Contemporary Mathematics
http://ojs.wiserpub.com/index.php/CM/

Research Article

Using Skew Cyclic Codes Over $\mathscr{R} = \mathscr{R}_1 \times \mathscr{R}_2 \times \mathscr{R}_3$ to Detect Skew Cyclic Codes Over $\mathbb{F}_q$

Ouarda Haddouche, Karima Chatouh*

LAMIE Laboratory, Faculty of Economic, Commercial, and Management Sciences, Batna 1 University, Batna, Algeria
E-mail: karima.chatouh@univ-batna.dz

Received: 25 September 2024; **Revised:** 28 November 2024; **Accepted:** 28 November 2024

Abstract: This article investigates linear codes over the ring $\mathscr{R} = \mathscr{R}_1 \times \mathscr{R}_2 \times \mathscr{R}_3$, focusing on the properties and structure of skew cyclic codes within this framework. We explore various algebraic features of these codes, highlighting their distinctiveness from traditional cyclic codes. In addition, we examine the utility of skew cyclic codes over $\mathscr{R}$ in the context of identifying skew cyclic codes over the finite field $\mathbb{F}_q$ with optimal parameters. The findings offer fresh perspectives on developing efficient and high-performing coding systems, which could benefit error correction and data transmission applications.

***Keywords*:** linear codes, skew cyclic codes, gray map, optimal codes, automorphism

MSC: 11TXX, 11T71, 14G50, 15Axx, 15B33

1. Introduction

Linear codes are foundational in coding theory, serving as essential tools for error detection and correction across diverse communication and data storage systems. These codes play a critical role in applications that demand high data integrity, including telecommunications, data storage, and network communication, where they enable the reliable transmission of information by detecting and correcting errors that may arise during data transfer. Historically, the study of linear codes has predominantly focused on finite fields, which have provided a well-established mathematical foundation for understanding their properties and applications. This focus has facilitated significant advancements in coding theory, particularly in error detection and correction. However, the reliance on finite fields has also limited the exploration of alternative algebraic structures, prompting researchers to investigate the potential benefits of coding schemes defined over more complex systems, such as finite rings. Finite rings provide a richer, more versatile algebraic framework, introducing novel properties and avenues for research that are not achievable with conventional finite fields.

One key area of current research is the study of codes over finite rings, which offers the potential for designing innovative coding schemes with improved performance and error-correcting capabilities. Unlike codes over fields, codes defined over rings exhibit unique characteristics that can enhance their structure and function, particularly for complex coding applications. A growing body of research, including those cited here [1–11], underscores the importance of this approach in advancing coding theory and its applications in practical systems.

DOI: https://doi.org/10.37256/cm.5420245789

This study specifically explores linear codes over the ring $\mathscr{R} = \mathscr{R}_1 \times \mathscr{R}_2 \times \mathscr{R}_3$, where each $\mathscr{R}_i$ is a finite commutative ring. This ring-based structure introduces a rich algebraic environment, offering the potential to develop new codes with properties that could outperform those defined over finite fields. Our investigation focuses on skew cyclic codes, a generalization of classical cyclic codes that leverages an automorphism to introduce non-commutative elements into the ring. By incorporating the action of an automorphism, skew cyclic codes exhibit distinctive structural properties and can enhance applications in non-commutative rings. This unique feature gives skew cyclic codes several advantages, particularly in scenarios where the ring's non-commutative properties can be applied for enhanced error correction. We aim to extend the theoretical framework of skew cyclic codes over the ring $\mathscr{R}$, exploring their algebraic properties, structural uniqueness, and coding potential. A significant part of this study is dedicated to examining how these codes over $\mathscr{R}$ can be used to identify skew cyclic codes over finite fields $\mathbb{F}_q$ that exhibit optimal parameters. By translating the codes from the ring to a finite field, we aim to broaden their applicability in practical coding systems. Identifying skew cyclic codes with optimal parameters-such as minimal error rates and high throughput-provides valuable insights for designing coding schemes that meet the demands of high-performance communication systems. Furthermore, this approach contributes a novel perspective to coding theory. While classical cyclic codes have been studied, skew cyclic codes over rings offer an innovative pathway for creating efficient codes. This research assesses the advantages of using the ring structure to derive skew cyclic codes that can be directly translated to finite fields, thereby bridging theoretical insights with practical applications. The proposed approach not only broadens the scope of skew cyclic codes but also has the potential to enhance coding performance by leveraging the unique algebraic properties of rings.

The structure of this paper is organized as follows: Section 2 provides the necessary background on coding theory and the algebraic properties of finite rings, establishing a foundation for understanding the subsequent sections. In Section 3 we analyze the structure and relevance of linear codes over the composite ring $\mathscr{R} = \mathscr{R}_1 \times \mathscr{R}_2 \times \mathscr{R}_3$, focusing on the interplay between each subring's properties. Section 4 delves into the specific characteristics of skew cyclic codes over $\mathscr{R}$, discussing their advantages and potential applications. Section 5 highlights how skew cyclic codes over $\mathscr{R}$ can be associated with skew cyclic codes over the finite field $\mathbb{F}_q$, identifying codes with optimal parameters to demonstrate their practical applications in coding theory. Each section is logically structured to produce an uninterrupted transition from theoretical foundations to applications, focusing on validation and comparison to classical methods. The approach taken in this paper represents a significant innovation in the field by utilizing linear codes over a composite ring structure $\mathscr{R}$ and examining the unique properties of skew cyclic codes within this framework. Compared to classical cyclic codes, skew cyclic codes over $\mathscr{R}$ exhibit unique algebraic properties that enhance their adaptability, especially when mapped onto finite fields for practical use. This innovative methodology highlights a distinct difference from traditional field-based cyclic codes, positioning skew cyclic codes over $\mathscr{R}$ as a valuable tool for developing optimized coding schemes with enhanced performance characteristics.

2. Overview of background information

In this section, we revisit some concepts related to the ring $\mathscr{R} = \mathscr{R}_1 \times \mathscr{R}_2 \times \mathscr{R}_3$, constructed over a field $\mathbb{F}_q$ of size $q = p^s$ with a prime p. It focuses on the additive rings $\mathscr{R} = \mathscr{R}_1 \times \mathscr{R}_2 \times \mathscr{R}_3$, where $\mathscr{R}_1 = \mathbb{F}_q + u\mathbb{F}_q$, $\mathscr{R}_2 = \mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$, and $\mathscr{R}_3 = \mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + w\mathbb{F}_q + uv\mathbb{F}_q + uw\mathbb{F}_q + vw\mathbb{F}_q + uvw\mathbb{F}_q$, with $u^2 = 1$, $v^2 = 1$, and $w^2 = 1$.

Using $q = p^s$ expands the range of elements while keeping efficient operations. This structure supports fields with higher prime powers, benefiting cryptographic and error-correction applications by enhancing algebraic robustness. Larger q affects the rings' structure, influencing rank, element distribution, and computational complexity. In cryptographic contexts, these properties strengthen security by increasing resilience against attacks, especially with larger primes that complicate efficient reductions, further enhancing security margins.

Each element in this ring is expressed as $c = (c_1,\ c_2,\ c_3)$, where $c_1 \in \mathscr{R}_1$, $c_2 \in \mathscr{R}_2$, and $c_3 \in \mathscr{R}_3$. As noted in [2], an element c_i from $\mathscr{R}_i$, where $0 \le i \le 3$, can be expressed using orthogonal idempotents in the following format

$$c_1 =< \alpha,\ \vartheta_1 >_{\mathscr{R}_1}, \tag{1}$$

where

$$\alpha = \begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix}, \text{ and } \vartheta_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} c_1^0 \\ c_1^1 \end{bmatrix}, \tag{2}$$

following the idempotent properties for α_i (where $0 \le i \le 1$) are satisfied-namely, $\sum_{i=0}^{1} \alpha_i = 1$, $\alpha_0 \alpha_1 = 0$, and $\alpha_i^2 = \alpha_i$, for $0 \le i \le 1$, we obtain

$$c_1 = \sum_{i=0}^{1} \alpha_i c_1^i, \text{ with } \begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ u \end{bmatrix}, \text{ and } c_1^i \in {}_q. \tag{3}$$

$$c_2 =< \beta,\ \vartheta_2 >_{\mathscr{R}_2}, \tag{4}$$

where

$$\beta = \begin{bmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ \beta_3 \end{bmatrix} \text{ and } \vartheta_2 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} c_2^0 \\ c_2^1 \\ c_2^2 \\ c_2^3 \end{bmatrix}. \tag{5}$$

The elements β_j are idempotents for $0 \le j \le 3$, we obtain

$$c_2 = \sum_{j=0}^{3} \beta_j c_2^j, \text{ with } \begin{bmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ \beta_3 \end{bmatrix} = \frac{1}{4} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ u \\ v \\ uv \end{bmatrix}, \text{ and } c_2^j \in {}_q, \tag{6}$$

and

$$c_3 =< \gamma,\ \vartheta_3 >_{\mathscr{R}_3}, \tag{7}$$

where

$$\gamma = \begin{bmatrix} \gamma_0 \\ \gamma_1 \\ \gamma_2 \\ \gamma_3 \\ \gamma_4 \\ \gamma_5 \\ \gamma_6 \\ \gamma_7 \end{bmatrix} \text{ and } \vartheta_3 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix} \begin{bmatrix} c_3^0 \\ c_3^1 \\ c_3^2 \\ c_3^3 \\ c_3^4 \\ c_3^5 \\ c_3^6 \\ c_3^7 \end{bmatrix}. \tag{8}$$

However, the elements γ_k are idempotents, for $0 \leq k \leq 7$, we get

$$c_3 = \sum_{k=0}^{7} \gamma_k c_3^k, \text{ with } \begin{bmatrix} \gamma_0 \\ \gamma_1 \\ \gamma_2 \\ \gamma_3 \\ \gamma_4 \\ \gamma_5 \\ \gamma_6 \\ \gamma_7 \end{bmatrix} = \frac{1}{8} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ u \\ v \\ w \\ uv \\ uw \\ vw \\ uvw \end{bmatrix} \text{ and } c_3^k \in \mathbb{F}_q. \tag{9}$$

The parameters α_i, β_j, and γ_k are orthogonal idempotents that serve to decompose elements within the ring $\mathscr{R} = \mathscr{R}_1 \times \mathscr{R}_2 \times \mathscr{R}_3$ into simpler components. Each parameter is associated with an additive ring $\mathscr{R}_i$ and corresponds to a partitioning of the ring space. Specifically:

The parameter α_i, with $0 \leq i \leq 1$, is linked to $\mathscr{R}_1$, decomposing it into two parts.

Similarly, β_j (where $0 \leq j \leq 3$) and γ_k (where $0 \leq k \leq 7$) are associated with $\mathscr{R}_2$ and $\mathscr{R}_3$, respectively, and they enable finer divisions of these spaces.

The following lemma holds and serves as an essential basis for the subsequent analysis.

Lemma 2.1 [12] The element $\alpha_i \beta_j \gamma_k$, for $0 \leq i \leq 1$, $0 \leq j \leq 3$, and $0 \leq k \leq 7$, constitute a fundamental set of idempotents in $\mathscr{R}$, then

1. $(\alpha_i \beta_j \gamma_k)(\alpha_{i'} \beta_{j'} \gamma_{k'}) = 0$, for $0 \leq i \neq i' \leq 1$, $0 \leq j \neq j' \leq 3$ and $0 \leq k \neq k' \leq 7$
2. $(\alpha_i \beta_j \gamma_k)^2 = \alpha_i \beta_j \gamma_k$, for $0 \leq i \leq 1$, $0 \leq j \leq 3$ and $0 \leq k \leq 7$
3. $\sum_{i=0}^{1} \sum_{j=0}^{3} \sum_{k=0}^{7} \alpha_i \beta_j \gamma_k = 1$.

