Palestine Journal of Mathematics

Vol 14(4)(2025) , 90–106

Utilizing Additive Simplex Codes over the Ring $\mathbb{Z}_2\mathbb{Z}_6$ in Some Applications

Mohammed. M. Al-Ashker and Karima Chatouh

Communicated by: Manoj Kumar Patel

MSC 2010 Classifications: Primary 16P10; Secondary 11T71.

Keywords and phrases: Simplex codes, Finite rings, Additive codes, Covering radius, Chinese Euclidean weights.

The authors would like to thank the reviewers and editor for their constructive comments and valuable suggestions that improved the quality of our paper.

Corresponding Author: Karima Chatouh

Abstract *This work explores the application of simplex codes of types α, β, and γ over the ring $\mathbb{Z}_2\mathbb{Z}_6$. It investigates the covering radius of Simplex Codes belonging to these types, examining their capabilities in error detection and correction. Additionally, the research introduces a multi-secret sharing scheme grounded in α, β, and γ-linear Simplex Codes, scrutinizing the scheme's characteristics and presenting data concerning coalitions. The article culminates in a thorough security assessment of the multi-secret sharing scheme, providing insights into the reliability and robustness of employing α, β, and γ linear Simplex Codes in cryptography.*

1 Introduction

Simplex codes have become fundamental in various algebraic structures due to their significance in coding theory and cryptographic applications. These codes are fundamental to error detection and correction, making them fundamental in communication systems and secure data transmission. In particular, researchers have explored their properties over different rings and fields, leading to various generalizations and extensions. Exploring simplex codes over various algebraic structures has been a subject of extensive research. Specifically, in [3] and [4], simplex codes of types α and β were introduced over the ring $\mathbb{F}_2 + u\mathbb{F}_2$, where $u^2 = 0$. These codes served as generalizations and extensions of simplex codes over $\mathbb{Z}_4$ and $\mathbb{Z}_{2^s}$. Simultaneously, simplex linear codes of types α and β over the ring $\mathbb{F}_2 + v\mathbb{F}_2$ were presented, where $v^2 = v$ and $\mathbb{F}_2 = \{0, 1\}$, along with their associated properties. The authors in [9] and [10] extended this exploration by constructing simplex codes of types α, β, and γ over the ring $\mathbb{F}_3 + v\mathbb{F}_3$, where $v^2 = 1$ and $\mathbb{F}_3 = \{0, 1, 2\}$, determining the minimum Hamming, Lee, and Bachoc weights of these codes. Additionally, senary simplex codes of types α, β, and γ over $\mathbb{Z}_6$ were determined in [19], and quaternary MacDonald codes were obtained in [15].

The exploration of codes over finite commutative rings has been motivated by their connection to codes over finite fields, facilitated by the Gray map. This research area has gained prominence, recently focusing on additive codes. Notably, Delsarte's contributions in [17] to the algebraic theory of association schemes have provided valuable insights into characterizing subgroups within association schemes, generating significant interest within the coding theory community.

The study of covering radii has been pivotal in understanding the error-correcting capabilities of codes. In [14], exploring the covering radius of linear codes over binary finite fields was done, while works such as [1], [6], [7], and [8] delved into covering radii of additive codes over $\mathbb{Z}_2\mathbb{Z}_4$. Contributions in [13] provided both lower and upper bounds on the covering radius for codes over the ring $\mathbb{Z}_6$. Moreover, in [12], the types α and β of Simplex and MacDonald codes over $\mathbb{Z}_2\mathbb{Z}_4$ were introduced, followed by an analysis of their covering radii.

Concurrently, these investigations contribute to a comprehensive understanding of codes *over diverse algebraic structures, offering insights into their properties, applications in covering radii, and multi-secret sharing scheme Based on* α*,* β *and* γ*-linear simplex codes.*

The article's structure unfolds systematically, beginning with Section 2, which furnishes essential background and preliminary information. There are two subsections in this section. The initial subsection, the Hamming weight of linear codes over $\mathbb{Z}_2\mathbb{Z}_6$*, meticulously elucidates the concept of Hamming weight within the realm of linear codes over the ring* $\mathbb{Z}_2\mathbb{Z}_6$*. It delves into the nuanced properties and characteristics of Hamming weights specific to these codes. The subsequent subsection, bounds on the covering radius: Upper and lower limits, rigorously explores the constraints on the covering radius for linear codes over* $\mathbb{Z}_2\mathbb{Z}_6$*. This exploration encompasses theoretical results and methodologies for establishing upper and lower limits on the covering radius. Section 3 shifts the focus to the construction of simplex codes of types* α*,* β*, and* γ *over the ring* $\mathbb{Z}_2\mathbb{Z}_6$*. Diverse methods and techniques for generating these simplex codes are investigated, with a potential discussion of specific code parameters. Section 4 focuses on examining the covering radius of simplex codes of types* α*,* β*, and* γ *over* $\mathbb{Z}_2\mathbb{Z}_6$*. The section investigates the covering radius properties of these codes, examining computational methods or bounds related to the covering radius. Furthermore, the intricate relationship between the covering radius and code parameters is studied. Sections 5 and 6 pivot towards the practical applications and security facets of the proposed simplex codes. Section 5 delves into a multi-secret sharing scheme anchored in* α*,* β*, and* γ*-linear simplex codes, unraveling the construction and properties of this cryptographic scheme. Simultaneously, Section 5 undertakes a meticulous security assessment of the multi-secret sharing scheme utilizing* α*,* β*, and* γ *linear simplex codes. This evaluation encompasses an analysis of the scheme's resilience against potential threats, examining its performance in the face of coalitions and security breaches. Collectively, these sections contribute to the theoretical underpinnings and practical applications of the studied codes, presenting a comprehensive exploration of their properties and utility.*

2 Context and Preliminaries

To establish a strong foundation for our study, we introduce key definitions, notations, and theoretical tools essential for understanding additive simplex codes over the ring $\mathbb{Z}_2\mathbb{Z}_6$*. This section overviews the relevant algebraic structures, weight functions, and properties necessary for the subsequent discussions.*

2.1 Additive Codes over $\mathbb{Z}_2\mathbb{Z}_6$

A code C *is defined as a* $\mathbb{Z}_2\mathbb{Z}_6$*-additive code when it forms a subgroup of* $\mathbb{Z}_2^{\gamma} \times \mathbb{Z}_6^{\delta}$*. In such a code, the first* γ *coordinates belong to* $\mathbb{Z}_2$*, while the remaining* δ *coordinates belong to* $\mathbb{Z}_6$*. By the structure theorem for finite abelian groups, any such additive code is isomorphic to:*

$$C \cong \mathbb{Z}_2^{m_1} \times \mathbb{Z}_2^{m_2} \times \mathbb{Z}_3^{m_3}, \tag{2.1}$$

where the parameters $(\gamma, \delta, m_1, m_2, m_3)$ *characterize the code.*

2.2 Weight Functions

Several weight functions play a significant role in studying additive codes over mixed alphabets. The Lee weight, Euclidean weight, and Chinese Euclidean weight are commonly used in $\mathbb{Z}_2\mathbb{Z}_6$ *coding theory. These weights are defined as follows:*

Definition 2.1. The **Lee**, **Euclidean**, and **Chinese Euclidean** weights of an element $x \in \mathbb{Z}_6$ are given by:

$x \in \mathbb{Z}_6$	$w_L(x)$	$w_E(x)$	$w_{CE}(x)$
0	0	0	0
1	1	1	1
2	2	4	2
3	3	9	4
4	2	4	2
5	1	1	1

Table 1. Lee, Euclidean, and Chinese Euclidean weights of elements in $\mathbb{Z}_6$.

Weight Functions in $\mathbb{Z}_2\mathbb{Z}_6$-Codes

In $\mathbb{Z}_2\mathbb{Z}_6$ coding theory, the following weight functions are commonly used:

- *The **Hamming weight** $w_H(c)$ counts the number of nonzero entries in a codeword $c \in \mathbb{Z}_2^\gamma \times \mathbb{Z}_6^\delta$.*
- *The **Lee weight** $w_L(c)$ is defined as:*

$$w_L(c) = w_H(x) + w_L(y), \tag{2.2}$$

  where $x \in \mathbb{Z}_2^\gamma$ and $y \in \mathbb{Z}_6^\delta$.
- *The **Euclidean weight** and **Chinese Euclidean weight** are derived from their respective norms and metric properties.*

For completeness, Table 2 provides explicit weight values for elements in $\mathbb{Z}_2 \times \mathbb{Z}_6$.

