tau} c_2^{i_1i_2})+\ldots-c_{2^\tau-1}, \exists c_0, c_1^{i_1}, c_2^{i_1i_2},\ldots,c_{2^\tau-1}\in\mathbb{F}_p, \forall c\in C\}$.

Definition 4.1. *Linear codes C of length n over $\mathcal{R}_p$, can be uniquely expressed as*

$$C = \bigoplus_{i=0}^{2^\tau-1} \varpi_i C_i. \tag{13}$$

This description of C outlines a number of outcomes, among them the subsequent ones.

Theorem 4.1. *Let C be a linear code of length n over $\mathcal{R}_p$, then*

$$\Phi(C) = \bigotimes_{i=0}^{2^\tau-1} C_i \text{ and } |C| = |C_0||C_1|\ldots|C_{2^\tau-1}|. \tag{14}$$

Proof. Applying the definition provided in Equation 4.1 along with the insights from Theorem 3.1. □

Corollary 4.1. *Let C be a linear code of length n over $\mathcal{R}_p$, then $\Phi(C^\perp) = [\Phi(C)]^\perp$. Further, C is a self-dual code if and only if $\Phi(C)$ is a self-dual code.*

Proof. Considering an element c from C and c' from $C^\perp$, it follows that $c\cdot c'=0$. This conclusion is based on the insights provided by Theorem 3.2. Consequently, we arrive at the outcome that $\Phi(c)\cdot\Phi(c')=0$. This leads us to the relation

$$\Phi(C^\perp) \subseteq [\Phi(C)]^\perp, \tag{15}$$

With reference to Theorem 3.1, we deduce the following relationship

$$|\Phi(C^\perp)| = |\,[\Phi(C)]^\perp\,|, \tag{16}$$

By combining Equations (15) and (16), we arrive at the conclusion $\Phi(C^\perp) = [\Phi(C)]^\perp$. The demonstration for the second aspect is evidently straightforward. □

Theorem 4.2. *Let $C = \bigoplus_{i=0}^{2^\tau-1} \varpi_i C_i$ be a linear code of length n over $\mathcal{R}_p$, then $C^\perp = \bigoplus_{i=0}^{2^\tau-1} \varpi_i C_i^\perp$. Further, C is self-dual if and only if C_i, for $0\le i\le 2^\tau-1$ are self-duals.*

Proof. Let $C^\perp$ be a linear code over $\mathcal{R}_p$. If,

$\overline{C}_0 = \{c_0+(\sum_{i_1=1}^{\tau} c_1^{i_1})+(\sum_{i_1=1}^{\tau-1}\sum_{i_2=i_1+1}^{\tau} c_2^{i_1i_2})+\ldots+c_{2^\tau-1}, \exists c_0, c_1^{i_1}, c_2^{i_1i_2},\ldots,c_{2^\tau-1}\in\mathbb{F}_p, \forall c\in C^\perp\}$,

$\overline{C}_1 = \{c_0+(-1)^{i_1}(\sum_{i_1=1}^{\tau} c_1^{i_1})+(-1)^{i_2}(\sum_{i_1=1}^{\tau-1}\sum_{i_2=i_1+1}^{\tau} c_2^{i_1i_2})+\ldots-c_{2^\tau-1}, \exists c_0, c_1^{i_1}, c_2^{i_1i_2},\ldots,c_{2^\tau-1}\in\mathbb{F}_p, \forall c\in C^\perp\}$,

$\vdots$

$\overline{C}_{2^\tau-1} = \{c_0+(\sum_{i_1=1}^{\tau} c_1^{i_1})-(\sum_{i_1=1}^{\tau-1}\sum_{i_2=i_1+1}^{\tau} c_2^{i_1i_2})+\ldots-c_{2^\tau-1}, \exists c_0, c_1^{i_1}, c_2^{i_1i_2},\ldots,c_{2^\tau-1}\in\mathbb{F}_p, \forall c\in C^\perp\}$,

Considering the definition of c in Equation (11), it follows that $C^\perp = \bigoplus_{i=0}^{2^\tau-1} \varpi_i \overline{C}_i$. It is evident that $\overline{C}_i \subseteq C_i^\perp$, for $0\le i\le 2^\tau-1$. Furthermore, if we select an element c from

$C_i^{\perp}$, for $0 \leq i \leq 2^{\tau}-1$, this implies that $c \cdot y = 0$ holds for all y in C_i. For an element $\overline{x}$ belonging to C, the following holds

$$\frac{1}{2^{\tau}}\left(1+\left(\sum_{i_1=1}^{\tau} v_{i_1}\right)+\left(\sum_{i_1=1}^{\tau-1} v_{i_1} \sum_{i_2=i_1+1}^{\tau} v_{i_2}\right)+\ldots+\left(\prod_{k=1}^{\tau} v_k\right)\right) c \cdot \overline{x} = 0$$

so,

$$\frac{1}{2^{\tau}}\left(1+\left(\sum_{i_1=1}^{\tau} v_{i_1}\right)+\left(\sum_{i_1=1}^{\tau-1} v_{i_1} \sum_{i_2=i_1+1}^{\tau} v_{i_2}\right)+\ldots+\left(\prod_{k=1}^{\tau} v_k\right)\right) c = 0.$$