We propose defining a skew cyclic code based on the automorphism Θ acting on the ring $\mathscr{R}$. This automorphism is an extension of the one discussed in various works [3, 8, 9, 12–14].

$$\Theta : \mathscr{R} = \mathscr{R}_1 \times \mathscr{R}_2 \times \mathscr{R}_3 \to \mathscr{R} = \mathscr{R}_1 \times \mathscr{R}_2 \times \mathscr{R}_3$$

$$c = (c_1,\ c_2,\ c_3) \mapsto \Theta(c) = (\theta_1(c_1),\ \theta_2(c_2),\ \theta_3(c_3)), \tag{10}$$

where

$$\theta_i : \mathscr{R}_i \to \mathscr{R}_i$$

$$c_i \mapsto \theta_i(c_i), \; for \; 1 \le i \le 3, \tag{11}$$

with

$$\theta_1\left(\sum_{i=0}^{1} \alpha_i c_1^i\right) = \sum_{i=0}^{1} \alpha_i \theta_1(c_1^i) = \sum_{i=0}^{1} \alpha_i (c_1^i)^{p^{sm}}, \tag{12}$$

$$\theta_2\left(\sum_{j=0}^{3} \beta_j c_2^j\right) = \sum_{j=0}^{3} \beta_j \theta_2(c_2^j) = \sum_{j=0}^{3} \beta_j (c_2^j)^{p^{sm}}, \tag{13}$$

$$\theta_3\left(\sum_{k=0}^{7} \gamma_k c_3^k\right) = \sum_{k=0}^{k} \gamma_k \theta_3(c_3^k) = \sum_{k=0}^{7} \gamma_k (c_3^k)^{p^{sm}}, \tag{14}$$

the order of this automorphism is given by $|< \theta_i >| = \dfrac{s}{m}$, for $1 \le i \le 3$.

2.1 *Gray map and gray images*

The Gray map and its corresponding Gray images play a significant role in coding theory, providing a bridge between different algebraic structures. The Gray map is a specific function used to translate elements from one structure, such as a ring, to another, often simplifying the representation of codes. Gray images resulting from this mapping allow for the visualization and analysis of these codes in a more accessible form. This process is essential for understanding the properties of codes. Based on Equations (3), (6), and (9), the Gray map Φ over the ring $\mathscr{R}$ is defined as follows.

$$\Phi : \mathscr{R} = \mathscr{R}_1 \times \mathscr{R}_2 \times \mathscr{R}_3 \to \mathbb{F}_q^{14}$$

$$c = (c_1, \; c_2, \; c_3) \mapsto \Phi(c) = (\phi_1(c_1), \; \phi_2(c_2), \; \phi_3(c_3)) \tag{15}$$

where

$$\phi_1 : \mathscr{R}_1 \to \mathbb{F}_q^2$$

$$c_1 \mapsto \phi(c_1) = \left(c_1^0 + c_1^1, \; c_1^0 - c_1^1\right), \tag{16}$$

$$\phi_2 : \mathscr{R}_2 \to \mathbb{F}_q^4$$

$$c_2 \mapsto \phi(c_2), \tag{17}$$

with

$$\phi(c_2) = \left(c_2^0 + c_2^1 + c_2^2 + c_2^3,\ c_2^0 - c_2^1 + c_1^2 + c_2^3,\ c_2^0 - c_2^1 + c_1^2 - c_2^3,\ c_2^0 + c_2^1 + c_1^2 - c_2^3\right),$$

and

$$\phi_3 : \mathscr{R}_3 \to \mathbb{F}_q^8$$

$$c_3 \mapsto \phi(c_3), \tag{18}$$

with

$$\phi(c_3) = \Big(c_3^0 + c_3^1 + c_3^2 + c_3^3 + c_3^4 + c_3^5 + c_3^6 + c_3^7,\ c_3^0 - c_3^1 + c_3^2 - c_3^3 + c_3^4 - c_3^5 + c_3^6 - c_3^7,$$

$$c_3^0 + c_3^1 - c_3^2 - c_3^3 + c_3^4 + c_3^5 - c_3^6 - c_3^7,\ c_3^0 - c_3^1 - c_3^2 + c_3^3 + c_3^4 - c_3^5 - c_3^6 + c_3^7,$$

$$c_3^0 + c_3^1 + c_3^2 + c_3^3 - c_3^4 - c_3^5 - c_3^6 - c_3^7,\ c_3^0 - c_3^1 + c_3^2 - c_3^3 - c_3^4 - c_3^5 + c_3^6 + c_3^7,$$

$$c_3^0 + c_3^1 - c_3^2 - c_3^3 - c_3^4 - c_3^5 + c_3^6 + c_3^7,\ c_3^0 - c_3^1 - c_3^2 + c_3^3 - c_3^4 + c_3^5 + c_3^6 - c_3^7\Big).$$

It is clear that extending the map Φ from $\mathscr{R}^n$ to $\mathbb{F}_q^{14n}$ is a straightforward process. Therefore, the following results hold.

Theorem 2.2 The Gray map provides an isometric map from $\mathscr{R}$ with the minimal distance to $\mathbb{F}_q^{14n}$ with the Hamming distance.

An essential property of the Gray map we defined is its ability to preserve duality, as stated in the following lemma.

Lemma 2.3 If $\mathscr{C}$ is a linear code of length n over $\mathscr{R}$, with minimal distance d, then $\Phi(\mathscr{C})$ is a $[n' = 14n,\ k',\ d'_{Ham}]_q$-linear code over $\mathbb{F}_q$.

The Gray map highlights the differences between linear codes over rings and those over finite fields. On the other hand, linear codes over finite fields rely on field properties like unique inverses and the absence of zero divisors, codes over rings, such as $\mathscr{R} = \mathscr{R}_1 \times \mathscr{R}_2 \times \mathscr{R}_3$, incorporate more complex structures. The Gray map enables the translation of these ring-based codes into a format that is more accessible and comparable to field-based codes. Mapping the elements of the ring to vector spaces over finite fields simplifies the analysis and visualization of ring-based codes, allowing us to exploit the algebraic richness of rings-such as idempotents and zero divisors-which are absent in finite fields. This transformation is essential in understanding how linear codes over rings can exhibit unique properties, such as more flexible error detection and correction capabilities, that differ significantly from the behavior of codes over finite fields.

3. Linear codes over $\mathscr{R} = \mathscr{R}_1 \times \mathscr{R}_2 \times \mathscr{R}_3$

In this section, we explore the construction and analysis of linear codes over the ring $\mathscr{R} = \mathscr{R}_1 \times \mathscr{R}_2 \times \mathscr{R}_3$, where $\mathscr{R}_1$, $\mathscr{R}_2$, and $\mathscr{R}_3$ are finite commutative rings. The purpose of this section is to extend the classical theory of linear codes, traditionally defined over finite fields, to a product ring structure. By examining how the algebraic properties of each component ring $\mathscr{R}_i$ influence the overall code, we aim to uncover new insights into optimizing code parameters and improving the performance of error-correcting codes.

The results of this section include the formulation of linear codes over the ring $\mathscr{R}$, leveraging the structural characteristics of $\mathscr{R}_1$, $\mathscr{R}_2$, and $\mathscr{R}_3$. We demonstrate how such codes can be viewed as generalizations of classical codes, leading to enhanced flexibility in code design, especially concerning the choice of parameters such as length, dimension, and minimum distance. These codes provide a richer algebraic framework that may yield more efficient encoding and decoding schemes than traditional finite field-based codes.

According to [15] and the Chinese Remainder Theorem, we can express $\mathscr{R}$ in terms of orthogonal idempotents within $\mathscr{R}_i$, for $0 \leq i \leq 3$ as follows

$$\mathscr{R}_1 = \bigoplus_{i=0}^{1} \alpha_i \mathscr{R}_1 = \bigoplus_{i=0}^{1} \alpha_i \mathbb{F}_q, \tag{19}$$

$$\mathscr{R}_2 = \bigoplus_{i=0}^{1} \beta_j \mathscr{R}_2 = \bigoplus_{i=0}^{1} \beta_j \mathbb{F}_q, \tag{20}$$

and

$$\mathscr{R}_3 = \bigoplus_{i=0}^{1} \gamma_k \mathscr{R}_3 = \bigoplus_{i=0}^{1} \gamma_k \mathbb{F}_q, \tag{21}$$

then

$$\mathscr{R} = \left(\bigoplus_{i=0}^{1} \alpha_i \mathscr{R}_1 \right) \left(\bigoplus_{j=0}^{3} \beta_j \mathscr{R}_2 \right) \left(\bigoplus_{k=0}^{7} \gamma_k \mathscr{R}_3 \right) = \bigoplus_{i=0}^{1} \bigoplus_{j=0}^{3} \bigoplus_{k=0}^{7} \alpha_i \beta_j \gamma_k \mathbb{F}_q^3, \tag{22}$$

where $\mathscr{C}_1^i$, $\mathscr{C}_2^j$ and $\mathscr{C}_3^k$, for $0 \leq i \leq 1$, $0 \leq j \leq 3$ and $0 \leq k \leq 7$ are linear codes over $\mathbb{F}_q$, with

$$\mathscr{C}_1^0 = \{c_1^0 + c_1^1,\ \exists c_0,\ c_1^1 \in \mathbb{F}_q^{2n},\ \forall c_1 \in \mathscr{C}_1\},$$

$$\mathscr{C}_1^1 = \{c_1^0 - c_1^1,\ \exists c_0,\ c_1^1 \in \mathbb{F}_q^{2n},\ \forall c_1 \in \mathscr{C}_1\},$$

$$\mathscr{C}_2^0 = \{c_2^0 + c_2^1 + c_2^2 + c_2^3,\ \exists c_2^0,\ c_2^1,\ c_2^2,\ c_2^3 \in \mathbb{F}_q^{4n_2},\ \forall c \in \mathscr{C}_2\},$$

$$\mathscr{C}_2^1 = \{c_2^0 - c_2^1 + c_1^2 - c_2^3,\ \exists c_2^0,\ c_2^1,\ c_2^2,\ c_2^3 \in \mathbb{F}_q^{4n_2},\ \forall c \in \mathscr{C}_2\},$$

$$\mathscr{C}_2^2 = \{c_2^0 + c_2^1 - c_1^2 - c_2^3,\ \exists c_2^0,\ c_2^1,\ c_2^2,\ c_2^3 \in \mathbb{F}_q^{4n_2},\ \forall c \in \mathscr{C}_2\},$$

$$\mathscr{C}_2^3 = \{c_2^0 - c_2^1 - c_2^2 + c_2^3,\ \exists c_2^0,\ c_2^1,\ c_2^2,\ c_2^3 \in \mathbb{F}_q^{4n_2},\ \forall c \in \mathscr{C}_2\}.$$

and

$$\mathscr{C}_3^0 = \{c_3^0 + c_3^1 + c_3^2 + c_3^3 + c_3^4 + c_3^5 + c_3^6 + c_3^7,\ \exists c_3^0,\ c_3^1,\ c_3^2,\ c_3^2,\ c_3^4,\ c_3^5,\ c_3^6,\ c_3^7 \in \mathbb{F}_q^{8n_3},\ \forall c \in \mathscr{C}_3\},$$

$$\mathscr{C}_3^1 = \{c_3^0 - c_3^1 + c_3^2 - c_3^3 + c_3^4 + c_3^5 - c_3^6 - c_3^7,\ \exists c_3^0,\ c_3^1,\ c_3^2,\ c_3^2,\ c_3^4,\ c_3^5,\ c_3^6,\ c_3^7 \in \mathbb{F}_q^{8n_3},\ \forall c \in \mathscr{C}_3\},$$

$$\mathscr{C}_3^2 = \{c_3^0 + c_3^1 - c_3^2 - c_3^3 + c_3^4 + c_3^5 - c_3^6 - c_3^7,\ \exists c_3^0,\ c_3^1,\ c_3^2,\ c_3^2,\ c_3^4,\ c_3^5,\ c_3^6,\ c_3^7 \in \mathbb{F}_q^{8n_3},\ \forall c \in \mathscr{C}_3\},$$

$$\mathscr{C}_3^3 = \{c_3^0 + c_3^1 - c_3^2 - c_3^3 + c_3^4 - c_3^5 - c_3^6 + c_3^7,\ \exists c_3^0,\ c_3^1,\ c_3^2,\ c_3^2,\ c_3^4,\ c_3^5,\ c_3^6,\ c_3^7 \in \mathbb{F}_q^{8n_3},\ \forall c \in \mathscr{C}_3\},$$

