Filomat 39:11 (2025), 3609–3622
https://doi.org/10.2298/FIL2511609A

Published by Faculty of Sciences and Mathematics,
University of Niš, Serbia
Available at: http://www.pmf.ni.ac.rs/filomat

Exploring simplex codes and their applications over $\mathbb{Z}_3\mathbb{Z}_6$

Mohammed. M. Al-Ashker[a], Karima Chatouh[b,*]

[a] *Department of Mathematics, Islamic University of Gaza , PO Box 108, Gaza, Palestine*
[b] *Laboratoire D´applications des Mathématiques à L´informatique et à L´électronique Faculty of Economic, Commercial and Management Sciences Batna 1 University, Batna, Algeria*

Abstract. This article delves into the investigation of simplex codes of types α, β, and γ over the ring $\mathbb{Z}_3\mathbb{Z}_6$. It examines the fundamental properties of these codes, including their covering radius, association schemes, and practical applications in multi-secret sharing schemes. The covering radius analysis sheds light on the error-correcting capabilities of $\mathbb{Z}_3\mathbb{Z}_6$-simplex codes, crucial for reliable communication systems. Additionally, association schemes for $\mathbb{Z}_6$-simplex codes provide insights into efficient encoding and decoding strategies, enhancing their performance in various applications. Furthermore, the development of a multi-secret sharing scheme based on these codes highlights their versatility beyond traditional error correction, offering promising avenues for secure multi-party communication and data storage. This exploration of simplex codes over $\mathbb{Z}_3\mathbb{Z}_6$ not only contributes to theoretical coding theory but also opens up new opportunities in practical cryptography, advancing the realm of secure information exchange protocols.

1. Introduction

The covering radius, association schemes for linear codes over finite rings, and multi-secret sharing schemes based on linear codes over finite rings are interconnected concepts within the realms of coding theory and cryptography. The covering radius of a linear code over a finite ring defines the maximum radius within which any codeword can be covered by a sphere centered at another codeword. This parameter is crucial in assessing the error-correction capabilities of the code. Association schemes for linear codes over finite rings provide a systematic approach to understanding the relationships between codewords within the code. These schemes categorize the vertices or codewords based on specific properties or configurations, aiding in the analysis of the code's algebraic and geometric structures. The association schemes help in designing efficient encoding and decoding algorithms. Multi-secret sharing schemes based on linear codes over finite rings utilize the properties and configurations established by association schemes to securely distribute multiple secrets among parties. By leveraging the structure of the code, these schemes enable the distribution, combination, and reconstruction of secrets in a manner that ensures only authorized subsets of parties can access the secret information. Overall, the covering radius, association schemes, and multi-secret sharing schemes are integral components of coding theory and cryptography, working together to enable

2020 *Mathematics Subject Classification*. Primary 16P10; Secondary 11T71; 94B05.
Keywords. Simplex codes, Different weights, Covering radius, Association Schemes, Multi-secret sharing scheme.
Received: 04 May 2024; Accepted: 11 February 2025
Communicated by Dijana Mosić
* Corresponding author: Karima Chatouh
Email addresses: mashker@mail.iugaza.edu (Mohammed. M. Al-Ashker), karima.chatouh@univ-batna.dz (Karima Chatouh)
ORCID iDs: https://orcid.org/0000-0002-8088-8796 (Mohammed. M. Al-Ashker),
https://orcid.org/0000-0003-4061-1239 (Karima Chatouh)

efficient error correction and secure communication in various practical applications. For more detailed information, refer to the following references [1, 4–8, 14].

The aim of this article is to provide a comprehensive exploration of simplex codes of types α, β, and γ over the ring $\mathbb{Z}_3\mathbb{Z}_6$, focusing particularly on their covering radius, association schemes, and applications in multi-secret sharing schemes. The covering radius of $\mathbb{Z}_3\mathbb{Z}_6$-simplex codes of types α, β, and γ will be analyzed to understand the maximum radius within which any codeword can be covered by a sphere centered at another codeword. Furthermore, the article will delve into association schemes tailored for $\mathbb{Z}_6$-simplex codes of types α, β, and γ, aiming to elucidate the structural properties and relationships between codewords within the code. Finally, the article will explore the implementation of multi-secret sharing schemes based on $\mathbb{Z}_3\mathbb{Z}_6$-simplex codes of types α, β, and γ, demonstrating how these cryptographic protocols leverage the properties of simplex codes to securely distribute, combine, and reconstruct multiple secrets among authorized parties. Through a thorough examination of these topics, the article aims to contribute to the understanding and advancement of coding theory and cryptography, with practical implications for error correction and secure communication systems.