However, the uniqueness of the code $C^{\perp}$ becomes apparent. As a result, it follows that $c \in \overline{C}_i$, for $0 \leq i \leq 2^{\tau}-1$. Ultimately, we deduce that $\overline{C}_i = C_i^{\perp}$ holds for $0 \leq i \leq 2^{\tau}-1$, and we arrive at the expression

$$C^{\perp} = \bigoplus_{i=0}^{2^{\tau}-1} \varpi_i C_i^{\perp}.$$

Exploiting the self-duality property of the code C and taking into account Theorem 4.1, we derive the following equivalences

$$\begin{aligned} C^{\perp} = C \quad &\Leftrightarrow \quad \Phi\left(C^{\perp}\right) = \Phi\left(C\right) \\ &\Leftrightarrow \quad \bigotimes_{i=0}^{2^{\tau}-1} C_i^{\perp} = \bigotimes_{i=0}^{2^{\tau}-1} C_i \\ &\Leftrightarrow \quad C_i^{\perp} = C_i, \text{ for } 0 \leq i \leq 2^{\tau}-1. \end{aligned}$$

Consequently, we can ascertain that C_i, for $0 \leq i \leq 2^{\tau}-1$, are inherently self-dual codes. □

Theorem 4.3. *If G_i, for $0 \leq i \leq 2^{\tau}-1$ are generator matrices of C_i, for $0 \leq i \leq 2^{\tau}-1$ then the generator matrix of C is*

$$G = \frac{1}{2^{\tau}}\left[H_{2^{\tau}}\right] \cdot \begin{bmatrix} 1 \\ v_1 \\ \vdots \\ \left(\prod_{k=1}^{\tau} v_k\right) \end{bmatrix} \cdot \begin{bmatrix} G_0 \\ G_1 \\ \vdots \\ G_{2^{\tau}-1} \end{bmatrix}^{\top}. \tag{17}$$

Through the application of the Gray map Φ, the subsequent outcome can be readily derived.

Theorem 4.4. *If C is a linear code of length n over $\mathcal{R}_p$ with generator matrix G, then*

$$\Phi(G) = \begin{bmatrix} G_0 & G_0 & G_0 & \ldots & G_0 \\ G_1 & -G_1 & G_1 & \ldots & -G_1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ G_{2^{\tau}-1} & -G_{2^{\tau}-1} & -G_{2^{\tau}-1} & \ldots & -G_{2^{\tau}-1} \end{bmatrix}. \tag{18}$$

Proof. The result can be acquired using the matrix provided below

$$\Phi(G) = \begin{bmatrix} \Phi\left(\varpi_0 G_0\right) \\ \Phi\left(\varpi_1 G_1\right) \\ \vdots \\ \Phi\left(\varpi_{2^{\tau}-1} G_{2^{\tau}-1}\right) \end{bmatrix}.$$

□

Example 4.2. *In the context of* $\mathcal{R}_4 = \mathbb{F}_4 + v_1\mathbb{F}_4 + v_2\mathbb{F}_4 + v_1v_2\mathbb{F}_4$*, given the generator matrices* $G_i = \begin{bmatrix} 1 & w \\ w & 1 \end{bmatrix}$ *for* C_i*, where* $0 \leq i \leq 3$*, the resulting code* $\Phi(C)$ *generated by*

$$\Phi(G) = \begin{bmatrix} 1 & w & 1 & w & 1 & w & 1 & w \\ w & 1 & w & 1 & w & 1 & w & 1 \\ 1 & w & w^2+w & w^2+1 & 1 & w & w^2+w & w^2+1 \\ w & 1 & w^2+1 & w^2+w & w & 1 & w^2+1 & w^2+w \\ 1 & w & 1 & w & w^2+w & w^2+1 & w^2+w & w^2+1 \\ w & 1 & w & 1 & w^2+1 & w^2+w & w^2+1 & w^2+w \\ 1 & w & w^2+w & w^2+1 & w^2+w & w^2+1 & 1 & w \\ w & 1 & w^2+1 & w^2+w & w^2+1 & w^2+w & w & 1 \end{bmatrix}.$$

5. Skew Cyclic Codes over $\mathcal{R}_p$

The following section delves into the realm of skew cyclic codes over $\mathcal{R}_p$. This investigation revolves around the intricate study of codes with distinctive properties, specifically within the algebraic structure of the ring $\mathcal{R}_p$. Skew cyclic codes, an essential subset of linear codes, possess remarkable characteristics that stem from their cyclic nature. In this section, we explore the fundamental concepts, properties, and encoding techniques associated with skew cyclic codes over the ring $\mathcal{R}_p$. By delving into the intricacies of this coding theory, we aim to illuminate the potential applications and significance of skew cyclic codes within the context of $\mathcal{R}_p$.