$$\mathscr{C}_3^4 = \{c_3^0 + c_3^1 + c_3^2 + c_3^3 - c_3^4 - c_3^5 - c_3^6 - c_3^7,\ \exists c_3^0,\ c_3^1,\ c_3^2,\ c_3^2,\ c_3^4,\ c_3^5,\ c_3^6,\ c_3^7 \in \mathbb{F}_q^{8n_3},\ \forall c \in \mathscr{C}_3\},$$

$$\mathscr{C}_3^5 = \{c_3^0 - c_3^1 + c_3^2 - c_3^3 - c_3^4 - c_3^5 + c_3^6 + c_3^7,\ \exists c_3^0,\ c_3^1,\ c_3^2,\ c_3^2,\ c_3^4,\ c_3^5,\ c_3^6,\ c_3^7 \in \mathbb{F}_q^{8n_3},\ \forall c \in \mathscr{C}_3\},$$

$$\mathscr{C}_3^6 = \{c_3^0 + c_3^1 - c_3^2 - c_3^3 - c_3^4 + c_3^5 + c_3^6 + c_3^7,\ \exists c_3^0,\ c_3^1,\ c_3^2,\ c_3^2,\ c_3^4,\ c_3^5,\ c_3^6,\ c_3^7 \in \mathbb{F}_q^{8n_3},\ \forall c \in \mathscr{C}_3\},$$

$$\mathscr{C}_3^7 = \{c_3^0 + c_3^1 + c_3^2 + c_3^3 - c_3^4 - c_3^5 - c_3^6 - c_3^7,\ \exists c_3^0,\ c_3^1,\ c_3^2,\ c_3^2,\ c_3^4,\ c_3^5,\ c_3^6,\ c_3^7 \in \mathbb{F}_q^{8n_3},\ \forall c \in \mathscr{C}_3\}.$$

From the preceding relations, we deduce that each code $\mathscr{C}$ over $\mathscr{R}$ can be represented as follows:

$$\mathscr{C} = \left(\bigoplus_{i=0}^{1} \alpha_i \mathscr{C}_1^i\right)\left(\bigoplus_{j=0}^{3} \beta_j \mathscr{C}_2^j\right)\left(\bigoplus_{k=0}^{7} \gamma_i \mathscr{C}_3^k\right) \tag{23}$$

In this case, the following assertions stand true.

Theorem 3.1 Let $\mathscr{C}$ and $\mathscr{C}^{\perp}$ be linear codes of length n over $\mathscr{R} = \mathscr{R}_1 \times \mathscr{R}_2 \times \mathscr{R}_3$, then

$$\mathscr{C} = \bigoplus_{i=0}^{1}\bigoplus_{j=0}^{3}\bigoplus_{k=0}^{7} \alpha_i \beta_j \gamma_k \mathscr{C}_{ijk}, \tag{24}$$

and

$$\mathscr{C}^{\perp} = \bigoplus_{i=0}^{1}\bigoplus_{j=0}^{3}\bigoplus_{k=0}^{7} \alpha_i \beta_j \gamma_k (\mathscr{C}_{ijk})^{\perp}. \tag{25}$$

where the codes $\mathscr{C}_{ijk} = \mathscr{C}_1^i \times \mathscr{C}_2^j \times \mathscr{C}_3^k$, for $0 \le i \le 1$, $0 \le j \le 3$, and $0 \le k \le 7$.

Proof. The proof is obtained from Equations (19-23). □

Theorem 3.2 Let $\mathscr{C}$ be a linear code of length n over $\mathscr{R} = \mathscr{R}_1 \times \mathscr{R}_2 \times \mathscr{R}_3$, we obtain

$$\Phi(\mathscr{C}) = \bigotimes_{i=0}^{1}\bigotimes_{j=0}^{3}\bigotimes_{k=0}^{7}\mathscr{C}_{ijk}, \tag{26}$$

and

$$|\mathscr{C}| = \prod_{i=0}^{1}\prod_{j=0}^{3}\prod_{k=0}^{7}|\mathscr{C}_{ijk}|, \tag{27}$$

with

$$\mathscr{C}_{000} = \{(c_1^0 + c_1^1,\ c_2^0 + c_2^1 + c_2^2 + c_2^3,\ c_3^0 + c_3^1 + c_3^2 + c_3^3 + c_3^4 + c_3^5 + c_3^6 + c_3^7),$$

$$\exists c_1^0,\ c_1^1,\ c_2^0,\ c_2^1,\ c_2^2,\ c_2^{12},\ c_3^0,\ c_3^1,\ c_3^2,\ c_3^3,\ c_3^4,\ c_3^5,\ c_3^6,\ c_3^7 \in \mathbb{F}_q,\ \forall c \in \mathscr{C}\},$$

$$\mathscr{C}_{001} = \{(c_1^0 + c_1^1,\ c_2^0 + c_2^1 - c_2^2 - c_2^3,\ c_3^0 - c_3^1 + c_3^2 - c_3^3 + c_3^4 - c_3^5 + c_3^6 - c_3^7),$$

$$\exists c_1^0,\ c_1^1,\ c_2^0,\ c_2^1,\ c_2^2,\ c_2^{12},\ c_3^0,\ c_3^1,\ c_3^2,\ c_3^3,\ c_3^4,\ c_3^5,\ c_3^6,\ c_3^7 \in \mathbb{F}_q,\ \forall c \in \mathscr{C}\},$$

$$\vdots$$

$$\mathscr{C}_{137} = \{(c_1^0 - c_1^1,\ c_2^0 - c_2^1 - c_1^2 + c_2^3,\ c_3^0 + c_3^1 + c_3^2 + c_3^3 - c_3^4 - c_3^5 - c_3^6 - c_3^7),$$

$$\exists c_1^0,\ c_1^1,\ c_2^0,\ c_2^1,\ c_2^2,\ c_2^{12},\ c_3^0,\ c_3^1,\ c_3^2,\ c_3^3,\ c_3^4,\ c_3^5,\ c_3^6,\ c_3^7 \in \mathbb{F}_q,\ \forall c \in \mathscr{C}\}.$$

Proof. Using a similar approach to [16, Theorem 8] . □

Theorem 3.3 Let $\mathscr{C} = \bigoplus_{i=0}^{1}\bigoplus_{j=0}^{3}\bigoplus_{k=0}^{7}\alpha_i\beta_j\gamma_k\mathscr{C}_{ijk}$ be a linear code of length n over $\mathscr{R}$, then $\mathscr{C}^{\perp} = \bigoplus_{i=0}^{1}\bigoplus_{j=0}^{3}\bigoplus_{k=0}^{7}\alpha_i\beta_j\gamma_k\mathscr{C}_{ijk}^{\perp}$. Further, $\mathscr{C}$ is self-dual if and only if $\mathscr{C}_{ijk}$, for $0 \le i \le 1$, $0 \le j \le 3$ and $0 \le k \le 7$ are self-duals.

Proof. Assume that $x \in \mathscr{C}^{\perp}$ and $c = \sum_{i=0}^{1}\sum_{j=0}^{3}\sum_{k=0}^{7}\alpha_i\beta_j\gamma_k c_{ijk} \in \mathscr{C}$, with $c_{ijk} \in \mathscr{C}_{ijk}$. we can expand the product as follows,

$$x.c = \sum_{i=0}^{1}\sum_{j=0}^{3}\sum_{k=0}^{7}\alpha_i\beta_j\gamma_k(x.c_{ijk}), \tag{28}$$

sience $x \in \mathscr{C}^{\perp}$, we have

$$x.c_{ijk} = 0\ for\ c_{ijk} \in \mathscr{C}_{ijk}, \tag{29}$$

that means $x \in \mathscr{C}_{ijk}^{\perp}$, for $0 \leq i \leq 1$, $0 \leq j \leq 3$ and $0 \leq k \leq 7$. We arrive at the expression

$$\mathscr{C}^{\perp} = \bigoplus_{i=0}^{1} \bigoplus_{j=0}^{3} \bigoplus_{k=0}^{7} \alpha_i \beta_j \gamma_k \mathscr{C}_{ijk}^{\perp}.$$

If $\mathscr{C}$ is self-dual, then

$$\mathscr{C} = \mathscr{C}^{\perp} \Rightarrow \bigoplus_{i=0}^{1} \bigoplus_{j=0}^{3} \bigoplus_{k=0}^{7} \alpha_i \beta_j \gamma_k \mathscr{C}_{ijk} = \bigoplus_{i=0}^{1} \bigoplus_{j=0}^{3} \bigoplus_{k=0}^{7} \alpha_i \beta_j \gamma_k \mathscr{C}_{ijk}^{\perp}. \tag{30}$$

Since the direct sum is taken component-wise, this implies that each code $\mathscr{C}_{ijk}$ must also satisfy $\mathscr{C}_{ijk} = \mathscr{C}_{ijk}^{\perp}$, meaning that each $\mathscr{C}_{ijk}$ must be self-dual.

If each $\mathscr{C}_{ijk}$ is self-dual, that means $\mathscr{C}_{ijk} = \mathscr{C}_{ijk}^{\perp}$, for $0 \leq i \leq 1$, $0 \leq j \leq 3$ and $0 \leq k \leq 7$, then

$$\bigoplus_{i=0}^{1} \bigoplus_{j=0}^{3} \bigoplus_{k=0}^{7} \alpha_i \beta_j \gamma_k \mathscr{C}_{ijk} = \bigoplus_{i=0}^{1} \bigoplus_{j=0}^{3} \bigoplus_{k=0}^{7} \alpha_i \beta_j \gamma_k \mathscr{C}_{ijk}^{\perp} \tag{31}$$

is also self-dual, directly from the definition of dual code and the properties of direct sums $\mathscr{C}$ will be self-dual. □

Lemma 3.4 Let $\mathscr{C}$ be a linear code of length n over $\mathscr{R}$, then $\Phi(\mathscr{C}^{\perp}) = [\Phi(\mathscr{C})]^{\perp}$. Further, $\mathscr{C}$ is a self-dual code if and only if $\Phi(\mathscr{C})$ is a self-dual code.

Proof. We interpret $\Phi(\mathscr{C}) = \Phi(\mathscr{C}_1 \times \mathscr{C}_2 \times \mathscr{C}_3)$ to be some transformation to each codeword $c = (c_1 \mid c_2 \mid c_3) \in \mathscr{C}$. The code $\Phi(\mathscr{C}^{\perp}) = \Phi(\mathscr{C}_1^{\perp} \times \mathscr{C}_2^{\perp} \times \mathscr{C}_3^{\perp})$ consists of the transformed codewords of the dual code.