$c \in \mathbb{Z}_6$	$w_L(c)$	$w_E(c)$	$w_{CE}(c)$
00	0	0	0
01	1	1	1
02	2	4	3
03	3	9	4
04	2	4	3
05	1	1	1
10	1	1	1
11	2	2	2
12	3	5	4
13	4	10	5
14	3	5	4
15	2	2	2

Table 2. Weight values for elements in $\mathbb{Z}_2 \times \mathbb{Z}_6$.

Understanding these preliminaries is essential for analyzing the covering radii of simplex codes of types α, β, and γ. The subsequent sections leverage these weight functions to derive bounds and develop a multi-secret sharing scheme based on these codes.

2.3 The Gray Map and Gray Images on $\mathbb{Z}_2\mathbb{Z}_6$

*The **Gray map** is a fundamental tool in coding theory that transforms additive codes over $\mathbb{Z}_2\mathbb{Z}_6$ into ternary codes. This transformation enables the study of these codes using well-established techniques for ternary linear codes. Additionally, another significant mapping exists, which represents elements of $\mathbb{Z}_6$ in the direct sum $\mathbb{Z}_2\mathbb{Z}_3$. This alternative representation provides a different perspective on codes over $\mathbb{Z}_6$, offering further insights into their algebraic and combinatorial properties.*

Definition 2.2. The **Gray map** $\rho : \mathbb{Z}_2^{\gamma} \times \mathbb{Z}_6^{\delta} \to \mathbb{Z}_2^{\gamma+\delta} \times \mathbb{Z}_3^{\delta}$ is defined as:

$$\rho(x, y) = (x, \phi(y)),$$

where:

- $x = (x_1, x_2, \ldots, x_{\gamma}) \in \mathbb{Z}_2^{\gamma}$ remains unchanged.
- $y = (y_1, y_2, \ldots, y_{\delta}) \in \mathbb{Z}_6^{\delta}$ is mapped using the coordinate-wise application of the function $\phi : \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$ given by:

$$\phi(y_i) = \begin{cases} (0,0), & \text{if } y_i = 0, \\ (1,1), & \text{if } y_i = 1, \\ (0,2), & \text{if } y_i = 2, \\ (1,0), & \text{if } y_i = 3, \\ (0,1), & \text{if } y_i = 4, \\ (1,2), & \text{if } y_i = 5. \end{cases}$$

Thus, for a codeword $(x, y) \in \mathbb{Z}_2^{\gamma} \times \mathbb{Z}_6^{\delta}$, its **Gray image** $\rho(x, y)$ is given by:

$$\rho(x, y) = (x_1, x_2, \ldots, x_{\gamma}, \phi(y_1), \phi(y_2), \ldots, \phi(y_{\delta})).$$

2.4 Bounds on the Covering Radius

In this subsection, we will explore the upper and lower bounds on the covering radius of a code. The covering radius is a critical parameter in coding theory, as it quantifies the maximum distance between any codeword and its nearest neighbor outside the code. References [14] and [20] provide the covering radii of a code C over $\mathbb{Z}_2\mathbb{Z}_6$ concerning the Lee, Euclidean, and Chinese Euclidean distances, as follows:

$$r_D(C) = \max_{x \in \mathbb{Z}_2^{\gamma} \times \mathbb{Z}_6^{\delta}} \left\{ \min_{c \in C} d_L(x, c) \right\}, \tag{2.3}$$

and

$$\mathbb{Z}_2^{\gamma} \times \mathbb{Z}_6^{\delta} = \cup_{c \in C} S_{r_D}(c), \tag{2.4}$$

where $S_{r_D}(x) = \left\{ y \in \mathbb{Z}_2^{\gamma} \times \mathbb{Z}_6^{\delta}; d(x, y) \leq r_D \right\}$.

Definition 2.3. For a binary linear code C without a zero coordinate,$r_D(C) = \lfloor \frac{n(C)}{2} \rfloor$, where $n(C)$ is the length of the code C, which represents the number of coordinate positions in each codeword..

Proposition 2.4. *Let C be a code over $\mathbb{Z}_2^{\gamma} \times \mathbb{Z}_6^{\delta}$ and $\rho(C)$ be the Gray image of C, then $r_D(C) = r(\rho(C))$.*

Proof. Let C be a code over $\mathbb{Z}_2^{\gamma} \times \mathbb{Z}_6^{\delta}$ and let $\rho(C)$ denote its Gray image. The covering radius satisfies:

$$r_D(C) = r(\rho(C)). \tag{2.5}$$

This follows from the properties of the Gray map, which preserves distances in $\mathbb{Z}_2\mathbb{Z}_6$-additive codes. Since $\rho(C)$ is an isometric embedding of C, the maximal distance from any point in the space to the nearest codeword remains unchanged. □

The subsequent result proves to be valuable in determining the covering radius of codes over the ring $\mathbb{Z}_2\mathbb{Z}_6$.

Proposition 2.5. *If C_0 and C_1 are codes over $\mathbb{Z}_2\mathbb{Z}_6$ has length n_0 and n_1, of minimum distance d_0 and d_1, generated by: matrices G_0 and G_1, respectively, and if C is the code generated by*

$$G = \left[\begin{array}{c|c} 0 & G_1 \\ \hline G_0 & A \end{array} \right],$$

then $r_d(C) \leq r_d(C_0) + r_d(C_1)$*, and the covering radius of the concatenation of* C_0 *and* C_1*, denoted* C_c*, satisfies the following*

$$r_d(C_c) \geq r_d(C_0) + r_d(C_1)$$

for all distances d *over* $\mathbb{Z}_2\mathbb{Z}_6$*.*

Proof. Consider two codes C_0 and C_1 over $\mathbb{Z}_2^\gamma \times \mathbb{Z}_6^\delta$ of lengths n_0 and n_1 with minimum distances d_0 and d_1, generated by matrices G_0 and G_1. If C is the concatenation of C_0 and C_1 generated by:

$$G = \begin{bmatrix} 0 & G_1 \\ G_0 & A \end{bmatrix}, \tag{2.6}$$

where A is an additional structure matrix ensuring proper concatenation.

Let $x \in \mathbb{Z}_2^\gamma \times \mathbb{Z}_6^\delta$ be any element. Since C_0 and C_1 are subcodes, we can split x into two parts x_0 and x_1 corresponding to their respective coordinates. The minimal distance from x to C is given by:

$$d_L(x, C) = \min_{c \in C} d_L(x, c). \tag{2.7}$$

Since each codeword in C is a concatenation of codewords from C_0 and C_1, we can bound the distance component-wise:

$$d_L(x, C) \leq d_L(x_0, C_0) + d_L(x_1, C_1). \tag{2.8}$$

Taking the maximum over all x yields the desired bound:

$$r_D(C) \leq r_D(C_0) + r_D(C_1). \tag{2.9}$$

This completes the proof. □

This section introduced the algebraic structure of $\mathbb{Z}_2\mathbb{Z}_6$*-additive codes, essential weight functions, and their role in coding theory. The subsequent sections will build upon these foundations to explore the applications of simplex codes, covering the radii of these codes and multi-secret sharing schemes based on Gray images of these codes.*

3 Simplex Codes of Types α, β, and γ over $\mathbb{Z}_2\mathbb{Z}_6$

Our attention now turns to the three types of simplex codes: α, β*, and* γ*. Each type corresponds to a unique set of basis vectors, resulting in distinct codes. We use linear combinations to generate all possible codewords and carefully select suitable basis vectors for these codes.*

Definition 3.1. We define the generator matrix of S_k^α, the simplex code of type α over $\mathbb{Z}_2\mathbb{Z}_6$, as the concatenation of 6^k copies of the generator matrix of $S_{2,k}^\alpha$ and 2^k copies of the generator matrix of $S_{6,k}^\alpha$, given by:

$$\Theta_k^\alpha = \left[\ 1_{6^k} \otimes m_{2,k}^\alpha \ \middle|\ 1_{2^k} \otimes G_{6,k}^\alpha\ \right], \quad \text{for } k \geq 1. \tag{3.1}$$

Where $\Theta_1^\alpha = \begin{bmatrix} 00 & 01 & 02 & 03 & 04 & 05 & 10 & 11 & 12 & 13 & 14 & 15 \end{bmatrix}$. $m_{2,k}^\alpha$ is the generator matrix of $S_{2,k}^\alpha$, the binary simplex code of type α, and $G_{6,k}^\alpha$ is the generator matrix of $S_{2,k}^\alpha$, the senary simplex code of type α.