Theorem 5.1. *Let* $C = \bigoplus_{i=0}^{2^\tau-1} \varpi_i C_i$ *be a linear code over* $\mathcal{R}_p$ *of length* n *where* C_i*, for* $0 \leq i \leq 2^\tau - 1$ *are linear codes of length* n *over* $\mathbb{F}_p$*. Then* C *is a skew cyclic code over* $\mathcal{R}_p$ *if and only if* C_i*, for* $0 \leq i \leq 2^\tau - 1$ *are skew cyclic codes over* $\mathbb{F}_p$*, with respect to the automorphism* θ*.*

Proof. Considering an element $c = (c^0, c^1, \ldots, c^{n-1})$ within the set C, it follows that c^k can be expressed as $\sum_{i=0}^{2^\tau-1} \varpi_i c_i^k$, where $0 \leq k \leq n-1$. This relationship elucidates the manner in which

$$\begin{aligned} c_0 &= (c_0^0, c_0^1, \ldots, c_0^{n-1}) \in C_0, \\ c_1 &= (c_1^0, c_1^1, \ldots, c_1^{n-1}) \in C_1, \\ &\vdots \\ c_{2^\tau-1} &= (c_{2^\tau-1}^0, c_{2^\tau-1}^1, \ldots, c_{2^\tau-1}^{n-1}) \in C_{2^\tau-1}. \end{aligned}$$

Given that C_i, where $0 \leq i \leq 2^\tau - 1$, represents a collection of skew cyclic codes, it follows that $\sigma(c_i)$ belongs to C_i for each value of i within the specified range. Furthermore, assuming the equation

$$\theta(c^k) = \sum_{i=0}^{2^\tau-1} \varpi_i \theta(c_i^k), \text{ for } 0 \leq k \leq n-1,$$

we can then proceed to derive the expression

$$\begin{aligned} \sigma(c) &= (\theta(c^{n-1}), \theta(c^0), \theta(c^1), \ldots, \theta(c^{n-2})) \\ &= \sigma(c_0) + \left(\sum_{i_1=1}^{\tau} v_{i_1}\right)\sigma(c_1^{i_1}) + \left(\sum_{i_1=1}^{\tau-1}\sum_{i_2=i_1+1}^{\tau} v_{i_1}v_{i_2}\right)\sigma(c_2^{i_1 i_2}) \\ &\quad + \ldots + \left(\prod_{k=1}^{\tau} v_k\right)\sigma(c_{2^\tau-1}) \in C, \end{aligned}$$

This implication leads us to conclude that $\sigma(c) \in C$, thereby establishing that the code C is skew cyclic over $\mathcal{R}_p$. Similar reasoning applies for the converse implication. $\square$

Corollary 5.1. *The dual code $C^{\perp}$ is a skew cyclic code over $\mathcal{R}_p$, if C is a skew cyclic code over $\mathcal{R}_p$.*

Proof. In the event that C is formed as the direct sum $\bigoplus_{i=0}^{2^\tau-1} \varpi_i C_i$, establishing it as a skew cyclic code over $\mathcal{R}_p$, Theorem 5.1 comes into play. According to this theorem, it can be deduced that C_i, for $0 \leq i \leq 2^\tau - 1$, stands as skew cyclic codes over $\mathbb{F}_p$. Furthermore, drawing insights from [3], it follows that $C_i^{\perp}$, considering the same range for i, also hold the status of skew cyclic codes over $\mathbb{F}_p$. By leveraging the theorems outlined in 4.2 and 5.1, it becomes apparent that a compelling deduction can be made: $C^{\perp}$ emerges as a skew cyclic code over $\mathcal{R}_p$. $\square$

This culminates in a clear corollary which, in turn, leads to the realization of the following set of outcomes.

Corollary 5.2. *The code C is a self-dual skew cyclic code over $\mathcal{R}_p$ if and only if C_i, for $0 \leq i \leq 2^\tau - 1$ are self-dual skew cyclic codes over $\mathbb{F}_p$.*

Proof. To establish the validity of this proposition, it is adequate to utilize Theorems 4.2 and 5.1. $\square$

Theorem 5.2. *Let $C = \bigoplus_{i=0}^{2^\tau-1} \varpi_i C_i$ be a skew cyclic code of length n over $\mathcal{R}_p$. Assume that $g_i(x)$, is a generator polynomial of C_i, for $0 \leq i \leq 2^\tau - 1$, then $|C| = p^{2^\tau n - \sum_{i=0}^{2^\tau-1}(deg\ g_i(x))}$ and $C = \langle \varpi_0 g_0(x), \varpi_1 g_1(x), \ldots, \varpi_{2^\tau-1} g_{2^\tau-1}(x)\rangle$.*

Proof. According to Theorem 4.1 the equality below is satisfied

$$|C| = |C_0||C_1| \ldots |C_{2^\tau-1}| = p^{2^\tau n - \sum_{i=0}^{2^\tau-1}(deg\ g_i(x))}.$$