Let $v = (v_1,\ v_2,\ v_3) \in \Phi(\mathscr{C}^{\perp})$ that means it exists $x = (x_1,\ x_2,\ x_3) \in \mathscr{C}^{\perp}$, $\Phi(x) = v$. Since $x = (x_1,\ x_2,\ x_3) \in \mathscr{C}^{\perp}$ we have,

$$< x,\ c >_{\mathscr{R}} = 0 \Rightarrow < (x_1,\ x_2,\ x_3),\ (c_1,\ c_2,\ c_3) >_{\mathscr{R}} = 0, \text{ for all } c \in \mathscr{C},$$

and based on the information provided by the Theorem 2.2, we have

$$< \Phi(x_1,\ x_2,\ x_3),\ \Phi(c_1,\ c_2,\ c_3) >_{\mathscr{R}} = < (\phi_1(x_1),\ \phi_2(x_2),\ \phi_3(x_3)),\ (\phi_1(c_1),\ \phi_2(c_2),\ \phi_3(c_3)) >_{\mathscr{R}} = 0,$$

then

$$\langle \phi_1(x_1),\ \phi_1(c_1) \rangle_{\mathscr{R}_1} = 0,\ \langle \phi_2(x_2),\ \phi_2(c_2) \rangle_{\mathscr{R}_2} = 0,\ \langle \phi_2(x_1),\ \phi_2(c_2) \rangle_{\mathscr{R}_3} = 0.$$

we have $v_1 \in [\phi_1(\mathscr{C}_1)]^{\perp}$, $v_2 \in [\phi_2(\mathscr{C}_2)]^{\perp}$, $v_3 \in [\phi_3(\mathscr{C}_3)]^{\perp}$. This implies that $v \in [\Phi(\mathscr{C})]^{\perp}$. Conversely, if $v \in [\Phi(\mathscr{C})]^{\perp}$, this means,

$$\text{For any } c = (c_1,\ c_2,\ c_3) \in \Phi(\mathscr{C}), \text{ we have } < v,\ \Phi(c) >_{\mathscr{R}} = 0.$$

Following Theorem 2.1 we have, $< \Phi^{-1}(v),\ c >_{\mathscr{R}} = 0$ that means , $\Phi^{-1}(v) \in \mathscr{C}^{\perp}$, then $v \in [\Phi(\mathscr{C})]^{\perp}$, so we have

$$\Phi(\mathscr{C}^{\perp}) = [\Phi(\mathscr{C})]^{\perp}.$$

The demonstration for the second aspect. we Assume $\mathscr{C}$ is self-dual. Then $\mathscr{C} = \mathscr{C}^{\perp}$. Applying the result from Step 1 gives:

$$\Phi(\mathscr{C}^{\perp}) = \Phi(\mathscr{C}) \implies [\Phi(\mathscr{C})]^{\perp} = \Phi(\mathscr{C}),$$

thus, $\Phi(\mathscr{C})$ is self-dual. Conversely, assume $\Phi(\mathscr{C})$ is self-dual, we obtain

$$\Phi(\mathscr{C}) = [\Phi(\mathscr{C})]^{\perp},$$

Using the first step, we get

$$\mathscr{C}^{\perp} = \Phi(\mathscr{C}^{\perp}) \implies \mathscr{C} = \mathscr{C}^{\perp},$$

hence, $\mathscr{C}$ is self-dual. □

Theorem 3.5 Let G_{ijk} be the generator matrices of the linear codes $\mathscr{C}_{ijk}$, for $0 \leq i \leq 1$, $0 \leq j \leq 3$, and $0 \leq k \leq 7$ over $\mathbb{F}_q$. Then, the generator matrix G of the code $\mathscr{C} = \bigoplus_{i=0}^{1} \bigoplus_{j=0}^{3} \bigoplus_{k=0}^{7} \alpha_i \beta_j \gamma_k \mathscr{C}_{ijk}$ is given by

$$G = \begin{pmatrix} {}_0\beta_0\gamma_0 G_{000} \\ \alpha_0\beta_0\gamma_1 G_{001} \\ \vdots \\ \alpha_1\beta_3\gamma_7 G_{137} \end{pmatrix}. \tag{32}$$

Proposition 3.6 Suppose $\mathscr{C}$ is a linear code of length n over $\mathscr{R}$ with a generator matrix $G_{\mathscr{C}}$. Then the generator matrix $G_{\Phi(\mathscr{C})}$ of the code $\Phi(\mathscr{C})$ can be expressed as follows

$$G_{\Phi(\mathscr{C})} = \begin{pmatrix} G_{000} & 0 & \dots & 0 \\ 0 & G_{001} & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & G_{137} \end{pmatrix}.$$

4. Some properties of skew cyclic codes over $\mathscr{R} = \mathscr{R}_1 \times \mathscr{R}_2 \times \mathscr{R}_3$

In this section, we investigate skew cyclic codes over the product ring $\mathscr{R} = \mathscr{R}_1 \times \mathscr{R}_2 \times \mathscr{R}_3$, with a focus on understanding how the product structure influences the algebraic properties of these codes. Specifically, we analyze the generator polynomials, the structure of ideals, and the impact of ring automorphisms on the behavior of skew cyclic codes. The goal of this section is to extend the classical theory of cyclic codes by incorporating the product structure of rings, which introduces new possibilities for optimizing the properties of the codes, such as their minimum distance, error correction capabilities, and computational efficiency see [8, 9, 13, 17].

The primary results obtained in this section include the formulation of skew cyclic codes over the product ring $\mathscr{R}$, where the properties of each component ring $\mathscr{R}_i$ interact in ways that are crucial for understanding the overall structure of the codes. By leveraging the insights from skew cyclic code theory, we can define and analyze new types of codes that have potentially advantageous properties compared to standard cyclic codes, such as improved error correction or more efficient encoding and decoding algorithms.

Definition 4.1 A linear code $\mathscr{C}$ of length n over $\mathscr{R}$ is said to be a skew cyclic code with respect to the automorphism Θ if and only if for any codeword

$$c = (c^0,\ c^1,\ \ldots,\ c^{n-1}) \in \mathscr{C} \Rightarrow \sigma(c) = (\Theta(c^{n-1}),\ \Theta(c^0),\ \Theta(c^1),\ \ldots,\ \Theta(c^{n-2})) \in \mathscr{C}, \tag{33}$$

where σ is a skew cyclic shift of $\mathscr{C}$.

Theorem 4.2 Let $\mathscr{C} = \bigoplus_{i=0}^{1} \bigoplus_{j=0}^{3} \bigoplus_{k=0}^{7} \alpha_i \beta_j \gamma_k \mathscr{C}_{ijk}$ be a linear code over R of length n where $\mathscr{C}_{ijk}$, for $0 \leq i \leq 1$, $0 \leq j \leq 3$, and $0 \leq k \leq 7$ are linear codes of length n over $\mathbb{F}_q$. Then $\mathscr{C}$ is a skew cyclic code over $\mathscr{R}$ if and only if $\mathscr{C}_{ijk}$, for $0 \leq i \leq 1$, $0 \leq j \leq 3$, and $0 \leq k \leq 7$ are skew cyclic codes over $\mathbb{F}_q$, with respect to the automorphism Θ.

Proof. Considering an element $c = (c^0,\ c^1,\ c^2,\ \ldots,\ c^{n-1}) \in \mathscr{C}$, it follows that

$$c^l = \textstyle\sum_{i=0}^{1} \sum_{j=0}^{3} \sum_{k=0}^{7} \alpha_i \beta_j \gamma_k c^l_{ijk},\ 0 \leq l \leq n-1.$$

with $c^l_{ijk} = c_i^{1,\ l} c_j^{2,\ 3} c_k^{3,\ l}$, where $\left(c_i^{1,\ l},\ c_j^{2,\ l},\ c_k^{3,\ l}\right) \in C_1^i \times C_2^j \times C_3^k$, for $0 \leq i \leq 1$, $0 \leq j \leq 3$, and $0 \leq k \leq 7$.

Given that $\mathscr{C}_{ijk}$, where $0 \leq i \leq 1$, $0 \leq j \leq 3$, and $0 \leq k \leq 7$, represents a collection of skew cyclic codes, it follows that $\sigma(c^l_{ijk}) \in \mathscr{C}_{ijk}$, for $0 \leq i \leq 1$, $0 \leq j \leq 3$, and $0 \leq k \leq 7$. Furthermore, assuming the equation

$$\Theta(c^l_{ijk}) = \sum_{i=0}^{1} \sum_{j=0}^{3} \sum_{k=0}^{7} \alpha_i \beta_j \gamma_k \Theta(c^l_{ijk})$$

$$= \sum_{i=0}^{1} \sum_{j=0}^{3} \sum_{k=0}^{7} \alpha_i \beta_j \gamma_k \Theta(c_i^{1,\ l},\ c_j^{2,\ l},\ c_k^{3,\ l})$$

$$= \sum_{i=0}^{1} \sum_{j=0}^{3} \sum_{k=0}^{7} \alpha_i \beta_j \gamma_k (\theta_1(c_i^{1,\ l}),\ \theta_2(c_j^{2,\ l}),\ \theta_3(c_k^{3,\ l}))$$

$$= \sum_{i=0}^{1} \sum_{j=0}^{3} \sum_{k=0}^{7} \alpha_i \theta_1(c_i^{1,\ l}) \beta_j \theta_2(c_j^{2,\ l}) \gamma_k \theta_3(c_k^{3,\ l})$$

$$\Theta(c^l_{ijk}) = \sum_{i=0}^{1} \sum_{j=0}^{3} \sum_{k=0}^{7} \alpha_i \beta_j \gamma_k \left(\theta_1(c_i^{1,\ l}) \theta_2(c_j^{2,\ l}) \theta_3(c_k^{3,\ l})\right) \tag{34}$$

The skew cyclic property requires that these shifts when applied to codewords corresponding to skew cyclic shifts in each $\mathscr{C}_{ijk}$, should yield new valid codewords within the code $\mathscr{C}$, we can then proceed to derive the expression.

$$
\begin{aligned}
\sigma(c) &= \Big(\Theta(c^{n-1}),\ \Theta(c^{0}),\ \Theta(c^{1}),\ \ldots,\ \Theta(c^{n-2})\Big)\\
&= \Big(\Theta(c_1^{n-1},\ c_2^{n-1},\ c_3^{n-1}),\ \Theta(c_1^{0},\ c_2^{0},\ c_3^{0}),\ \Theta(c_1^{1},\ c_2^{1},\ c_3^{1}),\ \ldots,\ \Theta(c_1^{n-2},\ c_2^{n-2},\ c_3^{n-2})\Big)\\
&= \Big((\theta_1(c_1^{n-1}),\ \theta_2(c_2^{n-1}),\ \theta_3(c_3^{n-1})),\ (\theta_1(c_1^{0}),\ \theta_2(c_2^{0}),\ \theta_3(c_3^{0})),\ (\theta_1(c_1^{1}),\ \theta_2(c_2^{1}),\ \theta_3(c_3^{1})),\\
&\quad \ldots,\ (\theta_1(c_1^{n-2}),\ \theta_2(c_2^{n-2}),\ \theta_3(c_3^{n-2}))\Big)\\
&= \Big((\theta_1(c_1^{n-1}),\ \theta_1(c_1^{0}),\ \theta_1(c_1^{1}),\ \ldots,\ \theta_1(c_1^{n-2})),\ (\theta_2(c_2^{n-1}),\ \theta_2(c_2^{0}),\ \theta_2(c_2^{1}),\ \ldots,\ \theta_2(c_2^{n-2})),\\
&\quad (\theta_3(c_3^{n-1}),\ \theta_3(c_3^{0}),\ \theta_3(c_3^{1}),\ \ldots,\ \theta_3(c_3^{n-2}))\Big)\\
&= \Big(\sum_{i=0}^{1}\alpha_i\theta_1(c_1^{i,\ n-1}),\ \sum_{i=0}^{1}\alpha_i\theta_1(c_1^{i,\ 0}),\ \sum_{i=0}^{1}\alpha_i\theta_1(c_1^{i,\ 1}),\ \ldots,\ \sum_{i=0}^{1}\alpha_i\theta_1(c_1^{i,\ n-2}),\\
&\quad \sum_{j=0}^{3}\beta_j\theta_2(c_2^{j,\ n-1}),\ \sum_{j=0}^{3}\beta_j\theta_2(c_2^{j,\ 0}),\ \sum_{j=0}^{3}\beta_j\theta_2(c_2^{j,\ 1}),\ \ldots,\ \sum_{j=0}^{3}\beta_j\theta_2(c_2^{j,\ n-2}),\\
&\quad \sum_{k=0}^{7}\gamma_k\theta_3(c_3^{k,\ n-1}),\ \sum_{k=0}^{7}\gamma_k\theta_3(c_3^{k,\ 0}),\ \sum_{k=0}^{7}\gamma_k\theta_3(c_3^{k,\ 1}),\ \ldots,\ \sum_{k=0}^{7}\gamma_k\theta_3(c_3^{k,\ n-2})\Big)\\
&= \Big(\sum_{i=0}^{1}\sum_{j=0}^{3}\sum_{k=0}^{7}\alpha_i\theta_1(c_i^{1,\ n-1})\beta_j\theta_2(c_j^{2,\ n-1})\gamma_k\theta_3(c_k^{3,\ n-1}),\ \sum_{i=0}^{1}\sum_{j=0}^{3}\sum_{k=0}^{7}\alpha_i\theta_1(c_i^{1,\ 0})\beta_j\theta_2(c_j^{2,\ 0})\gamma_k\theta_3(c_k^{3,\ 0}),\\
&\quad \ldots,\ \sum_{i=0}^{1}\sum_{j=0}^{3}\sum_{k=0}^{7}\alpha_i\theta_1(c_i^{1,\ n-2})\beta_j\theta_2(c_j^{2,\ n-2})\gamma_k\theta_3(c_k^{3,\ n-2})\Big)\\
&= \sum_{i=0}^{1}\sum_{j=0}^{3}\sum_{k=0}^{7}\alpha_i\beta_j\gamma_k\Big(\theta_1(c_i^{1,\ n-1})\theta_2(c_j^{2,\ n-1})\theta_3(c_k^{3,\ n-1}),\\
&\qquad \theta_1(c_i^{1,\ 0})\theta_2(c_j^{2,\ 0})\theta_3(c_k^{3,\ 0}),\ \cdots,\ \theta_1(c_i^{1,\ n-2})\theta_2(c_j^{2,\ n-2})\theta_3(c_k^{3,\ n-2})\Big),
\end{aligned}
$$

then $\sigma(c) \in \mathscr{C}$. This implication leads us to conclude that $\sigma(c)$ belongs to $\mathscr{C}$, which establishes that the code $\mathscr{C}$ is a cyclic code over $\mathscr{R}$. A similar reasoning holds for the reverse implication. □

Corollary 4.3 The dual code $\mathscr{C}^{\perp}$ is a skew cyclic code over $\mathscr{R}$, if $\mathscr{C}$ is a skew cyclic code over $\mathscr{R}$.