The length of the simplex code of type α *over* $\mathbb{Z}_2\mathbb{Z}_6$ *is given by* $3^k \cdot 2^{2k+1}$*, and the total number of codewords is expressed as* $2^{k_0}6^{k_1}$ *for some values of* k_0 *and* k_1*. For the specific instance when* $k = 1$ *with* $k_0 = 0$ *and* $k_1 = 1$*, all codewords of the simplex codes* S_1^α *are as follows:*

00	00	00	00	00	00	00	00	00	00	00	00
00	01	02	03	04	05	10	11	12	13	14	15
00	02	04	00	02	04	00	02	04	00	02	04
00	03	00	03	00	03	10	13	10	13	10	13
00	04	02	00	04	02	00	04	02	00	04	02
00	05	04	03	02	01	10	15	14	13	12	11.

The simplex codes denoted as S_k^{β} over $\mathbb{Z}_2\mathbb{Z}_6$ can be considered as a punctured variation of S_k^{α}. These codes consist of a total of $2^{k_0}6^{k_1}$ codewords, with a length of $\frac{(2^k-1)^2(3^k-1)^2}{2}$.

Definition 3.2. To construct the generator matrix of S_k^{β}, we concatenate $\frac{(2^k-1)(3^k-1)}{2}$ copies of the generator matrix from the binary simplex code $S_{2,k}^{\beta}$ and (2^k-1) copies of the generator matrix from the simplex code $S_{6,k}^{\beta}$ over $\mathbb{Z}_6$.

$$\Theta_k^{\beta} = \left[\ 1_{\frac{(2^k-1)(3^k-1)}{2}} \otimes m_{2,k}^{\beta} \ \middle|\ 1_{2^k-1} \otimes G_{6,k}^{\beta}\ \right],\ for \geq 2, \tag{3.2}$$

where $m_{2,k}^{\beta}$ is the generator matrix of the binary simplex code of type β and $G_{6,k}^{\beta}$ is a generator matrix of the simplex code $S_{6,k}^{\beta}$ over $\mathbb{Z}_6$ of type β defined as, for $k \geq 2$,

$$G_{6,k}^{\beta} = \left[\begin{array}{c|c|c|c} 11\cdots1 & 00\cdots0 & 22\cdots2 & 33\cdots3 \\ \hline G_{6,k-1}^{\alpha} & G_{6,k-1}^{\beta} & \Lambda_{k-1} & \mu_{k-1} \end{array}\right] \tag{3.3}$$

where Λ_k is a $k \times 3^k(2^k-1)$ matrix defined inductively by $\Lambda_1 = [135]$ and

$$\Lambda_k = \left[\begin{array}{c|c|c|c|c|c} 00\cdots0 & 11\cdots1 & 22\cdots2 & 33\cdots3 & 33\cdots3 & 33\cdots3 \\ \hline \Lambda_{k-1} & G_{6,k-1}^{\alpha} & \Lambda_{k-1} & G_{6,k-1}^{\alpha} & \Lambda_{k-1} & G_{6,k-1}^{\alpha} \end{array}\right], \tag{3.4}$$

for $k \geq 2$, and μ_k is a $k \times 2^{k-1} \cdot (3^k-1)$ matrix defined inductively by: $\mu_1 = [12]$ and

$$\mu_k = \left[\begin{array}{c|c|c|c} 00\cdots0 & 11\cdots1 & 22\cdots2 & 33\cdots3 \\ \hline \mu_{k-1} & G_{6,k-1}^{\alpha} & G_{6,k-1}^{\alpha} & \mu_{k-1} \end{array}\right], \tag{3.5}$$

for $k \geq 2$, where $G_{6,k-1}^{\alpha}$ is the generator matrix of $S_{6,k-1}^{\alpha}$.

In the following we define the simplex code S_k^{γ} of type γ over $\mathbb{Z}_2\mathbb{Z}_6$.
As in [19], let $G_{6,k}^{\gamma}$ be the $k \times 2^{k-1}(3^k-2^k)$ matrix defined inductively by:

$$G_{6,2}^{\gamma} = \left[\begin{array}{c|c|c|c|c} 111111 & 0 & 2 & 3 & 4 \\ \hline 012345 & 1 & 1 & 1 & 1 \end{array}\right]. \tag{3.6}$$

And for $k > 2$

$$G_{6,k}^{\gamma} = \left[\begin{array}{c|c|c|c|c} 11\cdots1 & 00\cdots0 & 22\ldots2 & 33\cdots3 & 44\cdots4 \\ \hline G_{6,k-1}^{\alpha} & G_{6,k-1}^{\gamma} & G_{6,k-1}^{\gamma} & G_{6,k-1}^{\gamma} & G_{6,k-1}^{\gamma} \end{array}\right]. \tag{3.7}$$

Note that $G_{6,k}^{\gamma}$ is obtained from $G_{6,k}^{\alpha}$ by deleting $2^{k-1}(2^k+3^k)$ columns. By induction it is easy to verify that no two columns of $G_{6,k}^{\gamma}$ are multiples of each other. Let $S_{6,k}^{\gamma}$ be the code of type γ over $\mathbb{Z}_6$ generated by $G_{6,k}^{\gamma}$. Note that the length of $S_{6,k}^{\gamma}$ is $2^{k-1}(2^k-3^k)$.

Definition 3.3. The generator matrix of the simplex code S_k^{γ} over $\mathbb{Z}_2\mathbb{Z}_6$ is the concatenation of $2^{k-1}(2^k-3^k)$ copies of the generator matrix of $S_{2,k}^{\alpha}$ and 2^k copies of the generator matrix of $S_{6,k}^{\gamma}$ given by:

$$\Theta_k^{\gamma} = \left[\ 1_{2^{k-1}(2^k-3^k} \otimes m_{2,k}^{\alpha} \ \middle|\ 1_{2^k} \otimes G_{6,k}^{\gamma}\ \right],$$

for $k \geq 2$ where $m_{2,k}^{\alpha} = \left[\begin{array}{c|c} 00\cdots0 & 11\cdots1 \\ \hline m_{2,k-1}^{\alpha} & m_{2,k-1}^{\alpha} \end{array}\right]$, for $k \geq 2$, where $m_{2,1}^{\alpha} = [0,1]$.

Note that the length of the simplex code S_k^{γ} over $\mathbb{Z}_2\mathbb{Z}_6$ of type γ is $2^{2k}(3^k-2^k)$.

4 The Covering Radius of Simplex Codes of Types α, β and γ

This section investigates how to determine the covering radius for specific codes, which requires a thorough understanding of the covering radius of repetition codes. The references [12, 16, 19] provide valuable insights into this topic, serving as foundational resources for determining the covering radius of simplex codes of types α, β, and γ. The covering radius $r(S_k^\iota)$, $\iota \in \{\alpha,\beta,\gamma\}$ of a code S_k^ι, $\iota \in \{\alpha,\beta,\gamma\}$ is defined as the maximum Hamming distance from any vector in the ambient space to the nearest codeword in S_k^ι, $\iota \in \{\alpha,\beta,\gamma\}$. Mathematically, it is expressed as:

$$r(S_k^\iota) = \max_{x\in\mathbb{Z}_2^\gamma\times\mathbb{Z}_6^\delta} \min_{c\in S_k^\iota} d(x,c), \iota \in \{\alpha,\beta,\gamma\} \tag{4.1}$$

where $d(x,c)$ denotes the Hamming distance between x and c. This measure is crucial for understanding how well the code covers the space and its error correction capability. The covering radius offers a numerical evaluation of the worst-case for error correction, as it determines the farthest point from the codewords that still falls in the code's correcting ability. Studying the covering radius helps in designing efficient error-correcting codes and optimizing their performance in practical applications. Furthermore, for specific classes of simplex codes, deriving precise values of the covering radius requires an in-depth analysis of their structure and properties, which can be affected using combinatorial and algebraic techniques. This investigation is fundamental to enhancing the robustness of coding schemes in digital communication and data storage systems.

Theorem 4.1. *The covering radii of the $\mathbb{Z}_2\mathbb{Z}_6$-simplex codes of type α are given by:*

1. $r_L(S_k^\alpha) \le 2^k\left(27\times 6^{k-1}-4\right)$,
2. $2^k\left(11\times 6^k-16\right) \le r_E(S_k^\alpha) \le 2^{k-1}\left(55\times 6^k-54\right)$,
3. $r_{CE}(S_k^\alpha) \le 2^{k-1}\left(5\times 6^k-4\right)$.