Let $C_i = \langle g_i(x)\rangle$, for $0 \leq i \leq 2^\tau - 1$ and $C = \bigoplus_{i=0}^{2^\tau-1} \varpi_i C_i$ this assumption allows us to write C in the form $C = \{c(x) = \sum_{i=0}^{2^\tau-1} \varpi_i f_i(x) g_i(x),\ \forall f_i(x) \in \mathbb{F}_p[x, \theta],\ \text{for } 0 \leq i \leq 2^\tau - 1\}$, so

$$C \subseteq \langle \varpi_0 g_0(x), \varpi_1 g_1(x), \ldots, \varpi_{2^\tau-1} g_{2^\tau-1}(x)\rangle.$$

On the other hand, we have $\sum_{i=0}^{2^\tau-1} \varpi_i h_i(x) g_i(x) \in \langle \varpi_0 g_0(x), \varpi_1 g_1(x), \ldots, \varpi_{2^\tau-1} g_{2^\tau-1}(x)\rangle$, but $h_i(x) \in \mathcal{R}_p[x, \theta]/(x^n - 1)$, for $0 \leq i \leq 2^\tau - 1$, thus there exists $f_i(x) \in \mathbb{F}_p[x, \theta]$, such as $\varpi_i h_i(x) = \varpi_i f_i(x)$, for $0 \leq i \leq 2^\tau - 1$, so that $\langle \varpi_0 g_0(x), \varpi_1 g_1(x), \ldots, \varpi_{2^\tau-1} g_{2^\tau-1}(x)\rangle \subseteq C$, we find $C = \langle \varpi_0 g_0(x), \varpi_1 g_1(x), \ldots, \varpi_{2^\tau-1} g_{2^\tau-1}(x)\rangle$. $\square$

Theorem 5.3. *If C_i, for $0 \leq i \leq 2^\tau - 1$ be skew cyclic codes over $\mathbb{F}_p$ and $g_i(x)$, for $0 \leq i \leq 2^\tau - 1$ be the generator polynomials of these codes, then there is a unique polynomial $g(x) \in \mathcal{R}_p[x, \theta]$ such that $C = \langle g(x)\rangle$ and $g(x)$ is a right divisor of $x^n - 1$, where $g(x) = \sum_{i=0}^{2^\tau-1} \varpi_i g_i(x)$.*

Proof. Utilizing Theorem 4.6 from [16], one can make analogous arguments. $\square$

Corollary 5.3. *Let C_i, for $0 \leq i \leq 2^\tau - 1$ be skew cyclic codes over $\mathbb{F}_p$ and $g_i(x)$, for $0 \leq i \leq 2^\tau - 1$ their generator polynomials, such that $x^n - 1 = h_i(x)g_i(x)$ in $\mathbb{F}_p[x, \theta]$. If C is a skew cyclic code over $\mathcal{R}_p$, then $C^\perp = \sum_{i=0}^{2^\tau-1} \varpi_i \overline{h}_i(x)$, where $\overline{h}_i(x)$ are the reciprocal polynomials of $h_i(x)$ and $\overline{h}_i(x) = x^{deg(g_i(x))} g_i(x^{-1})$, for $0 \leq i \leq 2^\tau - 1$. Furthermore, $|C^\perp| = p^{\sum_{i=0}^{2^\tau-1} (deg\ g_i(x))}$.*

Proof. The proof closely parallels the one provided for Theorem 5.2. □

Example 5.1. *Let $q = 2$, $\tau = 3$, $s = 6$ and $\mathbb{F}_{64} = \mathbb{F}_2[\alpha]$, where $\alpha^6 = \alpha^3 + 1$ assume that $\theta(\alpha) = \alpha^8$ and $n = 9$, then $x^9 - 1 = (x + 1)(x^6 + x^3 + 1)(x^2 + x + 1)$. Note that $C_i = C_i^\perp = \langle f_i(x) = f_i^*(x) = x^6 + x^3 + 1 \rangle$, for $0 \leq i \leq 7$ are self-dual skew cyclic codes over $\mathbb{F}_{64}$. Then, $C = C^\perp = \langle \varpi_0(x^6 + x^3 + 1), \varpi_1(x^6 + x^3 + 1), \varpi_2(x^6 + x^3 + 1), \varpi_3(x^6 + x^3 + 1)(x), \varpi_4(x^6 + x^3 + 1), \varpi_5(x^6 + x^3 + 1), \varpi_6(x^6 + x^3 + 1), \varpi_7(x^6 + x^3 + 1) \rangle$ is a self-dual skew cyclic code over $\mathcal{R}_p$.*

5.1. **Certain Properties of Skew Cyclic Codes over $\mathcal{R}_p$.** In the preceding section, our investigation revolved around analyzing the structural characteristics of skew cyclic codes over the ring $\mathcal{R}_p$. We achieved this by delving into a decomposition theorem. In the current section, we are furthering our exploration by demonstrating their idempotent generators.