The article is organized as follows: Section 2 provides background information and preliminaries regarding the different weights in $\mathbb{Z}_3\mathbb{Z}_6$ and the covering radius, including discussions on upper and lower bounds. In Section 3, the focus shifts to simplex codes of types α, β, and γ over $\mathbb{Z}_3\mathbb{Z}_6$, exploring their construction and properties. Following that, Section 4 delves into an in-depth analysis of the covering radius of $\mathbb{Z}_3\mathbb{Z}_6$-simplex codes of types α, β, and γ, examining various factors influencing this critical parameter. In Section 5, attention is directed towards association schemes tailored for $\mathbb{Z}_6$-simplex codes of types α, β, and γ, shedding light on the structural relationships between codewords within the code. Finally, Section 6 presents a discussion on multi-secret sharing schemes based on $\mathbb{Z}_3\mathbb{Z}_6$-simplex codes of types α, β, and γ, detailing their implementation and cryptographic implications in securely distributing and managing multiple secrets among authorized parties. Through this structured approach, the article aims to provide a comprehensive understanding of simplex codes, covering radius analysis, association schemes, and multi-secret sharing schemes, thereby contributing to advancements in coding theory and cryptography.

2. Some Background and Preliminaries

This section presents preliminary findings based on references [2, 3]. Here, $\mathbb{Z}_3$ and $\mathbb{Z}_6$ represent the rings of integers modulo 3 and 6 respectively, and $\mathbb{Z}_3^n$ and $\mathbb{Z}_6^n$ denote the space of n-tuples over these rings. We define a ring

$$\mathbb{Z}_3\mathbb{Z}_6 = \{00, 01, 02, 03, 04, 05, 10, 11, 12, 13, 14, 15, 20, 21, 22, 23, 24, 25\},$$

with integers modulo 3 and 6. An non-empty set C is termed a $\mathbb{Z}_3\mathbb{Z}_6$-additive code if it forms a subgroup of $\mathbb{Z}_3^\gamma \times \mathbb{Z}_6^\delta$. In such cases, C is isomorphic to an abelian structure $\mathbb{Z}_3^\lambda \times \mathbb{Z}_6^\mu$ for some λ and μ, with the type of C being $3^\lambda 6^\mu$ as a group. Consequently, C comprises $|C| = 3^\lambda \times 6^\mu$ codewords, and the number of order for any two codewords in C is also $|C| = 3^\lambda \times 6^\mu$. Furthermore, a linear code C of length n over $\mathbb{Z}_6$ is an additive subgroup of $\mathbb{Z}_6^n$, where an element of C is called a codeword of C.

2.1. The Different Weights in $\mathbb{Z}_3\mathbb{Z}_6$

The Hamming weight $w_H(c)$ of a vector c in $(\mathbb{Z}_3\mathbb{Z}_6)^n$ counts the number of non-zero components within the vector. In addition to the Hamming weight, three other weight measures are commonly used: the Lee weight $w_L(c)$, the Euclidean weight $w_E(c)$, and the Chinese Euclidean weight $w_{CE}(c)$. These weights provide

alternative perspectives on the structure of the vector c within the space $(\mathbb{Z}_3\mathbb{Z}_6)^n$.

$c_i, 0 \le i \le n$	$w_L(c_i)$
00	0
01,05,10	1
02,04,20,11,15	2
03,12,21,14,25	3
13,22,24	4
23	5

$c_i, 0 \le i \le n$	$w_E(c_i)$
00	0
01,05,10	1
11,15	2
02,04,20	4
14,12,21,25	5
22,24	8
03	9
13	10
23	13

$c_i, 0 \le i \le n$	$w_{CE}(c_i)$
00	0
01,05,10	1
11,15	2
02,20,04	3
12,21,14,03,25	4
13	5
22,24	6
23	7

(1)

2.2. Covering Radius: Upper and Lower Bounds

In this subsection, we will explore upper and lower bounds on the covering radius of a code. The covering radius is a crucial parameter in coding theory, quantifying the maximum distance between a codeword and its nearest neighbor outside the code. According to [9, 13], the covering radii of a code C over $\mathbb{Z}_3\mathbb{Z}_6$, concerning the Lee, Euclidean, and Chinese Euclidean distances, are provided as follows:

$$r_D(C) = \max_{x \in \mathbb{Z}_3^\eta \times \mathbb{Z}_6^\delta} \left\{ \min_{c \in C} d_L(x, c) \right\}, \tag{2}$$

and

$$\mathbb{Z}_3^\eta \times \mathbb{Z}_6^\delta = \cup_{c \in C} S_{r_D}(c), \tag{3}$$

where $S_{r_D}(x) = \left\{ y \in \mathbb{Z}_3^\eta \times \mathbb{Z}_6^\delta; d(x, y) \le r_D \right\}$.