Proof. If the code $\mathscr{C} = \bigoplus_{i=0}^{1} \bigoplus_{j=0}^{3} \bigoplus_{k=0}^{7} \alpha_i \beta_j \gamma_k \mathscr{C}_{ijk}$ is a skew cyclic code over $\mathscr{R}$, we can apply the relevant theorems to establish that the dual code $\mathscr{C}^{\perp}$ is also skew cyclic. Recall that for a skew cyclic code $\mathscr{C}$, the shift operation, which moves the code elements according to a skew action, preserves the structure of the code. This property is crucial in both the original code and its dual. According to known results , such as Theorems 3.3, 4.2 and the reference [18] , the skew cyclic nature of a code is preserved under duality. Specifically, if $\mathscr{C}$ is a skew cyclic code over $\mathscr{R}$, then its dual $\mathscr{C}^{\perp}$ remains skew cyclic over the same ring. □

Corollary 4.4 The code $\mathscr{C}$ is a self-dual skew cyclic code over $\mathscr{R}$ if and only if $\mathscr{C}_{ijk}$, for $0 \le i \le 1$, $0 \le j \le 3$, and $0 \le k \le 7$ are self-dual skew cyclic codes over $\mathbb{F}_q$.

Proof. To confirm the validity of this proposition, it suffices to apply Theorems 3.3 and 4.2. These theorems provide the necessary framework to demonstrate that the dual code $\mathscr{C}^{\perp}$ maintains the skew cyclic structure when $\mathscr{C}$ itself is skew cyclic.

Theorem 4.5 Let $\mathscr{C} = \bigoplus_{i=0}^{1} \bigoplus_{j=0}^{3} \bigoplus_{k=0}^{7} \alpha_i \beta_j \gamma_k \mathscr{C}_{ijk}$ be a skew cyclic code of length n over $\mathscr{R}$. Assume that $g_{ijk}(x)$, is a generator polynomial of $\mathscr{C}_{ijk}$, for $0 \le i \le 1$, $0 \le j \le 3$, and $0 \le k \le 7$, then

1. $\mathscr{C} = \left\langle \alpha_i \beta_j \gamma_k g_{ijk}(x) \mid (i,\ j,\ k) \in \{(0,\ 0,\ 0),\ (0,\ 1,\ 0),\ \ldots,\ (1,\ 3,\ 7)\} \right\rangle$
2. A polynomial $g(x) \in \mathscr{R}[x,\ \Theta]$ can be found such that $\mathscr{C} = \langle g(x) \rangle$, where

$$g(x) = \sum_{i=0}^{1} \sum_{j=0}^{3} \sum_{k=0}^{7} \alpha_i \beta_j \gamma_k g_{ijk}, \tag{35}$$

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

Proof. For the first part, based on Theorem 4.2 it is established that the sets $\mathscr{C}_{ijk}$ represent skew cyclic codes of length n over $\mathscr{R}$ for $0 \le i \le 1$, $0 \le j \le 3$, and $0 \le k \le 7$. Hence, each $\mathscr{C}_{ijk}$ can expressed as $\langle g_{ijk}(x) \rangle$. On the other hand, the code $\mathscr{C} = \bigoplus_{i=0}^{1} \bigoplus_{j=0}^{3} \bigoplus_{k=0}^{7} \alpha_i \beta_j \gamma_k \mathscr{C}_{ijk}$, so that

$$\mathscr{C} \subseteq \left\langle \alpha_i \beta_j \gamma_k g_{ijk}(x) \mid (i,\ j,\ k) \in \{(0,\ 0,\ 0),\ (0,\ 1,\ 0),\ \ldots,\ (1,\ 3,\ 7)\} \right\rangle. \tag{36}$$

Concerning the second inclusion, we have the following details and information

$$\sum_{i=0}^{1} \sum_{j=0}^{3} \sum_{k=0}^{7} \alpha_i \beta_j \gamma_k g_{ijk}(x) h_{ijk}(x) \in \left\langle \alpha_i \beta_j \gamma_k g_{ijk}(x) \mid (i,\ j,\ k) \in \{(0,\ 0,\ 0),\ (0,\ 1,\ 0),\ \ldots,\ (1,\ 3,\ 7)\} \right\rangle.$$

So, the expression indicates that $h_{ijk}(x)$ belongs to the quotient ring $\mathscr{R}[x,\ \Theta]/\langle x^n - 1 \rangle$. For each polynomial $h_{ijk}(x)$, there exists another polynomial $r_{ijk}(x)$ in the same skew polynomial ring such that

$$\alpha_i \beta_j \gamma_k s_{ik}(x) = \alpha_i \beta_j \gamma_k r_{ik}(x)\ for\ 0 \le i \le 1,\ 0 \le j \le 3, \text{ and } 0 \le k \le 7. \tag{37}$$

This means that every polynomial $h_{ijk}(x)$ can be replaced by some corresponding $r_{ijk}(x)$ that still satisfies the equation, ensuring that the structure of the ideal is preserved. Hence,

$$\mathscr{C} \supseteq \left\langle \alpha_i\beta_j\gamma_k g_{ijk}(x) \mid (i,\ j,\ k) \in \{(0,\ 0,\ 0),\ (0,\ 1,\ 0),\ \ldots,\ (1,\ 3,\ 7)\}\right\rangle. \tag{38}$$

After examining Equations (36) and (37), the resulting conclusion is as follows

$$\mathscr{C} = \left\langle \alpha_i\beta_j\gamma_k g_{ijk}(x) \mid (i,\ j,\ k) \in \{(0,\ 0,\ 0),\ (0,\ 1,\ 0),\ \ldots,\ (1,\ 3,\ 7)\}\right\rangle.$$

This means that the code $\mathscr{C}$ can be generated by the set of all these generator polynomials $g_{ijk}(x)$ multiplied by the corresponding $\alpha_i\beta_j\gamma_k$.

For the second part, assume that $g_{ijk}(x)$, for $0 \leq i \leq 1$, $0 \leq j \leq 3$ and $0 \leq k \leq 7$, is a monic generator polynomial of $\mathscr{C}_{ijk}$. Then $g_{ijk}(x)$ divides $x^n - 1$ on the right such that

$$x^n - 1 = h_{ijk}(x)g_{ijk}(x),\ h_{ijk}(x) \in \mathscr{C}_{ik}, \text{ for } 0 \leq i \leq 3 \text{ and } 0 \leq k \leq 7.$$

We can represent this as

$$x^n - 1 = \sum_{i=0}^{3}\sum_{j=0}^{3}\sum_{k=0}^{7} \alpha_i\beta_j\gamma_k(x^n - 1)$$

$$= \alpha_0\beta_0\gamma_0(x^n - 1) + \alpha_0\beta_1\gamma_0(x^n - 1) + \cdots + \alpha_1\beta_3\gamma_7(x^n - 1),$$

which further simplifies to

$$= \alpha_0\beta_0\gamma_0 h_{000}(x)g_{000}(x) + \alpha_0\beta_1\gamma_0 h_{010}(x)g_{010}(x) + \cdots + \alpha_1\beta_3\gamma_7 h_{137}(x)g_{137}(x),$$

and finally, the summation form becomes

$$= \sum_{i=0}^{1}\sum_{j=0}^{3}\sum_{k=0}^{7} \alpha_i\beta_j\gamma_k h_{ijk}(x)g_{ijk}(x) = h(x)g(x).$$

This means that the polynomial $x^n - 1$ is expressed as a product of the polynomials $h_{ijk}(x)$ and $g_{ijk}(x)$, for $0 \leq i \leq 1$, $0 \leq j \leq 3$ and $0 \leq k \leq 7$. The structure of the code is preserved as $h(x)g(x)$ represents the code $\mathscr{C}$ generated by the polynomials $g_{ijk}(x)$. Hence, $g(x)$ divides $x^n - 1$ on the right. □

Theorem 4.6 Let $\mathscr{C} = \bigoplus_{i=0}^{1}\bigoplus_{j=0}^{3}\bigoplus_{k=0}^{7} \alpha_i\beta_j\gamma_k\mathscr{C}_{ijk}$ be a skew cyclic code of length n over $\mathscr{R}$. Assume that $g_{ijk}(x)$, is a generator polynomial of $\mathscr{C}_{ijk}$, for $0 \leq i \leq 1$, $0 \leq j \leq 3$, and $0 \leq k \leq 7$. Then

$$\mid \mathscr{C} \mid = q^{64n - \sum_{i=0}^{1}\sum_{j=0}^{3}\sum_{k=0}^{7} g_{ijk}(x)} \tag{39}$$

Proof. As stated in Theorem 3.2 the equality shown below holds true. □

Corollary 4.7 Let $\mathscr{C}_{ijk}$, for $0 \leq i \leq 1$, $0 \leq j \leq 3$, and $0 \leq k \leq 7$, be skew cyclic codes over $\mathbb{F}_q$ and $g_{ijk}(x)$, for $0 \leq i \leq 1$, $0 \leq j \leq 3$, and $0 \leq k \leq 7$, their generator polynomials, sach that $x^n - 1 = h_{ijk}(x)g_{ijk}(x) \in \mathscr{R}[x, \Theta]$. If $\mathscr{C}$ is a skew cyclic code over $\mathscr{R}$, then $\mathscr{C}^{\perp} = \sum_{i=0}^{1}\sum_{j=0}^{3}\sum_{k=0}^{7}\alpha_i\beta_j\gamma_k h_{ijk}(x)$, where $h_{ijk}(x)$ are the reciprocal polynomials of $g_{ijk}(x)$ and $h_{ijk}(x) = x^{\deg(g_{ijk}(x))}g_{ijk}(x^{-1})$, for $0 \leq i \leq 1$, $0 \leq j \leq 3$, and $0 \leq k \leq 7$, furthermore

$$|\mathscr{C}^{\perp}| = p^{\sum_{i=0}^{1}\sum_{j=0}^{3}\sum_{k=0}^{7} deg(g_{ijk}(x))}. \tag{40}$$

Proof. The proof closely parallels the one provided for Theorem 4.6. □

5. Utilizing skew cyclic codes over $\mathscr{R}$ to identify skew cyclic codes over $\mathbb{F}_q$ with optimal parameters

Based on [19], a linear code over a finite field is deemed to have good parameters if it satisfies specific bounds, including:

Singleton bound: $d \leq n - k + 1$,

Griesmer bound: $n \geq \sum_{i=0}^{k-1} \frac{d_H}{q^i}$,

Gilbert-Varshamov bound: $A_q(n, d) \geq \frac{q^n}{\sum_{i=0}^{d-1} C_n^i (q-1)^i}$, with $A_q(n, d)$ represents the maximum size of a q-ary code with block length n and minimum distance d.