The basis for our current approach is grounded in a result presented in [9]. This result asserts that, under the conditions where $\gcd(n, \frac{s}{m}) = 1$ and $\gcd(n, p) = 1$ hold, if we have a monic right divisor, denoted as $f(x)$, of $x^n - 1$ within the algebraic structure $\mathbb{F}_p[x, \theta]$, then it is guaranteed that $f(x)$ also belongs to $\mathbb{F}_p[x]$.

Theorem 5.4. [9] *Let $f(x) \in \mathbb{F}_p[x, \theta]$ be a monic right divisor of $(x^n - 1)$ and $C = \langle f(x) \rangle$. If $gcd(n, \frac{s}{m}) = 1$ and $gcd(n, p) = 1$ then, there exists an idempotent polynomial $e(x) \in \mathcal{R}_p[x, \theta]$ such that $C = \langle e(x) \rangle$.*

Corollary 5.4. *Let $gcd(n, \frac{s}{m}) = 1$ and $gcd(n, p) = 1$, if $C = \bigoplus_{i=0}^{2^\tau-1} \varpi_i C_i$ is a skew cyclic code of length n over $\mathcal{R}_p$. Then, C has an idempotent generator $e(x)$ in $\mathcal{R}_p[x, \theta]$.*

Proof. By applying Theorem 5.4, we establish the existence of idempotent generators, denoted as $e_i(x)$, for each C_i within the algebraic structure $\mathbb{F}_p[x, \theta]$. Additionally the code C_i is generated by $e_i(x)$, for $0 \leq i \leq 2^\tau - 1$.

Furthermore, as outlined in Theorem 5.3, it is affirmed that the idempotent generator $e(x)$ can be expressed as $e(x) = \sum_{i=0}^{2^\tau-1} \varpi_i e_i(x)$ for C, where ϖ_i is a coefficient. This theorem offers a comprehensive understanding of how $e(x)$ can be constructed as a combination of the idempotent generators $e_i(x)$ for the entire code. □

Theorem 5.5. *Let $gcd(n, \frac{s}{m}) = 1$ and $gcd(n, p) = 1$, if $C = \bigoplus_{i=0}^{2^\tau-1} \varpi_i C_i$ is a skew cyclic code of length n over $\mathcal{R}_p$, then $C^\perp$ has an idempotent generator $e'(x) = 1 - e(x^{-1})$ in $\mathcal{R}_p[x, \theta]$.*

Proof. Suppose that we have idempotent generators $e_i(x)$ for the subgroups C_i in $\mathbb{F}_p[x, \theta]$, for $0 \leq i \leq 2^\tau - 1$. As detailed in [10], each corresponding dual code $C_i^\perp$ possesses an idempotent generator denoted as $e_i^{'}(x)$, which can be expressed as $e_i^{'}(x) = 1 - e_i(x^{-1})$, for $0 \leq i \leq 2^{\tau} - 1$.

Now, drawing upon Theorem 5.3, we can deduce that the overall dual code $C^{\perp}$ is equipped with an idempotent generator denoted as $e^{'}(x)$. This generator is given by the expression $e^{'}(x) = 1 - e(x^{-1}) = \sum_{i=0}^{2^{\tau}-1} \varpi_i e_i^{'}(x)$. □

Additionally, as per the information presented in [8], when the conditions $\gcd(n, \frac{s}{m}) = 1$ are met, and C is a skew cyclic code with a length of n over the ring $\mathcal{R}_p$, it follows that C also qualifies as a cyclic code with the same length n over the same ring $\mathcal{R}_p$. This realization leads us directly to the following result.

Theorem 5.6. *Let* $x^n - 1 = \prod_{j=1}^{l} f_j^{l_j}(x)$ *and* $gcd(n, \frac{s}{m}) = 1$ *where,* $f_j(x) \in \mathbb{F}_p[x, \theta]$ *is irreducible. Then, the number of skew cyclic codes of length* n *over* $\mathcal{R}_p$ *is* $\prod_{j=1}^{l} (l_j + 1)^8$.

Proof. When the conditions $\gcd(n, \frac{s}{m}) = 1$ and $f_j(x) \in \mathbb{F}_p[x]$ are satisfied, the count of skew cyclic codes with a length of n over $\mathbb{F}_p$ equals $\prod_{j=1}^{l} (l_j + 1)$.