Proof. According to [12, 16, 19], from Definition 2.3 and Proposition 2.5 the the covering radius $r_L(S_k^\alpha), r_E(S_k^\alpha)$ and $r_{CE}(S_k^\alpha)$ are given by:

1. Concerning the code S_k^α and its correlation with the Lee weight, we possess the following information

$$\begin{aligned}
r_L(S_k^\alpha) &\le r_L(6^k S_{2,k}^\alpha) + r_L(2^k S_{6,k}^\alpha)\\
&\le 6^k r_L(S_{2,k}^\alpha) + 2^k r_L(S_{6,k}^\alpha)\\
&\le 6^k r_H(S_{2,k}^\alpha) + 2^k r_L(S_{6,k}^\alpha)\\
&\le 6^k\left(2^{k-1}\right) + 2^k\left(5\times 9\times 6^{k-1} + 5\times 9\times 6^{k-2} + \ldots + 5\times 9\times 6^0\right)\\
&\le 6^k\left(2^{k-1}\right) + 2^{k+2}\left(6^k-1\right)\\
&\le 2^k\left(27\times 6^{k-1}-4\right).
\end{aligned}$$

2. In relation to the code S_k^α and its connection to the Euclidean weight, we can state the following

$$\begin{aligned}
r_E(S_k^\alpha) &\ge 6^k\left(2^{k-1}\right) + 16\times 2^k(6^k-1)\\
&\ge 2^k\left(11\times 6^k-16\right).
\end{aligned}$$

On the other hand,

$$\begin{aligned}
r_E(S_k^\alpha) &\le 6^k\left(2^{k-1}\right) + 3^3\times 2^k(6^k-1)\\
&\le 2^{k-1}\left(55\times 6^k-54\right).
\end{aligned}$$

3. Regarding the code S_k^{α} and its association with the Chinese Euclidean weight, we have the following information

$$\begin{aligned} r_{CE}(S_k^{\alpha}) &\leq r_{CE}(6^k S_{2,k}^{\alpha}) + r_{CE}(2^k S_{6,k}^{\alpha}) \\ &\leq 6^k r_{CE}(S_{2,k}^{\alpha}) + 2^k r_{CE}(S_{6,k}^{\alpha}) \\ &\leq 6^k r_H(S_{2,k}^{\alpha}) + 2^k r_{CE}(S_{6,k}^{\alpha}) \\ &\leq 6^k \left(2^{k-1}\right) + 2 \times 2^k \left(6^k - 1\right) \\ &\leq 2^{k-1}\left(5 \times 6^k - 4\right). \end{aligned}$$

□

The forthcoming theorem provides a detailed analysis of the covering radius concerning $\mathbb{Z}_2\mathbb{Z}_6$-simplex codes of type β.

Theorem 4.2. *The given expression defines the covering radius for the $\mathbb{Z}_2\mathbb{Z}_6$-simplex codes of type β as follows:*

(1) $r_L(S_k^{\beta}) \leq \left(\frac{2^k - 1}{4}\right)\left[4 \times 2^k \left(3^k - 4\right) - 3^k + 12\right]$,

(2) $r_E(S_k^{\beta}) \leq \left(\frac{2^k - 1}{4}\right)\left[4 \times 2^k \left(4 \times 3^k - 11\right) - 3^k + 46\right]$,

(3) $r_{CE}(S_k^{\beta}) \leq \left(\frac{2^k - 1}{4}\right)\left[2^k \left(5 \times 3^k - 21\right) - 3^k + 16\right]$.

Proof. 1. Regarding the code S_k^{β} and its association with the Lee weight, we have

$$\begin{aligned} r_L(S_k^{\beta}) &\leq r_L\left(\frac{(2^k-1)(3^k-1)}{2} S_{2,k}^{\beta}\right) + r_L\left((2^k-1)S_{6,k}^{\beta}\right) \\ &\leq \frac{(2^k-1)(3^k-1)}{2} r_L(S_{2,k}^{\beta}) + (2^k-1) r_L(S_{6,k}^{\beta}) \\ &\leq \frac{(2^k-1)(3^k-1)}{2} r_H(S_{2,k}^{\beta}) + (2^k-1) r_L(S_{6,k}^{\beta}) \\ &\leq \frac{(2^k-1)^2(3^k-1)}{4} + \frac{15}{4}(2^k-1)\left[\left(\frac{6^k-1}{5}\right) - 2^k + 1\right] \\ &\leq \left(\frac{2^k-1}{4}\right)\left[4 \times 2^k \left(3^k - 4\right) - 3^k + 12\right]. \end{aligned}$$

2. For the code S_k^{β} with respect to the Euclidean weight, we have

$$\begin{aligned} r_E(S_k^{\beta}) &\leq r_E\left(\frac{(2^k-1)(3^k-1)}{2} S_{2,k}^{\beta}\right) + r_E\left((2^k-1)S_{6,k}^{\beta}\right) \\ &\leq \frac{(2^k-1)(3^k-1)}{2} r_E(S_{2,k}^{\beta}) + (2^k-1) r_E(S_{6,k}^{\beta}) \\ &\leq \frac{(2^k-1)(3^k-1)}{2} r_H(S_{2,k}^{\beta}) + (2^k-1) r_E(S_{6,k}^{\beta}) \\ &\leq \frac{(2^k-1)^2(3^k-1)}{4} + \frac{45}{4}(2^k-1)\left[\left(\frac{6^k-1}{5}\right) - 2^k + 1\right] \\ &\leq \left(\frac{2^k-1}{4}\right)\left[4 \times 2^k \left(4 \times 3^k - 11\right) - 3^k + 46\right]. \end{aligned}$$

3. For the code S_k^{β} with respect to the Chinese Euclidean weight, we have

$$\begin{aligned} r_{CE}(S_k^{\beta}) &\leq r_{CE}\left(\frac{(2^k-1)(3^k-1)}{2}S_{2,k}^{\beta}\right) + r_{CE}\left((2^k-1)S_{6,k}^{\beta}\right) \\ &\leq \frac{(2^k-1)(3^k-1)}{2} r_{CE}(S_{2,k}^{\beta}) + (2^k-1) r_{CE}(S_{6,k}^{\beta}) \\ &\leq \frac{(2^k-1)(3^k-1)}{2} r_H(S_{2,k}^{\beta}) + (2^k-1) r_{CE}(S_{6,k}^{\beta}) \\ &\leq \frac{(2^k-1)^2(3^k-1)}{4} + 5(2^k-1)\left[\left(\frac{6^k-1}{5}\right) - 2^k + 1\right] \\ &\leq \left(\frac{2^k-1}{4}\right)\left[2^k\left(5\times 3^k - 21\right) - 3^k + 16\right]. \end{aligned}$$

□

Theorem 4.3. *The simplex codes of types γ are characterized by their covering radius, which is defined as:*

(1) $r_L(S_k^{\gamma}) \leq \frac{2^{k-1}}{5}\left(\frac{69}{5}6^{k-1} - 75\times 2^{2(k-1)} - \frac{54}{5}\right)$,

(2) $r_E(S_k^{\gamma}) \leq 2^{k-1}\left[\frac{33}{5}6^{k-1} - 2^k\left(2^{k-1}+4\right) + \frac{38}{5}\right]$,

(3) $r_{CE}(S_k^{\gamma}) \leq 2^{k+2}\left(\frac{10}{3}3^{2k} - 5\times 3^k\right) - 3^k\left(\frac{2^{2k+2}}{3} - 32\right)$.

Proof. 1. Concerning the code S_k^{γ} and its relationship with the Lee weight, we observe that

$$\begin{aligned} r_L(S_k^{\gamma}) &\leq r_L(2^{k-1}\left(3^k-2^k\right)S_{3,k}^{\gamma}) + r_L(2^k S_{6,k}^{\gamma}) \\ &\leq 2^{k-1}\left(3^k-2^k\right) r_L(S_{3,k}^{\gamma}) + 2^k r_L(S_{6,k}^{\gamma}) \\ &\leq 2^{k-1}\left(3^k-2^k\right) r_H(S_{3,k}^{\gamma}) + 2^k r_L(S_{6,k}^{\gamma}) \\ &\leq 2^{k-1}\times 2^{k-1}\left(3^k-2^k\right) + 2^k\left[\frac{27}{5}\left(6^{k-1}-1\right) - 14\left(2^{2k-2}\right)\right] \\ &\leq \frac{2^{k-1}}{5}\left(\frac{69}{5}6^{k-1} - 75\times 2^{2(k-1)} - \frac{54}{5}\right). \end{aligned}$$