The primary goal of this research is to develop error-correcting codes with optimal parameters over the finite field $\mathbb{F}_q$ by utilizing the unique structure of skew cyclic codes within the ring $\mathscr{R}$. This aim arises from the practical necessity for highly effective error-correcting codes across various fields, including digital communication systems, cryptography, and other information processing applications. These codes are crucial for ensuring the integrity and security of data transmitted or processed in these domains. To achieve this, the research utilizes advanced computational tools like Magma and Sagemath, along with a detailed database provided by Codetables (https://www.codetables.de). These resources have been instrumental in identifying several codes that exhibit optimal or near-optimal parameters.

Example 5.1 Consider $\mathscr{R} = (\mathbb{F}_4 + u\mathbb{F}_4)(\mathbb{F}_4 + u\mathbb{F}_4 + v\mathbb{F}_4 + uv\mathbb{F}_4)(\mathbb{F}_4 + u\mathbb{F}_4 + v\mathbb{F}_4 + w\mathbb{F}_4 + uv\mathbb{F}_4 + uw\mathbb{F}_4 + vw\mathbb{F}_4 + uvw\mathbb{F}_4)$, utilizing Magma to compute the factorization of $x^{20} - 1 = (x+1)^4(x^2 + \alpha x + 1)^4(x^2 + \alpha^2 x + 1)^4$ through the following algorithm

Algorithmic 1 Factorization of $x^{20} - 1$

1. $\mathbb{F}_4$: = GF(4); // Define the finite field $\mathbb{F}_4$.
2. $P < x >$:= PolynomialRing($\mathbb{F}_4$); // Define the polynomial ring over $\mathbb{F}_4$.
3. Factorization $(x^{20} - 1)$; // Factorize $x^{20} - 1$ over $\mathbb{F}_4$.

Note that, for $0 \leq i \leq 1$, $0 \leq j \leq 3$, and $0 \leq k \leq 7$, $\mathscr{C}_{ijk}$ denotes a skew cyclic code over $\mathbb{F}_4$ defined by the generator polynomial $\langle 1\alpha^2 0\alpha^2 0\alpha^2 0\alpha^2 0\alpha^2 1\rangle$, and $\mathscr{C}$ is a code characterized by the parameters $[20, 10, 8]$. In accordance with Lemma 2.3, Theorems 4.2, and 4.5, it can be concluded that $\Phi(\mathscr{C})$ $[280, 140, 112]$ forms a skew cyclic code over $\mathbb{F}_4$ with good parameters.

The Tables 1-6. present a compilation of codes, highlighting their potential applicability and effectiveness for reference.

Table 1. Linear skew cyclic codes with good parameters over $\mathbb{F}_2$

n	k	d	$\mathscr{C}_{ijk} = \langle g_{ijk}(x) \rangle$	n'	k'	d'	O
27	9	9	(000000000110100111)	378	126	126	O
42	7	19	(000000000000000000000000000000110111)	588	98	266	O
51	19	14	(101000001001010010101111101101011)	714	266	196	O
73	36	16	(11011100001011011011001000110110101001)	1,022	504	224	O
78	12	32	000000000000000000000000000111111 011111001101011101101001011001000	1,092	168	448	O
90	14	36	000000000000000000000000000000000000 0000000000000000000111001001100001101	1,260	196	504	O

Table 2. Linear skew cyclic codes with good parameters over $\mathbb{F}_3$

n	k	d	$\mathscr{C}_{ijk} = \langle g_{ijk}(x) \rangle$	n'	k'	d'	O
28	8	15	(12110111020121002111)	392	112	210	O
30	10	13	(00000000002200200211)	420	140	182	O
36	9	18	(000000000000000000010210121)	504	126	252	O
50	10	25	(00000000000000000000000000000002222100112)	700	140	350	O
68	16	30	000000000000000000020201100 22211122011210101202212002	950	224	420	O
160	8	99	0000000000000000000000000000000000000000 0000000000000000000000000000000000001101 01201022002211202211001010011201002101 10210121122110222102111102220100000001	2,240	112	1,386	O
182	12	104	000000000000000000000000000000000000 000000000000000000000000000000000000 00000000000121201110212210121121101 12122210222210122220122212110110211 210122120111021210100000000000011022	2,548	168	1,456	O
182	36	72	1212101100122000121220122201022221120 1000110101202001222011210121202212202 1200011200211110121212010122210201120 010111111222021111021210021202010001	2,548	504	1,008	O

Table 3. Linear skew cyclic codes with good parameters over $\mathbb{F}_4$

n	k	d	$\mathscr{C}_{ijk} = \langle g_{ijk}(x) \rangle$	n'	k'	d'	O
21	15	5	$\left(1\alpha^2 10\alpha^2 1\alpha^2\right)$	294	210	70	O
43	36	5	$\left(10\alpha 11\alpha^2 01\right)$	602	504	70	O
51	6	34	$\begin{pmatrix} 1\alpha^2\alpha 0\alpha^2\alpha^2 0\alpha\alpha\alpha^2\alpha\alpha^2 0\alpha^2\alpha^2\alpha^2\alpha^2 1\alpha 0\alpha^2\alpha \\ \alpha\alpha^2 00\alpha 0\alpha\alpha^2\alpha\alpha\alpha\alpha 10\alpha^2\alpha 00\alpha\alpha^2\alpha^2 0\alpha^2 0\alpha \end{pmatrix}$	714	84	476	O
58	15	28	$\begin{pmatrix} 000000000000000\alpha\alpha\alpha^2\alpha 01\alpha 11 \\ \alpha^2 01000\alpha^2 11\alpha\alpha 0\alpha\alpha^2 1\alpha^2\alpha^2 010 \end{pmatrix}$	812	210	392	O
63	45	7	$\begin{pmatrix} 1\alpha^2\alpha^2 1\alpha\alpha^2 11\alpha\alpha 0\alpha^2 01\alpha\alpha^2\alpha^2 01 \end{pmatrix}$	882	630	98	O
65	51	5	$\left(11\alpha^2 1\alpha^2 0\alpha^2 1\alpha^2 0\alpha^2 1\alpha^2 11\right)$	910	714	70	O
85	14	48	$\begin{pmatrix} 1\alpha 0\alpha 00\alpha^2 111\alpha\alpha\alpha\alpha^2\alpha 0001\alpha 01\alpha^2 1 \\ 0\alpha\alpha 1\alpha^2 001\alpha^2\alpha 1\alpha 00\alpha^2\alpha 1\alpha^2\alpha\alpha\alpha\alpha^2 1\alpha \\ \alpha\alpha 1\alpha 01\alpha 1\alpha^2\alpha^2\alpha^2 110\alpha 1\alpha 0\alpha^2\alpha\alpha 011 \end{pmatrix}$	1,190	196	672	O
111	93	8	$\left(1\alpha\alpha^2\alpha\alpha^2 10\alpha^2\alpha^2\alpha^2\alpha^2 0\alpha^2\alpha^2\alpha^2\alpha\alpha 11\right)$	1,554	1,302	112	O
255	18	156	$\begin{pmatrix} 10\alpha^2 110\alpha^2\alpha 1\alpha^2\alpha\alpha\alpha\alpha 1\alpha 001\alpha\alpha^2\alpha^2 10\alpha^2 101 \\ 10\alpha^2\alpha^2 0\alpha\alpha^2\alpha 11\alpha\alpha 0\alpha\alpha^2\alpha 0\alpha\alpha\alpha^2\alpha^2 0000\alpha\alpha^2 \\ 0\alpha\alpha 0111\alpha 010\alpha\alpha 0\alpha\alpha^2\alpha^2 00\alpha\alpha^2\alpha 1\alpha^2 0\alpha^2\alpha^2 0 \\ \alpha^2\alpha^2\alpha 1\alpha^2 1110\alpha^2 000\alpha^2 011\alpha^2 10\alpha\alpha^2\alpha^2 1000 \\ \alpha^2 00\alpha\alpha 1\alpha\alpha\alpha\alpha 0\alpha\alpha^2\alpha 0\alpha^2 0\alpha\alpha^2\alpha^2 1\alpha^2 0\alpha\alpha^2\alpha^2 1 \\ \alpha 1\alpha^2\alpha^2 0\alpha 0\alpha^2\alpha^2 00\alpha^2 0\alpha\alpha^2\alpha^2 10011\alpha^2 1\alpha^2 1\alpha\alpha \\ 00\alpha 10\alpha^2 1\alpha 0\alpha 1111\alpha^2\alpha^2\alpha\alpha^2\alpha^2 00\alpha^2\alpha 11\alpha^2 1 \\ 01\alpha^2 01\alpha 00\alpha\alpha\alpha\alpha^2\alpha 110\alpha^2\alpha 1\alpha^2 10\alpha 11\alpha^2\alpha 1\alpha^2 \\ 11110\alpha 1\alpha\alpha^2 00\alpha\alpha 1\alpha^2 0\alpha^2 \end{pmatrix}$	3,570	252	2,184	O

Table 4. Linear skew cyclic codes with good parameters over $\mathbb{F}_5$

n	k	d	$\mathscr{C}_{ijk} = \langle g_{ijk}(x) \rangle$	n'	k'	d'	O
31	10	15	$(130133223443300004240 14)$	434	140	210	O
50	25	15	$(13112312200243422442133 41)$	700	350	210	O
63	50	8	$(14320341203412032 14)$	882	700	112	O
124	12	83	$\begin{pmatrix} 12310323224042131134233444 20 \\ 40413143211031422103133340 14 \\ 41233341431002140113013121 23 \\ 02323400043140040303423200 01 \end{pmatrix}$	1,736	168	11,626	O

Table 5. Linear skew cyclic codes with good parameters over $\mathbb{F}_7$

n	k	d	$\mathscr{C}_{ijk} = \langle g_{ijk}(x) \rangle$	n'	k'	d'	O
24	12	10	(15246351001)	336	168	140	O
29	7	19	(1636301660425313541111)	406	98	266	O
40	20	14	(122226321653345615221)	560	280	196	O
50	36	10	(134024606320441)	700	504	140	O
50	16	26	$\left(113642461010035450535400101145413 61\right)$	700	224	364	O
100	4	84	$\begin{pmatrix} 1105343524144204564323101424415 30 \\ 543132233320610006602434253633 50 \\ 321345460635336240234645544450 16 \end{pmatrix}$	1,400	56	1,176	O

Table 6. Linear skew cyclic codes with good parameters over $\mathbb{F}_8$

n	k	d	$\mathscr{C}_{ijk} = \langle g_{ijk}(x) \rangle$	n'	k'	d'	O
19	13	6	$(1\alpha^5\alpha^3\alpha^3\alpha^3\alpha^5 1)$	266	182	846	O
37	24	10	$(1\alpha^4 0\alpha^3 111111\alpha^3\alpha^4 1)$	518	336	140	O
40	20	14	$(\alpha^6\alpha^2\alpha^6\alpha^6\alpha^4\alpha^6\alpha^5 00\alpha\alpha^3\alpha^6 0\alpha\alpha^5\alpha^4\alpha^6\alpha^5 10)$	560	280	196	O
57	50	6	$(1\alpha^4\alpha\alpha^4\alpha^4\alpha\alpha^4 1)$	798	700	84	O
73	9	52	$\begin{pmatrix} 11\alpha\alpha^2 10\alpha^2\alpha^5\alpha^4\alpha^6\alpha^4 11\alpha^2 1\alpha^2\alpha^6 \\ 11\alpha\alpha\alpha^4\alpha^6\alpha^5 1\alpha^6 1\alpha^6\alpha^3\alpha^2\alpha^4 1\alpha^3 \\ \alpha\alpha^6\alpha^5\alpha^6\alpha^3\alpha^3\alpha^4\alpha\alpha^3\alpha^5\alpha^3 0\alpha\alpha^3 1\alpha^2 \\ \alpha^4\alpha\alpha^6\alpha^4 00\alpha^3\alpha^2\alpha^3\alpha^4\alpha^6\alpha^3\alpha 01 \end{pmatrix}$	1,022	126	728	O
73	58	7	$(1\alpha^5\alpha^3\alpha^3\alpha^3\alpha^6\alpha\alpha^2\alpha^6 10\alpha^2\alpha^3\alpha^3\alpha^4 1)$	1,022	812	98	O
103	17	64	$\begin{pmatrix} 1\alpha^2\alpha 1\alpha^3\alpha\alpha 01\alpha^2\alpha^4\alpha^6\alpha^2\alpha^5\alpha^3\alpha^6 1\alpha^3\alpha^4\alpha^3 0\alpha^4 \\ \alpha^3 0\alpha 1\alpha^4\alpha 11\alpha^3\alpha^6\alpha^5 0\alpha 1\alpha^4\alpha^5 0\alpha\alpha^5\alpha^2 11\alpha^6\alpha 0 \\ \alpha^6\alpha^6\alpha^2\alpha^6\alpha^5\alpha^5\alpha\alpha^6 1\alpha^5\alpha^3\alpha^6\alpha^2\alpha^5\alpha^5\alpha^5\alpha\alpha^2\alpha^2 \\ \alpha^4\alpha^3\alpha^4\alpha\alpha^2 0\alpha^5\alpha^3\alpha^2\alpha^3\alpha^4\alpha^6\alpha^2\alpha^3\alpha^4 1\alpha^6\alpha^5\alpha^5 1 \end{pmatrix}$	1,442	238	896	O