Moreover, we can extend this concept to skew cyclic codes with a length of n over $\mathcal{R}_p$, where the number of such codes is equivalent to the count of ideals in $\mathcal{R}_p[x, \theta]$ modulo the factor $(x^n - 1)$. By referencing Definition 4.1, it is established that the count of skew cyclic codes of length n over $\mathcal{R}_p$ is $\prod_{j=1}^{l} (l_j + 1)^8$. □

5.2. **Gray Images of Skew Cyclic Codes with Good Parameters.** According to the reference provided in [15], a linear code over a finite field is considered to have good parameters if it satisfies certain bounds, such as those defined by Singleton, Griesmer, or Gilbert-Varshamov. These bounds are articulated through the following expressions: $d \leq n - k + 1$, $n \geq \sum_{i=0}^{k-1} \frac{d_H}{q^i}$ and $A_q(n, d) \geq \frac{q^n}{\sum_{i=0}^{d-1} C_n^i (q-1)^i}$ respectively. In the provided context, $A_q(n, d)$ represents the maximum size of a q-ary code with a block length of n and a minimum distance of d. Within the scope of our research, a primary objective is to construct codes with good parameters over the finite field $\mathbb{F}_p$, originating from the rich structure of skew cyclic codes over the ring $\mathcal{R}_p$. This goal is motivated by the practical necessity of implementing error-correcting codes in finite field settings, frequently encountered in digital communication systems, cryptography, and other information processing applications. Through a computer search conducted using Magma, Sage, and the database (http://www.codetables.de), we have identified several codes exhibiting optimal or nearly optimal parameters. Presented below is a selection of these codes for reference.

Example 5.2. *Consider* $\mathcal{R}_7 = \mathbb{F}_7 + v_1\mathbb{F}_7 + v_2\mathbb{F}_7 + v_1v_2\mathbb{F}_7$*, the factorization of* $x^{20} - 1 = (x+1)(x+6)(x^2+1)(x^4+x^3+x^2+x+1)(x^4+3x^3+4x^2+4x+1)(x^4+4x^3+4x^2+3x+1)(x^4+6x^3+x^2+6x+1)$. *Note that for* $0 \leq i \leq 7$, C_i *denotes a skew cyclic code over* $\mathbb{F}_7$ *defined by the generator polynomial* $\langle x^4+x^3+x^2+x+1 \rangle$*, and* C *is a code characterized by the parameters* $[20, 16, 4]$. *In accordance with Lemma 3.1, Theorems 4.4, and 5.3, it can be concluded that* $\Phi(C)[80, 64, 8]$ *forms a skew cyclic code over* $\mathbb{F}_7$ *with good parameters.*

Example 5.3. *Consider $\mathcal{R}_5$, for $\tau = 3$ the factorization of $x^{16} - 1 = (x+1)(x+2)(x+3)(x+4)(x^2+2)(x^2+3)(x^4+2)(x^4+3)$. Note that for $0 \leq i \leq 7$, C_i denotes a skew cyclic code over $\mathbb{F}_5$ defined by the generator polynomial $\langle x^8 + x^6 + 2x^2 + 1\rangle$, and C is a code characterized by the parameters $[16, 8, 8]$, admitting a generator matrix G given by:*

$$G = \begin{bmatrix} 1000000010100020 \\ 0100000001010002 \\ 0010000030401010 \\ 0001000003040101 \\ 0000100040204040 \\ 0000010004020404 \\ 0000001010002010 \\ 0000000101000201 \end{bmatrix}. \tag{19}$$

According to Lemma 3.1, Theorems 4.4, and 5.3, it can be concluded that $\Phi(C)[128, 64, 32]$ forms a skew cyclic code over $\mathbb{F}_5$ with good parameters.

Example 5.4. *Consider $\mathcal{R}_{11}$, for $\tau = 4$ the factorization of $x^{48} - 1 = (x+1)(x+10)(x^2+1)(x^2+3x+10)(x^2+8x+10)(x^4+3x^2+10)(x^4+8x^2+10)(x^8+3x^4+10)(x^8+8x^4+10)(x^{16}+3x^8+10)(x^{16}+8x^8+10)(x^{32}+3x^{16}+10)(x^{32}+8x^{16}+10)(x^{64}+3x^{32}+10)(x^{64}+8x^{32}+10)$. Note that for $0 \leq i \leq 7$, C_i denotes a skew cyclic code over $\mathbb{F}_{11}$ defined by the generator polynomial $\langle x^{16} + 5x^{14} + 10x^{12} + 3x^{10} + 4x^8 + 8x^6 + 10x^4 + 6x^2 + 1\rangle$, and C is a code characterized by the parameters $[48, 32, 8]$. In accordance with Lemma 3.1, Theorems 4.4, and 5.3, it can be concluded that $\Phi(C)[768, 512, 64]$ forms a skew cyclic code over $\mathbb{F}_{11}$ with good parameters.*

Some optimal linear skew cyclic codes, obtained through the Gray map Φ, are detailed in the table below,