2. In the context of the code S_k^{γ} and its association with the Euclidean weight, it can be observed that

$$\begin{aligned} r_E(S_k^{\gamma}) &\leq r_E(2^{k-1}\left(3^k-2^k\right)S_{3,k}^{\gamma}) + r_E(2^k S_{6,k}^{\gamma}) \\ &\leq 2^{k-1}\left(3^k-2^k\right) r_E(S_{3,k}^{\gamma}) + 2^k r_E(S_{6,k}^{\gamma}) \\ &\leq 2^{k-1}\left(3^k-2^k\right) r_H(S_{3,k}^{\gamma}) + 2^k r_E(S_{6,k}^{\gamma}) \\ &\leq 2^{k-1}\times 2^{k-1}\left(3^k-2^k\right) + 2^k\left[36\left(\frac{6^{k-1}-1}{5}\right) - 4\left(2^{k-1}-1\right)\right] \\ &\leq 2^{k-1}\left[\frac{33}{5}6^{k-1} - 2^k\left(2^{k-1}+4\right) + \frac{38}{5}\right]. \end{aligned}$$

3. For the code S_k^γ with respect to the Chinese Euclidean weight, we have

$$\begin{aligned} r_{CE}(S_k^\gamma) &\leq r_{CE}(2^{k-1}\left(3^k-2^k\right)S_{3,k}^\gamma)+r_{CE}(2\times 3^k S_{6,k}^\gamma) \\ &\leq 2^{k-1}\left(3^k-2^k\right)r_{CE}(S_{3,k}^\gamma)+2\times 3^k r_{CE}(S_{6,k}^\gamma) \\ &\leq 2^{k-1}\left(3^k-2^k\right)r_H(S_{3,k}^\gamma)+2\times 3^k r_{CE}(S_{6,k}^\gamma) \\ &\leq 2^{k-1}\times 2^{k-1}\left(3^k-2^k\right)+5\times 2^k\left[36\left(\frac{6^{k-1}-1}{5}\right)-4\left(2^{k-1}-1\right)\right] \\ &\leq 2^{k-1}\left[5\times 6^{k-1}-2^k\left(2^{k-1}+20\right)+38\right]. \end{aligned}$$

□

5 Multi-Secret Sharing Scheme Based on α, β and γ-Linear Simplex Codes

In this section, we focus on a multi-secret sharing scheme based on linear codes, specifically using Blakley's method as detailed by Alahmadi et al [2]. This approach is designed to securely distribute multiple secrets through the use of codes over a finite field, namely $\mathbb{Z}_6$, which is the set of integers modulo 6. The purpose and applications of this multi-secret sharing scheme are as follows:

5.1 Purpose of Multi-Secret Sharing

The main objective of a multi-secret sharing scheme is to safeguard several secrets concurrently, ensuring that no individual party or entity can independently access all the secrets. Each secret is partitioned into shares and then allocated to the participants. This method ensures that only a designated group of participants, referred to as a coalition, can reconstruct the secrets. Such an approach proves particularly advantageous in cases where regulation confidentiality and access control across multiple pieces of sensitive information is required.

5.2 Applications of Multi-Secret Sharing

- ***Security and Privacy:*** *Multi-secret sharing is essential in settings where the protection of multiple pieces of sensitive data is required.*
- ***Blockchain and Distributed Systems:*** *In decentralized systems, such as blockchain, multi-secret sharing can be applied to distribute control over multiple private keys or critical system parameters without relying on a single party.*
- ***Cloud Storage:*** *When storing encrypted secrets across various cloud servers, multi-secret sharing ensures that no single server can access the entire data. This enhances security and prevents data breaches by distributing shares across different locations.*
- ***Collaborative Projects:*** *For collaborative work involving sensitive data, a multi-secret sharing scheme allows multiple parties to collaborate on different aspects of a project without exposing the entire dataset, thus maintaining privacy.*

In essence, this scheme combines the power of linear codes with secret sharing, providing security and efficient recovery of secrets under controlled conditions. The advantage is its ability to handle multiple secrets simultaneously, which is ideal for complex applications requiring high levels of confidentiality and distributed control.

Let $\overline{S_k^\alpha}$, $\overline{S_k^\beta}$, and $\overline{S_k^\gamma}$ be subcodes of S_k^α, S_k^β, and S_k^γ over $\mathbb{Z}_6$, with generator matrices $\overline{\Theta_k^\alpha}$, $\overline{\Theta_k^\beta}$, and $\overline{\Theta_k^\gamma}$, respectively. This method builds upon the foundations established in [2], providing a solid framework for secret sharing using linear codes.

- *The secret distribution takes place in the secret space denoted as $\mathbb{Z}_6^n$, where a given codeword represents the secret $s=(s_1,s_2,\ldots,s_n)$. The dealer, who knows the secret s, computes the share ϖ of the user with the attached codeword c by taking the scalar product: $\varpi=h_c(s)=c\cdot s^t$ where, t denotes transposition.*

- *Secret recovery involves considering a system with the private secret* s *and the coalition corresponding to the rows of* $\overline{\Theta_k^\iota}$*, where* $\iota \in \{\alpha, \beta, \gamma\}$*. The system of equations is given by:*

$$\overline{\Theta_k^\iota} \cdot s^t = \varpi^t, \tag{5.1}$$

where $\iota \in \{\alpha, \beta, \gamma\}$*,* $\varpi = (\varpi_1, \varpi_2, \ldots, \varpi_k)$*, and* ϖ_i *is the share attached to the* i*-th row of* $\overline{\Theta_k^\iota}$*,* $\iota \in \{\alpha, \beta, \gamma\}$*.*

In this context, the set of solutions forms an affine space with the associated vector space $(S_k^\iota)^\perp$*, where* $\iota \in \{\alpha, \beta, \gamma\}$*. Assuming that* S_k^ι*,* $\iota \in \{\alpha, \beta, \gamma\}$*, is a Linearly Complementary Dual (LCD) code, we recall that an* ***LCD code*** *is a linear code whose intersection with its dual code is trivial. Specifically, if* S_k^ι*,* $\iota \in \{\alpha, \beta, \gamma\}$*, is a linear code of length* n *over a finite field* $\mathbb{Z}_6$*, it is classified as an LCD code if* $S_k^\iota \cap (S_k^\iota)^\perp = \{0\}$*, where* $\iota \in \{\alpha, \beta, \gamma\}$*. Additionally, we have:*

$$rank\left(\overline{\Theta_k^\iota}\right) = rank\left(\overline{\Theta_k^\iota}\right)\left(\overline{\Theta_k^\iota}\right)^\perp = rank\left(\overline{\Theta_k^\iota}\right)^\perp\left(\overline{\Theta_k^\iota}\right) \neq 0, \iota \in \{\alpha, \beta, \gamma\}, \tag{5.2}$$

the system admits a unique solution in $\mathcal{C}$*. Solving the following linear system can compute the secret.*

$$\begin{cases} \overline{\Theta_k^\iota} \cdot s^t = \varpi^t, & \iota \in \{\alpha, \beta, \gamma\} \\ H(\overline{\Theta_k^\iota}) \cdot s^t = 0, & \iota \in \{\alpha, \beta, \gamma\}, \end{cases} \tag{5.3}$$

where $H(\overline{\Theta_k^\iota})$ *is the parity-check matrix of* $\overline{\Theta_k^\iota}$*,* $\iota \in \{\alpha, \beta, \gamma\}$*. The parity-check matrix* $H(\overline{\Theta_k^\iota})$ *defines the constraints that a valid codeword must satisfy. It plays a fundamental role in error detection and correction by ensuring that any received vector can be verified against the code structure. The construction of* $H(\overline{\Theta_k^\iota})$*,* $\iota \in \{\alpha, \beta, \gamma\}$ *guarantees that each codeword in the code* S_k^ι*,* $\iota \in \{\alpha, \beta, \gamma\}$ *satisfies the condition* $H(\overline{\Theta_k^\iota})x^T = 0$*, where* x *represents a codeword. This property ensures that all valid codewords lie in the null space of* $H(\overline{\Theta_k^\iota})$*. Furthermore, the syndrome calculation, given by* $s = H(\overline{\Theta_k^\iota})r^T$ *for a received vector* r*, is crucial for identifying errors. If the syndrome* s *is nonzero, it indicates the presence of errors, which can then be located and corrected using appropriate decoding algorithms.*

5.3 Characteristics of the Scheme and Data Regarding Coalitions

The features of the proposed scheme emphasize its robustness and efficiency in multi-secret sharing. The scheme's use of linear codes and Blakley's method ensures secure information distribution. Significantly, an $[n, k, d_H]$*-linear code* $\overline{S_k^\iota}$*,* $\iota \in \{\alpha, \beta, \gamma\}$ *parameters, offer valuable insight into its error detection and correction potential. Additionally, information about possible coalitions is crucial for assessing the security scheme.*

Theorem 5.1. *We obtain the following information in this multi-secret sharing scheme:*

(i) The access structure forms the k*-tuple of codewords that are linearly independent.*

(ii) The number of elements recovering the secret is at least k*.*

Proof. To establish the theorem, we analyze the structure of the multi-secret sharing scheme based on linear codes.