5.1 *Practical application: optimal skew cyclic codes for multi-secret sharing schemes*

This section demonstrates the steps involved in the new multi-secret sharing scheme, ref showing how linear algebra techniques can be applied to share and recover multiple secrets securely [20]. Let $\Phi(\mathscr{C})$ be an $[n, k]$-code over $\mathbb{F}_q$, defined by a generator matrix $\Phi(\mathscr{G})$ and a parity-check matrix $\Phi(\mathscr{H})$. Since the rank of $\Phi(\mathscr{G})$, denoted $r(\Phi(\mathscr{G}))$, is equal to k, the transpose of $\Phi(\mathscr{G})$, written as $\Phi(\mathscr{G})^T$, is an $k \times n$ matrix with full column rank k.

Theorem 5.2 [20] Let $\Phi(\mathscr{G})$ be a generator matrix of an $[n,\ k]$-code $\Phi(\mathscr{C})$ over $\mathbb{F}_q$. Then there exists a unique word $x = (\Phi(\mathscr{G})^T)^+ s$ in $(\mathbb{F}_q)^k$ that approximates a received word s near the codewords of $\Phi(\mathscr{C})$ if and only if the following equation is satisfied.

$$r(\Phi(\mathscr{G})) = r(\Phi(\mathscr{G})\Phi(\mathscr{G})^T) = r(\Phi(\mathscr{G})^T\Phi(\mathscr{G})) \neq 0. \tag{41}$$

Proposition 5.3 In the scheme just introduced, the secret is determined if and only if

$$r(\Phi(\mathscr{G})) = r(\Phi(\mathscr{G})\Phi(\mathscr{G})^T) = r(\Phi(\mathscr{G})^T\Phi(\mathscr{G})) \neq 0 \tag{42}$$

is satisfied.

Proof. According to Theorem 5.1 a unique word $x \in (\mathbb{F}_5)^k$ approximates a received word s near the codewords of $\Phi(\mathscr{C})$ if and only if the condition $r(\Phi(\mathscr{G})) = r(\Phi(\mathscr{G})\Phi(\mathscr{G})^T) = r(\Phi(\mathscr{G})^T\Phi(\mathscr{G}))$ is met. □

In this scheme, sharing a secret among n participants is formalized using a mathematical approach where each participant receives a share via a sharing function. First, it is essential to note that $\Phi(\mathscr{G})^+ = \Phi(\mathscr{G})^T(\Phi(\mathscr{G})\Phi(\mathscr{G})^T)^{-1}$. The sharing function is defined as

$$f(s) = s - \Phi(\mathscr{G})^T x, \tag{43}$$

where $s = (s_1\ s_2\ \ldots\ s_n)$ represents the secret to be shared, and $\Phi(\mathscr{G})$ is a $k \times n$ matrix over $(\mathbb{F}_q)^n$ with rank k. Here, x is computed as

$$x = (\Phi(\mathscr{G})^T)^+ s, \tag{44}$$

utilizing the pseudoinverse of $\Phi(\mathscr{G})$. The scheme operates under specific steps. First, participants belong to the set $(\mathbb{F}_q)^n$, and the secret space is defined as $(\mathbb{F}_q)^n/(\mathbb{F}_q)^k$, where the secret s resides. The secret s can be represented as

$$s = \Phi(\mathscr{G})^T x \tag{45}$$

with $x \in (\mathbb{F}_q)^k$. To establish that there is a unique x for secret recovery, the rank condition is required:

$$\text{rank}(\Phi(\mathscr{G})) = \text{rank}(\Phi(\mathscr{G})\Phi(\mathscr{G})^T) = \text{rank}(\Phi(\mathscr{G})^T\Phi(\mathscr{G})).$$

Once verified, the share for each participant is calculated as

$$r = f(s) = s - \Phi(\mathscr{G})^T x. \tag{46}$$

To reconstruct the secret, one solves the system

$$(s_1\ s_2\ \dots\ s_n) - \Phi(\mathscr{G})^T x = r. \tag{47}$$

By solving this equation, the original secret s is successfully recovered, completing the sharing and recovery process.

Example 5.4 Let $f : (\mathbb{F}_5)^{16}/(\mathbb{F}_5)^{16} \longrightarrow (\mathbb{F}_5)^{16}$. We construct a multisecret-sharing scheme based on $[16,\ 16]$-code linear over $\mathbb{F}_5$ with generator matrix G by using

$$r(\Phi(\mathscr{G})) = r(\Phi(\mathscr{G})\Phi(\mathscr{G})^T) = r(\Phi(\mathscr{G})^T\Phi(\mathscr{G})).$$

We know that $r(\Phi(\mathscr{G})) = 16$, where $r(\Phi(\mathscr{G}))$ is the rank of $\Phi(\mathscr{G})$. So $\Phi(\mathscr{G})^T$, the transpose of $\Phi(\mathscr{G})$ is an 16×16 matrix of full column rank 16. The generator matrix of this code is given by

$$\Phi(\mathscr{G}) = \begin{bmatrix}
2&0&0&0&0&0&0&0&3&1&0&2&4&2&0&2\\
4&3&0&0&0&2&4&4&1&0&2&4&4&0&0&0\\
0&2&0&0&0&0&0&0&3&1&0&2&4&2&0&2\\
0&0&2&0&0&0&0&0&0&3&1&0&2&4&2&0\\
0&0&0&2&0&0&0&0&0&0&3&1&0&2&4&2\\
0&0&0&0&2&0&0&0&0&0&0&3&1&0&2&4\\
0&0&0&0&0&2&0&0&0&0&0&0&3&1&0&2\\
0&0&0&0&0&0&2&0&0&0&0&0&0&0&3&1\\
0&0&0&0&0&0&0&2&0&0&0&0&0&0&0&3\\
0&0&0&0&0&0&0&0&2&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&2&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&2&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&2&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&2&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&0
\end{bmatrix},$$

then

$$\Phi(\mathscr{G})^T = \begin{bmatrix} 2 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 3 & 1 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 2 & 4 & 2 & 0 & 1 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 4 & 4 & 4 & 2 & 0 & 1 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ 2 & 0 & 2 & 4 & 2 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 & 4 & 2 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \\ 2 & 0 & 2 & 0 & 2 & 4 & 2 & 1 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Let the secret $s = (1\,2\,3\,4\,0\,1\,2\,3\,4\,0\,1\,2\,3\,4\,0\,1) \notin \Phi(\mathscr{C})$. This means the equality $s = \Phi(\mathscr{G})^T x$ is inconsistent.

$$\Phi(\mathscr{G})^T \Phi(\mathscr{G}) = \begin{bmatrix} 0 & 2 & 0 & 0 & 0 & 3 & 1 & 1 & 0 & 2 & 3 & 0 & 4 & 4 & 0 & 4 \\ 2 & 3 & 0 & 0 & 0 & 1 & 2 & 2 & 4 & 2 & 1 & 1 & 0 & 4 & 0 & 4 \\ 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 0 & 4 & 3 & 4 & 0 \\ 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 0 & 4 & 3 & 4 \\ 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 0 & 4 & 3 \\ 3 & 1 & 0 & 0 & 0 & 3 & 3 & 3 & 2 & 0 & 4 & 3 & 4 & 2 & 0 & 4 \\ 1 & 2 & 0 & 0 & 0 & 3 & 0 & 1 & 4 & 0 & 3 & 1 & 1 & 0 & 1 & 2 \\ 1 & 2 & 0 & 0 & 0 & 3 & 1 & 0 & 4 & 0 & 3 & 1 & 1 & 0 & 0 & 1 \\ 0 & 4 & 0 & 0 & 0 & 2 & 4 & 4 & 3 & 1 & 2 & 1 & 3 & 2 & 0 & 2 \\ 2 & 2 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 3 & 4 & 4 & 1 & 1 & 4 \\ 3 & 1 & 2 & 1 & 0 & 4 & 3 & 3 & 2 & 3 & 3 & 1 & 0 & 0 & 4 & 1 \\ 0 & 1 & 0 & 2 & 1 & 3 & 1 & 1 & 1 & 4 & 1 & 3 & 0 & 0 & 0 & 2 \\ 4 & 0 & 4 & 0 & 2 & 4 & 1 & 1 & 3 & 4 & 0 & 0 & 1 & 2 & 1 & 1 \\ 4 & 4 & 3 & 4 & 0 & 2 & 0 & 0 & 2 & 1 & 0 & 0 & 2 & 3 & 1 & 4 \\ 0 & 0 & 4 & 3 & 4 & 0 & 1 & 0 & 0 & 1 & 4 & 0 & 1 & 1 & 2 & 4 \\ 4 & 4 & 0 & 4 & 3 & 4 & 2 & 1 & 2 & 4 & 1 & 2 & 1 & 4 & 4 & 2 \end{bmatrix}.$$

Since $r(\Phi(\mathscr{G})) = r(\Phi(\mathscr{G})\Phi(\mathscr{G})^T) = r(\Phi(\mathscr{G})^T\Phi(\mathscr{G})) = 16$, there exists a unique x, meaning the secret can be recovered. Thus, we have

$$
\Phi(\mathscr{G})\Phi(\mathscr{G})^{T} = \begin{bmatrix}
2 & 0 & 3 & 4 & 0 & 3 & 3 & 2 & 1 & 1 & 2 & 0 & 4 & 3 & 4 & 0 \\
0 & 3 & 3 & 0 & 0 & 1 & 1 & 3 & 3 & 2 & 0 & 4 & 3 & 3 & 0 & 0 \\
3 & 3 & 2 & 4 & 0 & 3 & 3 & 2 & 1 & 1 & 2 & 0 & 4 & 3 & 4 & 0 \\
4 & 0 & 4 & 3 & 4 & 1 & 0 & 1 & 0 & 0 & 1 & 2 & 0 & 4 & 3 & 4 \\
0 & 0 & 0 & 4 & 3 & 4 & 1 & 4 & 1 & 0 & 0 & 1 & 2 & 0 & 4 & 3 \\
3 & 1 & 3 & 1 & 4 & 4 & 1 & 0 & 2 & 0 & 0 & 0 & 1 & 2 & 0 & 4 \\
3 & 1 & 3 & 0 & 1 & 1 & 3 & 2 & 1 & 0 & 0 & 0 & 0 & 1 & 2 & 0 \\
2 & 3 & 2 & 1 & 4 & 0 & 2 & 4 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 3 & 1 & 0 & 1 & 2 & 1 & 3 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 \\
0 & 4 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 \\
4 & 3 & 4 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 \\
3 & 3 & 3 & 4 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 \\
4 & 0 & 4 & 3 & 4 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 \\
0 & 0 & 0 & 4 & 3 & 4 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4
\end{bmatrix}.
$$