TABLE 1. Linear skew cyclic codes $\Phi(C)$ with good parameters

τ	p	$C[n,k,d]$	$C_i = \langle g_i(x)\rangle$, $0 \leq i \leq 7$	$\Phi(C)[2^\tau n, 2^\tau k, d']$	O
5	3	$[40, 30, 8]$	$\left(x^{10} + 2x^9 + x^8 + 2x^7 + x^6 + x^3 + x + 1\right)$	$[1280, 960, 128]$	yes
4	5	$[28, 12, 12]$	$\begin{pmatrix} x^{16} + 3x^{15} + 2x^{14} + x^9 + 3x^8 + 2x^7 \\ +3x^2 + 4x + 1 \end{pmatrix}$	$[448, 192, 96]$	yes
6	7	$[36, 24, 10]$	$\begin{pmatrix} x^{12} + 2x^{11} + 4x^{10} + 3x^9 + 4x^8 + x^7 \\ +4x^6 + 4x^5 + x^4 + 6x^3 + x^2 + 2x + 4 \end{pmatrix}$	$[2304, 1536, 320]$	yes
3	11	$[18, 8, 4]$	$\begin{pmatrix} x^{10} + x^8 + x^7 + x^6 + x^5 + x^4 \\ +x^3 + x^2 + 1 \end{pmatrix}$	$[144, 64, 16]$	yes
3	13	$[32, 24, 4]$	$\begin{pmatrix} x^8 + 7x^7 + 10x^6 + 9x^5 + 4x^4 \\ +9x^3 + 11x^2 + 6x + 8 \end{pmatrix}$	$[256, 192, 16]$	yes
2	17	$[24, 7, 18]$	$\begin{pmatrix} x^{17} + 12x^{16} + 8x^{15} + 15x^{14} + 11x^{13} \\ +8x^{12} + 15x^{11} + 11x^{10} + 9x^9 + 10x^8 \\ +2x^7 + 6x^6 + 9x^5 + 2x^4 + 6x^3 \\ +9x^2 + 3x + 1 \end{pmatrix}$	$[96, 28, 36]$	yes

6. SKEW CYCLIC LCD CODES OVER $\mathcal{R}_p$

In this section of the article, we delve into the intriguing realm of skew cyclic Linear-Complementary-Dual (LCD) codes over the ring $\mathcal{R}_p$. These codes represent a vital and mathematically fascinating area of study in coding theory and information theory, offering unique properties and applications that set them apart from traditional linear codes. Skew cyclic LCD codes are particularly noteworthy due to their robust error correction capabilities, efficient encoding and decoding procedures, and their relevance in various practical scenarios, such as data transmission, cryptography, and storage systems. Our exploration in this section will shed light on the fundamental concepts, structural properties, and encoding techniques associated with skew cyclic LCD codes over the ring $\mathcal{R}_p$.

Drawing inspiration from the concepts presented in [14], we arrive at the subsequent findings.

Theorem 6.1. *Let* $C = \bigoplus_{i=0}^{2^\tau-1} \varpi_i C_i$ *be a skew cyclic LCD code over* $\mathcal{R}_p$ *if and only if* C_i*, for* $0 \leq i \leq 2^\tau - 1$ *are skew cyclic LCD codes over* $\mathbb{F}_p$.

Proof. By making use of Definition 4.1 in conjunction with Theorems 4.2 and 5.1, we obtain the following

$$\begin{aligned} C \cap C^\perp = \{0_{\mathcal{R}_p}\} \quad &\Leftrightarrow \quad \left(\bigoplus_{i=0}^{2^\tau-1} \varpi_i C_i\right) \cap \left(\bigoplus_{i=0}^{2^\tau-1} \varpi_i C_i^\perp\right) = \{0_{\mathcal{R}_p}\} \\ &\Leftrightarrow \quad \bigoplus_{i=0}^{2^\tau-1} \varpi_i \left(C_i \cap C_i^\perp\right) = \{0_{\mathcal{R}_p}\} \\ &\Leftrightarrow \quad C_i \cap C_i^\perp = \{0_{\mathbb{F}_p}\}, \text{ for } \; 0 \leq i \leq 2^\tau - 1. \end{aligned}$$

□

Theorem 6.2. *If* $C = \bigoplus_{i=0}^{2^\tau-1} \varpi_i C_i$ *be a skew cyclic LCD code over* $\mathcal{R}_p$*, then* $C^\perp = \bigoplus_{i=0}^{2^\tau-1} \varpi_i C_i^\perp$ *is a skew cyclic LCD code.*

Proof. Consider the skew cyclic LCD code C over $\mathcal{R}_p$, which can be expressed as $C = \bigoplus_{i=0}^{2^\tau-1} \varpi_i C_i$. According to Theorem 6.1, when we obtained C_i, for $0 \leq i \leq 2^\tau - 1$, these codes are skew cyclic LCD codes over $\mathbb{F}_p$. Consequently, we can assert that

$$(C_i)^\perp \cap \left((C_i)^\perp\right)^\perp = (C_i)^\perp \cap C_i = \{0_{\mathbb{F}_p}\}.$$

This implies that the dual code $C^\perp$, defined as $C^\perp = \bigoplus_{i=0}^{2^\tau-1} \varpi_i C_i^\perp$, is also a skew cyclic LCD code over $\mathcal{R}_p$. □

Theorem 6.3. *Let* $C = \bigoplus_{i=0}^{2^\tau-1} \varpi_i C_i$ *is a skew cyclic LCD code over* $\mathcal{R}_p$*, then* $\Phi(C)$ *is a skew cyclic LCD code over* $\mathbb{F}_p$.