(i) The access structure forms the k**-tuple of linearly independent codewords:**

- The secret sharing scheme is constructed using an $[n, k, d_H]$-linear code $\overline{S_k^\iota}$, $\iota \in \{\alpha, \beta, \gamma\}$ over Z_6, where $\overline{S_k^\iota}$ is a subcode of a simplex code of type α, β, or γ.
- The generator matrix $\overline{\Theta_k^\iota}$ (where $\iota \in \{\alpha, \beta, \gamma\}$) defines the shares assigned to the participants.
- Each participant receives a share computed as $s_i = c_i \cdot s^T$, where c_i is a row of $\overline{\Theta_k^\iota}$ and s is the secret vector.
- Since the generator matrix consists of k linearly independent rows, the shares also form a k-tuple of linearly independent codewords.

(ii) The number of elements required to recover the secret is at least k:

- The secret reconstruction process involves solving the linear system:

$$\overline{\Theta_k^\iota} \cdot s^T = \varpi^T.$$

- The system has a unique solution if and only if the rank of $\overline{\Theta_k^\iota}$ is k.
- If fewer than k participants attempt to recover the secret, the system becomes underdetermined, leading to multiple possible solutions.
- Therefore, at least k shares are necessary to uniquely determine the secret s.

Hence, claims (i) and (ii) are established, and the proof is complete. □

Theorem 5.2. *Let $\overline{S_k^\iota}$, $\iota \in \{\alpha, \beta, \gamma\}$ be an a code over $\mathbb{Z}_6$ with generator matrix $\overline{\Theta_k^\iota}$, $\iota \in \{\alpha, \beta, \gamma\}$. In a multi-secret-sharing scheme based on $\mathcal{C}$, the number of minimal coalitions is given by:*

$$\frac{6^k \prod_{j=0}^{k-1} (6^k - 6^j)}{k!}. \tag{5.4}$$

Proof. To determine the number of minimal coalitions, we analyze the structure of the multi-secret-sharing scheme based on the linear code $\overline{S_k^\iota}$, $\iota \in \{\alpha, \beta, \gamma\}$ over $\mathbb{Z}_6$.

Step 1: Understanding the Coalition Structure

- The secret-sharing scheme distributes the secret across participants using a generator matrix $\overline{\Theta_k^\iota}$, $\iota \in \{\alpha, \beta, \gamma\}$.
- A coalition refers to a subset of participants who can collectively reconstruct the secret.
- Minimal coalitions are those subsets of participants that can reconstruct the secret but would fail if any member were removed.

Step 2: Counting the Number of Minimal Coalitions

- The generator matrix $\overline{\Theta_k^\iota}$, $\iota \in \{\alpha, \beta, \gamma\}$ has k linearly independent rows, ensuring that at least k shares are needed to recover the secret.
- Each coalition of size k must correspond to a selection of k rows that form a basis of the secret space.
- Since there are 6^k possible values for each row component in $\mathbb{Z}_6$, the total number of distinct choices of k rows is computed as:

$$6^k \times (6k - 6(k-1)) \times \cdots \times (6k - 6 \cdot 1).$$

- Since the order of selection does not matter, we divide by $k!$ to eliminate duplicate orderings:

$$\frac{6^k}{k!} \prod_{j=0}^{k-1} (6k - 6j).$$

Thus, we establish the formula for the number of minimal coalitions, concluding the proof. □

5.4 Examples

The computations presented in these examples were performed using computational algebra systems, which facilitate efficient symbolic and numerical calculations. In particular

- ***SageMath**: Used for matrix operations, weight distributions, and code construction (https://www.sagemath.org/)*

- ***MAGMA**: Applied for verification of linear code properties and secret-sharing scheme calculations (`http://magma.maths.usyd.edu.au/`).*

Example 5.3. For $k = 2$, the generator matrix of $\overline{S_2^\alpha}$ is given by:

$$\overline{\Theta_2^\alpha} = \begin{bmatrix} 10111111222222333333444444555555 \\ 01012345012345012345012345012345 \end{bmatrix}. \tag{5.5}$$

Following Equation 5.2, we have

$$\left(\overline{\Theta_2^\alpha}\right) = \left(\overline{\Theta_2^\alpha}\right)\left(\overline{\Theta_2^\alpha}\right)^\perp = \left(\overline{\Theta_2^\alpha}\right)^\perp\left(\overline{\Theta_2^\alpha}\right) = 2 \neq 0. \tag{5.6}$$

If $s = (55543210432105321054210543105432) \in \overline{S_2^\alpha}$, we verify a multi-secret-sharing scheme utilizing Equation 5.1. This involves calculating the shares based on $\overline{S_2^\alpha}$ as outlined below:

$$\varpi = (23), \tag{5.7}$$

let $s = (s_1 s_2 s_3 s_4 s_5 s_6 s_7 s_8 s_9 s_{10} s_{11} s_{12} s_{13} s_{14} s_{15} s_{16} s_{17} s_{18} s_{19} s_{20} s_{21} s_{22} s_{23} s_{24} s_{25} s_{26} s_{27} s_{28} s_{29} s_{30} s_{31} s_{32}) \in \overline{S_2^\alpha}$ represent the secret. Upon examining the system of equations specified in Equation 5.3, we obtain:

$$\begin{pmatrix} 10111111222222333333444444555555 \\ 01012345012345012345012345012345 \\ 10000000000000000000000000000052 \\ 01000000000000000000000000000015 \\ 00100000000000000000000000000052 \\ 00010000000000000000000000000001 \\ 00001000000000000000000000000010 \\ 00000100000000000000000000000025 \\ 00000010000000000000000000000034 \\ 00000001000000000000000000000043 \\ 00000000100000000000000000000044 \\ 00000000010000000000000000000053 \\ 00000000001000000000000000000002 \\ 00000000000100000000000000000011 \\ 00000000000010000000000000000020 \\ 00000000000001000000000000000035 \\ 00000000000000100000000000000030 \\ 00000000000000010000000000000045 \\ 00000000000000001000000000000054 \\ 00000000000000000100000000000003 \\ 00000000000000000010000000000012 \\ 00000000000000000001000000000021 \\ 00000000000000000000100000000022 \\ 00000000000000000000010000000031 \\ 00000000000000000000001000000040 \\ 00000000000000000000000100000055 \\ 00000000000000000000000010000004 \\ 00000000000000000000000001000013 \\ 00000000000000000000000000100014 \\ 00000000000000000000000000010023 \\ 00000000000000000000000000001032 \\ 00000000000000000000000000000141 \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \\ s_5 \\ s_6 \\ s_7 \\ s_8 \\ s_9 \\ s_{10} \\ s_{11} \\ s_{12} \\ s_{13} \\ s_{14} \\ s_{15} \\ s_{16} \\ s_{17} \\ s_{18} \\ s_{19} \\ s_{20} \\ s_{21} \\ s_{22} \\ s_{23} \\ s_{24} \\ s_{25} \\ s_{26} \\ s_{27} \\ s_{28} \\ s_{29} \\ s_{30} \\ s_{31} \\ s_{32} \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \tag{5.8}$$

A unique solution exists for the system of equations, and its determination yields

$$s = (55543210432105321054210543105432).$$

Furthermore, the number of minimal coalitions is 18900.