It is clear that

$$
(\Phi(\mathscr{G})\Phi(\mathscr{G})^{T})^{-1} = \begin{bmatrix}
2 & 2 & 4 & 0 & 2 & 4 & 0 & 2 & 4 & 0 & 2 & 0 & 3 & 2 & 2 & 4 \\
2 & 1 & 0 & 0 & 4 & 3 & 3 & 0 & 4 & 4 & 4 & 3 & 2 & 3 & 0 & 4 \\
4 & 0 & 3 & 0 & 4 & 3 & 4 & 2 & 1 & 2 & 4 & 4 & 4 & 1 & 2 & 1 \\
0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 3 & 0 & 1 & 2 & 1 \\
2 & 4 & 4 & 0 & 4 & 0 & 1 & 2 & 2 & 4 & 2 & 0 & 4 & 1 & 2 & 4 \\
4 & 3 & 3 & 0 & 0 & 4 & 2 & 4 & 4 & 3 & 4 & 2 & 1 & 0 & 2 & 0 \\
0 & 3 & 4 & 0 & 1 & 2 & 2 & 2 & 3 & 0 & 3 & 3 & 4 & 2 & 4 & 3 \\
2 & 0 & 2 & 0 & 2 & 4 & 2 & 0 & 3 & 4 & 3 & 2 & 4 & 2 & 3 & 2 \\
4 & 4 & 1 & 0 & 2 & 4 & 3 & 3 & 4 & 3 & 0 & 3 & 0 & 3 & 4 & 0 \\
0 & 4 & 2 & 0 & 4 & 3 & 0 & 4 & 3 & 4 & 4 & 0 & 1 & 4 & 4 & 3 \\
2 & 4 & 4 & 4 & 2 & 4 & 3 & 3 & 0 & 4 & 0 & 1 & 4 & 2 & 0 & 1 \\
0 & 3 & 4 & 3 & 0 & 2 & 3 & 2 & 3 & 0 & 1 & 2 & 2 & 0 & 1 & 2 \\
3 & 2 & 4 & 0 & 4 & 1 & 4 & 4 & 0 & 1 & 4 & 2 & 2 & 3 & 2 & 0 \\
2 & 3 & 1 & 1 & 1 & 0 & 2 & 2 & 3 & 4 & 2 & 0 & 3 & 3 & 3 & 4 \\
2 & 0 & 2 & 2 & 2 & 2 & 4 & 3 & 4 & 4 & 0 & 1 & 2 & 3 & 2 & 0 \\
4 & 4 & 1 & 1 & 4 & 0 & 3 & 2 & 0 & 3 & 1 & 2 & 0 & 4 & 0 & 2
\end{bmatrix},
$$

and

$$
\Phi(\mathscr{G})^{+} = \begin{bmatrix}
2 & 3 & 3 & 0 & 0 & 0 & 2 & 4 & 4 & 1 & 0 & 2 & 4 & 1 & 4 & 4 \\
4 & 3 & 1 & 0 & 0 & 0 & 2 & 4 & 4 & 1 & 0 & 2 & 4 & 1 & 4 & 4 \\
0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 1 & 0 & 2 & 4 & 2 \\
4 & 3 & 3 & 0 & 3 & 0 & 2 & 4 & 4 & 3 & 4 & 0 & 3 & 2 & 4 & 3 \\
3 & 1 & 1 & 0 & 0 & 3 & 4 & 3 & 3 & 1 & 3 & 4 & 2 & 0 & 4 & 0 \\
4 & 3 & 3 & 0 & 0 & 0 & 0 & 4 & 4 & 3 & 4 & 2 & 2 & 0 & 3 & 4 \\
2 & 4 & 4 & 0 & 0 & 0 & 1 & 0 & 2 & 4 & 2 & 1 & 1 & 1 & 1 & 0 \\
1 & 2 & 2 & 0 & 0 & 0 & 3 & 1 & 4 & 2 & 1 & 3 & 3 & 3 & 3 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 \\
1 & 2 & 2 & 0 & 0 & 0 & 3 & 1 & 1 & 2 & 1 & 3 & 3 & 3 & 3 & 1
\end{bmatrix}.
$$

Thus, x is calculated as

$$x^T = \Phi(\mathscr{G})^T (\Phi(\mathscr{G})\Phi(\mathscr{G})^T)^{-1} s = (3\ 4\ 2\ 0\ 2\ 0\ 3\ 0\ 0\ 3\ 1\ 4\ 2\ 0\ 3\ 3).$$

Let the message vector (1 2 3 4 0 1 2 3 4 0 1 2 3 4 0 1) represent the secret. Then, the sharing function becomes

$$\Phi(\mathscr{G})^T x = (3\ 4\ 2\ 0\ 2\ 0\ 3\ 0\ 0\ 3\ 1\ 4\ 2\ 0\ 3\ 3)$$

and

$$f(s) = s - \Phi(\mathscr{G})^T x = (3\ 3\ 1\ 4\ 3\ 1\ 4\ 3\ 4\ 2\ 0\ 3\ 1\ 4\ 2\ 3).$$

To retrieve the secret s, we solve the following equation:

$$(s_1\ s_2\ \dots\ s_{16}) - (3\ 4\ 2\ 0\ 2\ 0\ 3\ 0\ 0\ 3\ 1\ 4\ 2\ 0\ 3\ 3) = (3\ 3\ 1\ 4\ 3\ 1\ 4\ 3\ 4\ 2\ 0\ 3\ 1\ 4\ 2\ 3). \tag{48}$$

Thus, the secret is

$$(s_1\ s_2\ \dots\ s_{16}) = (1\ 2\ 3\ 4\ 0\ 1\ 2\ 3\ 4\ 0\ 1\ 2\ 3\ 4\ 0\ 1).$$

5.2 *Limitations of the proposed model*

While the proposed model of skew cyclic codes over the ring $\mathscr{R}$ offers significant potential for constructing codes with optimal parameters over $\mathbb{F}_q$, it operates under certain assumptions and limitations that affect its generalizability. Primarily, the construction assumes specific ring structures and relies on the particular algebraic properties of $\mathscr{R} = \mathscr{R}_1 \times \mathscr{R}_2 \times \mathscr{R}_3$, where $\mathscr{R}_i$ are finite commutative rings with selected idempotent decompositions. This choice facilitates the factorization and construction of generator polynomials within the product ring framework but may not apply to rings that lack these properties. Additionally, the computational approach used to achieve optimal parameters-employing tools like Magma, SageMath, and reference tables from Codetables-relies on empirical validation and is limited by computational power and the scope of available databases. Hence, the model's effectiveness in discovering new, optimal skew cyclic codes has some constraints by these tools and the specific parameters (e.g., block length n, field size q) available in pre-existing code tables.

5.3 *Research directions and applicability*

The current study opens several avenues for future research in both theoretical and practical applications of skew cyclic codes over product rings. One promising direction is the exploration of alternative ring structures, including non-commutative or more complex rings, to expand the scope of skew cyclic code applications. Another research focus centers on optimizing parameters more effectively by refining factorization algorithms and computational tools, potentially using quantum computing or machine learning to enhance code search efficiency. In terms of practical applications, the results of this study are particularly relevant for fields requiring robust error-correction mechanisms, such as digital communications, secure data transmission, and cryptographic protocols. The unique structure of skew cyclic codes over $\mathscr{R}$ enables efficient encoding and decoding, with parameters suited to high-reliability environments where data integrity and security are paramount. Subsequent studies could aim to incorporate these codes into real-world communication systems and investigate their application in developing new cryptographic schemes, especially considering the growing demands for data security and integrity in extensive information networks.

6. Conclusion

In conclusion, this article explores the structure and properties of linear codes over the ring $\mathscr{R} = \mathscr{R}_1 \times \mathscr{R}_2 \times \mathscr{R}_3$, with a particular focus on skew cyclic codes. By examining the behavior of these codes over $\mathscr{R}$, we highlight significant characteristics that differentiate them from classical cyclic codes. Additionally, we demonstrate how skew cyclic codes over $\mathscr{R}$ can be utilized to identify skew cyclic codes over the finite field $\mathbb{F}_q$ with optimal parameters. These findings provide valuable insights into the construction of efficient coding schemes and further our understanding of the algebraic structures underlying such codes.

Conflict of interest

The authors declare no competing financial interest.

References

[1] Chatouh K, Guenda K, Gulliver TA, Noui L. On some classes of linear codes over $\mathbb{Z}_2\mathbb{Z}_4$ and their covering radii. *Journal of Applied Mathematics and Computing*. 2017; 53(1): 201-222.

[2] Chatouh K, Guenda K, Gulliver TA. New classes of codes over $R_{q,\ p,\ m} = \mathbb{Z}_{p^m}[u_1,\ u_2,\ \cdots,\ u_q]/\langle u_i^2 = 0, u_iu_j - u_ju_i\rangle$ and their Applications. *Computational and Applied Mathematics*. 2020; 39: 1-19.

[3] Chatouh K. Some codes over $\mathscr{R} = \mathscr{R}_1\mathscr{R}_2\mathscr{R}_3$ and their applications in secret sharing schemes. *Afrika Matematika*. 2024; 35(1): 1.

[4] Chatouh K. Linear codes over $\mathbb{Z}_p\mathscr{R}_1\mathscr{R}_2$ and their applications. *Matematychni Studii*. 2024; 62(1): 3-10.

[5] Chatouh K, Guenda K, Gulliver TA, Noui L. Simplex and MacDonald codes over R_q. *Journal of Applied Mathematics and Computing*. 2017; 55: 455-478.

[6] Dinh HQ, Bag T, Upadhyay AK, Bandi R, Tansuchat RA. A class of skew cyclic codes and application in quantum codes construction. *Discrete Mathematics*. 2021; 344(2): 112-189.

[7] Ranya DB, Aicha B. Skew Constacyclic and LCD Codes over $\mathbb{F}_q + v\mathbb{F}_q$. *arXiv:190208557*. 2019. Available from: https://arxiv.org/pdf/1902.08557.

[8] Islam H, Prakash O. 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:190208557*. 2018. Available from: https://arxiv.org/abs/1710.07785v2.

[9] Dertli A, Cengellenmis Y. Skew cyclic codes over $F_q + uF_q + vF_q + uvF_q$. *Journal of Science and Arts*. 2017; 17: 215-222.

[10] Ndiaye O. One cyclic codes over $F_p^k + vF_p^k + v^2F_p^k + \ldots + v^rF_p^k$. *Gulf Journal of Mathematics*. 2016; 4(4): 98-12.

[11] Melakhessou A, Chatouh K, Guenda K. DNA multi-secret sharing schemes based on linear codes over $\mathbb{Z}_4 \times R$. *Journal of Applied Mathematics and Computing*. 2023; 69(6): 4833-4853.

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

[13] Yao T, Shi M, Solé P. Skew cyclic codes over $\mathbb{F} + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$. *Journal of Algebra Combinatorics Discrete Structures and Applications*. 2015; 2: 163-168.

[14] Haddouche O, Chatouh K. Hommogenous on weights over the ring $R_{5,\,3} = \mathbb{F}_5 + u_1\mathbb{F}_5 + u_2\mathbb{F}_5 + u_3\mathbb{F}_5$. *Advances in Mathematics, Scientific Journal*. 2022; 11: 1103-1114.

[15] Atiyah MF, MacDonald IG. *Introduction to Commutative Algebra*. Addison-Wesley; 1969.

[16] Dertli A, Cengellenmis Y, Eren S. On the codes over a semilocal finite ring. *International Journal of Advanced Computer Science and Applications*. 2015; 6(10): 1-5.

[17] Mohammadi R, Rahimi S, Mousavi H. On skew cyclic codes over a finite ring. *Iranian Journal of Mathematical Sciences and Informatics*. 2019; 14(1): 135-145.

[18] Boucher D, Umer F. Coding with skew polynomial rings. *Journal of Symbolic Computation*. 2009; 44: 1644-1656.

[19] Sari M. One-weight codes over the ring $\mathbb{F}_q[v]/ < v^s - 1 >$. *Journal of Engineering Technology and Applied Sciences*. 2023; 8: 35-47.

[20] Çalkavur S, Nauman SK, Özel C, Zekraoui H. The least-squares solutions in linear codes based multisecret-sharing approach. *International Journal of Information and Coding Theory*. 2019; 5(3/4): 290.