Proof. Applying Theorems 4.1 and 6.1, we derive the following result

$$\Phi(C) \cap (\Phi(C))^\perp = \left(\bigotimes_{i=0}^{2^\tau-1} C_i\right) \cap \left(\bigotimes_{i=0}^{2^\tau-1} C_i^\perp\right) = \bigotimes_{i=0}^{2^\tau-1} \left(C_i \cap C_i^\perp\right) = \{0_{\mathbb{F}_p}\}.$$

□

7. Conclusion

Overall, this article contributes to the advancement of coding theory by investigating the intricacies of linear codes, skew cyclic codes, and skew cyclic LCD codes over $\mathcal{R}_p$. The New Gray map serves as a valuable tool for visualizing code structures, aiding researchers in better understanding the underlying principles. The insights into the properties and applications of these codes have the potential to impact various fields, ranging from communication systems to error correction techniques, ultimately leading to improved data reliability and transmission efficiency in practical settings.

References

[1] Aleams, B., Muchtadi, I.M., and Muchlis, A., (2018), Skew-cyclic codes over B_k, J. Appl. Math. Comput., (57), 69-84.

[2] Barra, I.A., Dougherty, S.T., Muchlis, A., Muchtadi-Alamsyah, I., Solé, P., Suprijanto, D., and Yemen, O., (2016) θ_s-cyclic codes over A_k, International Journal of Computer Mathematics: Computer Systems Theory., (1), 14-31.

[3] Boucher, D., and Umer, F., (2009), Coding with skew polynomial rings, Journal of Symbolic Computation, (44), 1644-1656.

[4] Chatouh, K., Guenda, K., and Gulliver, T.A., (2020), New classes of codes over New Classes of Codes Over $\mathbb{R}_{q,p,m} = \mathbb{Z}_{p^m}[u_1, u_2, \cdots, u_q]/\left\langle u_i^2 = 0, u_iu_j - u_ju_i \right\rangle$ and their applications, Computational and Applied Mathematics, (39), 1-19.

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

[6] Dertli, A., and Cengellenmis, Y., (2017), Skew cyclic codes over $F_q + uF_q + vF_q + uvF_q$, Journal of Science and Arts, (17), 215.

[7] Dougherty, S.T., Yildiz, B., and Karadeniz, S., (2011), Codes over R_k, gray maps and their binary images, Finite Fields and Their Applications, (17), 205-219.

[8] Gao, J., (2013), Skew cyclic codes over $F_p + vF_p$, Journal of applied mathematics & informatics, (31), 337-342.

[9] Gursoy, F., Siap, I., and Yildiz, B., (2014), Construction of skew cyclic codes over $F_q + vF_q$, Adv. Math. Commun, (8), 313-322.

[10] Hufman, W.C., and Pless, V., (2010), Fundamentals of error-correcting codes, Cambridge university press.

[11] Islam, H., and Prakash, O., (2018), Skew cyclic and skew $\alpha_1 + u\alpha_2 + v\alpha_3 + uv\alpha_4$-constacyclic codes over $F_q + uF_q + vF_q + uvF_q$, arXiv:1710.07785v2 [cs.IT].

[12] Islam, H., and Prakash, O., (2019), Quantum codes from the cyclic codes over $\mathbb{F}_p[u, v, w]/\langle u^2 - 1, v^2 - 1, w^2 - 1, uv - vu, vw - wv, uw - wu\rangle$, J. Appl. Math. Comput, (60), 625-635.

[13] J. Kaborè, J., and Charkani, M.E., (2015), constacyclic codes over $\mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p + uv\mathbb{F}_p$, arXiv:1507.03084 [cs.IT].

[14] Ranya, D.B., and Aicha, B., (2019), Skew constacyclic and LCD codes over $\mathbb{F}_q + v\mathbb{F}_q$, arXiv:1902.08557v1 [cs.IT].

[15] Sari, M., (2023), One-weight codes over the ring $\mathbb{F}_q[v]/\langle v^s - 1\rangle$, Journal of Engineering Technology and Applied Sciences, (8), 35-47.

[16] Yao, T., Shi, M. and Solé, P., (2015), Skew cyclic codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$., J. Algebra Comb. Discrete Appl, (2), 163-168.

[17] Yildiz, B., and Karadeniz, S., (2010), Linear codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, Designs, Codes and Cryptography, (54), 61-81.

[18] Zheng, X., and Kong, B., (2017), Cyclic codes and $\lambda_1 + \lambda_2u + \lambda_3v + \lambda_4uv$-constacyclic codes over $\mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p + uv\mathbb{F}_p$, Applied Mathematics and Computation, (306), 86-91.

Karima Chatouh The individual holds an MSc degree in Applied Mathematics (2007), a postgraduate degree in Applied Mathematics (2011), a Doctorate in Mathematics (2017), and an Habilitation in Applied Mathematics (2020). Presently, she serves as an associate professor at the University of Batna 1 in Algeria. Her research primarily centers on coding theory, reflecting her extensive academic background and expertise in the field.