Example 5.4. For $k = 3$, the generator matrix for $\overline{S_3^\beta}$ is represented as:

$$\overline{\Theta_3^\gamma} = \begin{bmatrix} 110000000000222222222233333333334444444444 \\ 051111110234111111023411111102341111110234 \\ 550123451111012345111101234511110123451111 \end{bmatrix}. \tag{5.9}$$

Following Equation 5.2, it can be observed that

$$\left(\overline{\Theta_3^\gamma}\right) = \left(\overline{\Theta_3^\gamma}\right)\left(\overline{\Theta_3^\gamma}\right)^\perp = \left(\overline{\Theta_3^\gamma}\right)^\perp\left(\overline{\Theta_3^\gamma}\right) = 3 \neq 0. \tag{5.10}$$

If $s = (404321055153432105515310543224204321055153) \in \overline{S_3^\gamma}$, we verify a multi-secret-sharing scheme using Equation 5.1. This procedure involves calculating the shares derived from $\overline{S_3^\gamma}$ as outlined below:

$$\varpi = (153), \tag{5.11}$$

Consider the secret

$$s = (s_1 s_2 s_3 s_4 s_5 s_6 s_7 s_8 s_9 s_{10} s_{11} s_{12} s_{13} s_{14} s_{15} s_{16} s_{17} s_{18} s_{19} s_{20} s_{21} s_{22} s_{23} s_{24} s_{25} s_{26} s_{27} s_{28} s_{29} s_{30} s_{31} s_{32} s_{33} s_{34} s_{35} s_{36} s_{37} s_{38} s_{39} s_{40} s_{41} s_{42}) \in \overline{\Phi(\mathcal{S}_3^{\gamma})}.$$

Upon examining the set of equations provided in Equation 5.3, we obtain:

$$\begin{pmatrix} 11000000000022222222222333333333334444444444 \\ 051111110234111111023411111102341111110234 \\ 550123451111012345111101234511110123451111 \\ 100000000000000000000000000000010000010034 \\ 010000000000000000000000000000010000010025 \\ 001000000000000000000000000000000000000015 \\ 000100000000000000000000000000000000020010 \\ 000010000000000000000000000000000000010041 \\ 000001000000000000000000000000000000000012 \\ 000000100000000000000000000000000000020013 \\ 000000010000000000000000000000000000010044 \\ 000000001000000000000000000000000000020001 \\ 000000000100000000000000000000000000020025 \\ 000000000010000000000000000000000000020034 \\ 000000000001000000000000000000000000020043 \\ 000000000000100000000000000000000000020053 \\ 000000000000010000000000000000000000010024 \\ 000000000000001000000000000000000000000055 \\ 000000000000000100000000000000000000020050 \\ 000000000000000010000000000000000000010021 \\ 000000000000000001000000000000000000000052 \\ 000000000000000000100000000000000000010015 \\ 000000000000000000010000000000000000010033 \\ 000000000000000000001000000000000000010042 \\ 000000000000000000000100000000000000010051 \\ 000000000000000000000010000000010000020052 \\ 000000000000000000000001000000010000010023 \\ 000000000000000000000000100000010000000054 \\ 000000000000000000000000010000010000020055 \\ 000000000000000000000000001000010000010020 \\ 000000000000000000000000000100010000000051 \\ 000000000000000000000000000010010000010014 \\ 000000000000000000000000000001010000010032 \\ 000000000000000000000000000000110000010041 \\ 000000000000000000000000000000020000010050 \\ 000000000000000000000000000000001000010001 \\ 000000000000000000000000000000000100000032 \\ 000000000000000000000000000000000010020033 \\ 000000000000000000000000000000000001010004 \\ 000000000000000000000000000000000000100035 \\ 000000000000000000000000000000000000030030 \\ 000000000000000000000000000000000000001023 \\ 000000000000000000000000000000000000000141 \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \\ s_5 \\ s_6 \\ s_7 \\ s_8 \\ s_9 \\ s_{10} \\ s_{11} \\ s_{12} \\ s_{13} \\ s_{14} \\ s_{15} \\ s_{16} \\ s_{17} \\ s_{18} \\ s_{19} \\ s_{20} \\ s_{21} \\ s_{22} \\ s_{23} \\ s_{24} \\ s_{25} \\ s_{26} \\ s_{27} \\ s_{28} \\ s_{29} \\ s_{30} \\ s_{31} \\ s_{32} \\ s_{33} \\ s_{34} \\ s_{35} \\ s_{36} \\ s_{37} \\ s_{38} \\ s_{39} \\ s_4 \\ s_{41} \\ s_{42} \end{pmatrix} = \begin{pmatrix} 1 \\ 5 \\ 3 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \tag{5.12}$$

A unique solution exists for the system of equations, and solving it yields

$$s = (404321055153432105515310543224204321055153).$$

Additionally, the count of minimal coalitions is 1393200.

Example 5.5. When $k = 3$, the generator matrix of $\overline{S_3^{\beta}}$ is expressed as:

$$\overline{\Theta_3^{\beta}} = \begin{bmatrix} 1000000000000222222222222222222222222222222223333333333333333 \\ 011111102222330001111112222333333444555555001111122222233 \\ 001234511351213501234513501234513501234512012345012345 12 \end{bmatrix}. \tag{5.13}$$

In accordance with Equation 5.2, we observe that

$$\left(\overline{\Theta_3^{\beta}}\right) = \left(\overline{\Theta_3^{\beta}}\right)\left(\overline{\Theta_3^{\beta}}\right)^{\perp} = \left(\overline{\Theta_3^{\beta}}\right)^{\perp}\left(\overline{\Theta_3^{\beta}}\right) = 3 \neq 0. \tag{5.14}$$

If

$$s = (452525231110355514141433352525211130303030525252414141 03) \in \overline{S_3^{\beta}},$$

we validate a multi-secret-sharing scheme using Equation 5.1. This process entails computing the shares based on $\overline{S_3^{\beta}}$ as described below:

$$\varpi = (433), \tag{5.15}$$

Consider the secret

$$s = (s_1 s_2 s_3 s_4 s_5 s_6 s_7 s_8 s_9 s_{10} s_{11} s_{12} s_{13} s_{14} s_{15} s_{16} s_{17} s_{18} s_{19} s_{20} s_{21} s_{22} s_{23} s_{24} s_{25} s_{26} s_{27} s_{28} s_{29} s_{30} s_{31} s_{32} s_{33} s_{34} s_{35} s_{36} s_{37} s_{38} s_{39} s_{40} s_{41} s_{42} s_{43} s_{44} s_{45} s_{46} s_{47} s_{48} s_{49} s_{50} s_{51} s_{52} s_{53} s_{54} s_{55} s_{56}) \in \overline{S_3^{\beta}}.$$

Upon scrutinizing the system of equations outlined in Equation 5.3, we derive:

$$\begin{pmatrix}
10000000000002222222222222222222222222223333333333333333 \\
01111110222330001111112223333334445555550011111122222233 \\
00123451135121350123451350123451350123451201234501234512 \\
10000000000000000000000000000000000000010000000000000214 \\
01000000000000000000000000000000000000000000000000000110 \\
00100000000000000000000000000000000000000000000000000103 \\
00010000000000000000000000000000000000000000000000000112 \\
00001000000000000000000000000000000000000000000000000105 \\
00000100000000000000000000000000000000000000000000000114 \\
00000010000000000000000000000000000000000000000000000101 \\
00000001000000000000000000000000000000000000000000000015 \\
00000000100000000000000000000000000000000000000000000213 \\
00000000010000000000000000000000000000000000000000000215 \\
00000000001000000000000000000000000000000000000000000211 \\
00000000000100000000000000000000000000000000000000000301 \\
00000000000010000000000000000000000000000000000000000310 \\
00000000000001000000000000000000000000020000000000000415 \\
00000000000000100000000000000000000000020000000000000411 \\
00000000000000010000000000000000000000020000000000000413 \\
00000000000000001000000000000000000000020000000000000510 \\
00000000000000000100000000000000000000020000000000000503 \\
00000000000000000010000000000000000000020000000000000512 \\
00000000000000000001000000000000000000020000000000000505 \\
00000000000000000000100000000000000000020000000000000514 \\
00000000000000000000010000000000000000020000000000000501 \\
00000000000000000000001000000000000000020000000000000013 \\
00000000000000000000000100000000000000020000000000000015 \\
00000000000000000000000010000000000000020000000000000011 \\
00000000000000000000000001000000000000020000000000000114 \\
00000000000000000000000000100000000000020000000000000101 \\
00000000000000000000000000010000000000020000000000000110 \\
00000000000000000000000000001000000000020000000000000103 \\
00000000000000000000000000000100000000020000000000000112 \\
00000000000000000000000000000010000000020000000000000105 \\
00000000000000000000000000000001000000020000000000000211 \\
00000000000000000000000000000000100000020000000000000213 \\
00000000000000000000000000000000010000020000000000000215 \\
00000000000000000000000000000000001000020000000000000312 \\
00000000000000000000000000000000000100020000000000000305 \\
00000000000000000000000000000000000010020000000000000314 \\
00000000000000000000000000000000000001020000000000000301 \\
00000000000000000000000000000000000000120000000000000310 \\
00000000000000000000000000000000000000030000000000000303 \\
00000000000000000000000000000000000000001000000000000304 \\
00000000000000000000000000000000000000000100000000000313 \\
00000000000000000000000000000000000000000010000000000405 \\
00000000000000000000000000000000000000000001000000000414 \\
00000000000000000000000000000000000000000000100000000401 \\
00000000000000000000000000000000000000000000010000000410 \\
00000000000000000000000000000000000000000000001000000403 \\
00000000000000000000000000000000000000000000000100000412 \\
00000000000000000000000000000000000000000000000010000515 \\
00000000000000000000000000000000000000000000000001000502 \\
00000000000000000000000000000000000000000000000000100511 \\
00000000000000000000000000000000000000000000000000010504 \\
00000000000000000000000000000000000000000000000000001513 \\
00000000000000000000000000000000000000000000000000000022
\end{pmatrix}
\begin{pmatrix}
s_1 \\ s_2 \\ s_3 \\ s_4 \\ s_5 \\ s_6 \\ s_7 \\ s_8 \\ s_9 \\ s_{10} \\ s_{11} \\ s_{12} \\ s_{13} \\ s_{14} \\ s_{15} \\ s_{16} \\ s_{17} \\ s_{18} \\ s_{19} \\ s_{20} \\ s_{21} \\ s_{22} \\ s_{23} \\ s_{24} \\ s_{25} \\ s_{26} \\ s_{27} \\ s_{28} \\ s_{29} \\ s_{30} \\ s_{31} \\ s_{32} \\ s_{33} \\ s_{34} \\ s_{35} \\ s_{36} \\ s_{37} \\ s_{38} \\ s_{39} \\ s_4 \\ s_{41} \\ s_{42} \\ s_{43} \\ s_{44} \\ s_{45} \\ s_{46} \\ s_{47} \\ s_{48} \\ s_{49} \\ s_{50} \\ s_{51} \\ s_{52} \\ s_{53} \\ s_{54} \\ s_{55} \\ s_{56}
\end{pmatrix}
=
\begin{pmatrix}
4 \\ 3 \\ 3 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0
\end{pmatrix}
\tag{5.16}$$

A singular solution is present for the system of equations, and resolving it provides $s = (45252523111035551414143335252521113030303052525241414103)$. Furthermore, the number of minimal coalitions is 1393200.

6 Security Assessment of a Multi-Secret Sharing Scheme Utilizing α, β, and γ Linear Simplex Codes

The security of the proposed multi-secret sharing scheme is enhanced by the structural properties of the α, β, and γ-linear simplex codes, which provide a robust framework for encoding and distributing multiple secrets among participants. These codes ensure that only authorized sets of participants, forming minimal coalitions, can reconstruct the secret while preventing unauthorized access. Their error-correcting capabilities are essential to enhancing the scheme's resilience against adversarial threats, including collusion attacks where subsets of participants attempt to recover secrets without fulfilling the minimum coalition requirement. Defined over finite rings, α, β, and γ-simplex codes contribute to security through their distinct parameters, *such as code length, dimension, and minimum Hamming distance, that secure error detection and correction mechanisms.*

These properties ensure participants or coalitions cannot easily reconstruct secrets without the requisite shares. The security strength of the scheme is tightly bound to the ability of these codes to prevent unauthorized information recovery, even in scenarios where multiple participants collaborate.

Additionally, security evaluation can be further developed to assess resistance against various attack models, including structured collusion strategies. Future research may explore enhancements to the security model by incorporating advanced cryptographic techniques, such as homomorphic encryption or threshold cryptography, to bolster the scheme's security against evolving risks. Ultimately, α, β, and γ-simplex codes provide a flexible yet secure foundation for multi-secret sharing, ensuring robust protection against individual and collaborative attacks.

7 Conclusion

This article investigates simplex codes of types α, β, and γ over $\mathbb{Z}_2\mathbb{Z}_6$, exploring their properties and applications in the context of multi-secret sharing schemes. The research delves into the covering radius of simplex codes of these types, shedding light on their effectiveness in error detection and correction. Additionally, the study encompasses the design and analysis of a multi-secret sharing scheme that employs α, β, and γ-linear simplex codes. The features of this scheme are meticulously analyzed, and information concerning coalitions is provided. The security assessment highlights the robustness of the scheme against unauthorized access, emphasizing the importance of linear codes in cryptographic applications. Future work could extend this research by exploring additional applications of these codes in secure communications, optimizing the scheme for improved efficiency, and integrating advanced cryptographic techniques such as homomorphic encryption or lattice-based cryptography. Furthermore, an in-depth complexity analysis of the scheme's implementation could provide insights into its practical feasibility for large-scale systems. These findings contribute to the ongoing development of secure and efficient cryptographic protocols, reinforcing the role of algebraic coding theory in enhancing information security.

References

[1] T. Abualrub, I. Siap and N. Aydin, $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes, IEEE Transactions on Information Theory, 60(3), 115-121 (2014).

[2] A. Alahmadi, A. Altassan, A. AlKenani, S. Calkavur, S. Hatoon and S. Patrick, A Multi-secret sharing Scheme Based on LCD Codes, Mathematics, 8(2), 272 (2020).

[3] M.M. Al Ashker, Simplex codes over the ring F_2+uF_2, The Arabian Journal For Science and Engineering, 30(2A), 277-285 (2005).

[4] M.M. Al Ashker, Simplex codes over the ring $\sum_{n=0}^{s} u^n F_2$, Turkish Journal of Mathematics, 29, 221-233 (2005).

[5] M.M. Al Ashker and I.M Isleem, Simplex codes over the ring $F_2 + vF_2$, An-Najah University Journal for Research - A (Natural Sciences), 22, 25-42 (2008).

[6] M. Bilal, J. Borges, S.T. Dougherty and C. Fernandez-Cordoba, Maximum distance separable codes over $\mathbb{Z}_4$ and $\mathbb{Z}_2\mathbb{Z}_4$, Designs, Codes and Cryptography, 61(1), 31-40 (2011).

[7] J. Borges, S.T. Dougherty and C. Fernandez-Cordoba, Characterization and constructions of self-dual codes over $\mathbb{Z}_2\mathbb{Z}_4$, Advances in Mathematics of Communications, 6(3), 287-303 (2012).

[8] J. Borges, C. Fernandez-Cordoba, J. Pujol, J. Rifa and M. Villanueva, $\mathbb{Z}_2\mathbb{Z}_4$-linear codes: generator matrices and duality, Designs, Codes and Cryptography, 54(2), 167-179 (2010).

[9] Y.Cengellenmis and M. Al-Ashker, Simplex codes of type β over $F_3 + vF_3$, Proceedings of the Jangjeon Mathematical Society, 14(3), (2011).

[10] Y.Cengellenmis and M. Al-Ashker, Simplex codes of type γ over $F_3 + vF_3$, International Mathematical Forum, 5, 1993-2000 (2010).

[11] R. Chapman, S.T. Dougherty,P. Gaborit and P. Solé, 2-modular lattices from ternary codes, Journal de Theorie des Nombres de Bordeaux, 14(1), 73-85 (2002).

[12] K. Chatouh, K. Guenda, T.A. Gulliver and L. Noui, On some classes of linear codes over $\mathbb{Z}_2\mathbb{Z}_4$ and their covering radii, Journal of Applied Mathematics and Computing, 53(1-2), 201-222 (2017).

[13] P. Chellapandian, On the Covering radius of Codes over $\mathbb{Z}_6$, International Journal on Information Theory (IJIT), 5(2), 1-9 (2016).

[14] G.D. Cohen, M.G. Karpovsky, H.F. Mattson and J.R. Schatz, Covering radius-Survey and recent results, IEEE Transactions on Information Theory, 31(3), 328-343 (1985).

[15] C.J. Colbourn and M.K. Gupta, On quaternary MacDonald codes, Proceedings ITCC 2003. International Conference on Information Technology: Coding and Computing, 212-215, (2003).

[16] M. Cruz, C. Durairajan and P. Solé, On the Covering Radius of Codes over $\mathbb{Z}_{p^k}$, Mathematics, 8, 328 (2020).

[17] P. Delsarte, An algebraic approach to the association schemes of coding theory, Philips Research Reports: Supplements, 10, (1973).

[18] I.M Isleem, On Linear codes $F_2 \times F_2$, Master Thesis, Islamic University of Gaza, 2007.

[19] M. Gupta, D. Glynn end T. Gulliver, On senary simplex codes, In International Symposium on applied Algebra, algebraic algorithm and Error- correcting Codes (Springer, berlin Heidelberg), 112-121 (2001).

[20] M.K. Gupta and C. Durairajan, On the covering radius of some modular codes, arXiv:1206.3038 v2 [cs.IT] Jun. 2012.

Author information

Mohammed. M. Al-Ashker, Department of Mathematics, Islamic University of Gaza , PO Box 108, Gaza,, Palestine.
E-mail: mashker@mail.iugaza.edu

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

Received: 2024-10-02
Accepted: 2025-02-11