Definition 2.1. *For a ternary linear code C without a zero coordinate,* $r_D(C) = \lfloor \frac{n}{3} \rfloor$.

Proposition 2.2. *Let C be a code over* $\mathbb{Z}_3^\gamma \times \mathbb{Z}_6^\delta$ *and* $\rho(C)$ *be the Gray image of C, then* $r_D(C) = r(\rho(C))$.

The subsequent result proves to be valuable in determining the covering radius of codes over the ring $\mathbb{Z}_3\mathbb{Z}_6$.

Proposition 2.3. *If* C_0 *and* C_1 *are codes over* $\mathbb{Z}_3\mathbb{Z}_6$ *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*

$$G = \begin{pmatrix} 0 & G_1 \\ G_0 & A \end{pmatrix},$$

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

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

for all distances d over $\mathbb{Z}_3\mathbb{Z}_6$.

3. Simplex Codes of Types α, β, and γ over $\mathbb{Z}_3\mathbb{Z}_6$

In this section, according to [5, 6, 12, 14] we delve into the construction of Simplex Codes of Types α, β, and γ over the ring $\mathbb{Z}_3\mathbb{Z}_6$. Simplex codes, a class of linear error-correcting codes, play a pivotal role in various communication and data storage systems due to their simplicity and efficiency.

Definition 3.1. *The generator matrix of S_k^α, the simplex code of type α over $\mathbb{Z}_3\mathbb{Z}_6$ is constructed by concatenating 6^k copies of the generator matrix of $S_{3,k}^\alpha$ and 3^k copies of the generator matrix of $S_{6,k}^\alpha$, given by*

$$\mathfrak{G}^\alpha = \left(\begin{array}{c|c} 1_{6^k} \otimes T_{3,k}^\alpha & 1_{3^k} \otimes G_{6,k}^\alpha \end{array} \right), \text{for } k \geq 1, \tag{4}$$

with

$$T_{3,k}^\alpha = \begin{pmatrix} 00\cdots0 & 11\cdots1 & 22\cdots2 \\ T_{3,k-1}^\alpha & T_{3,k-1}^\alpha & T_{3,k-1}^\alpha \end{pmatrix}, \text{ for } k \geq 2, \tag{5}$$

and

$$G_{6,k}^\alpha = \begin{pmatrix} 00\ldots0 & 11\ldots1 & 22\ldots2 & 33\ldots3 & 44\ldots4 & 555\ldots5 \\ G_{6,k-1}^\alpha & G_{6,k-1}^\alpha & G_{6,k-1}^\alpha & G_{6,k-1}^\alpha & G_{6,k-1}^\alpha & G_{6,k-1}^\alpha \end{pmatrix}, \text{ for } k \geq 2. \tag{6}$$

Remark 3.2. *The simplex code of type α over $\mathbb{Z}_3\mathbb{Z}_6$ has a length equal to $2^{k+1} \times 3^{2k}$, and the total number of codewords is given by $3^{k_0}6^{k_1}$, where k_0 and k_1 are certain exponents.*

Example 3.3. *When $k = 1$ and $k_0 = 0$, $k_1 = 1$, all codewords of the simplex codes S_1^α are*

$$\begin{aligned} c_1 &= 000000000000000000000000000000000000, \\ c_2 &= 000102030405101112131415202122232425, \\ c_3 &= 000204000204202224202224101214101214, \\ c_4 &= 000300030003000300030003000300030003, \\ c_5 &= 000402000402101412101412202422202422, \\ c_6 &= 000504030201202524232221101514131211. \end{aligned}$$

The type β of the simplex codes S_k^β over $\mathbb{Z}_3\mathbb{Z}_6$ is a punctured version of S_k^α. The number of codewords is $3^{k_0}6^{k_1}$ and its length is $\frac{(2^k-1)(3^k-1)^2}{2}$.

Definition 3.4. *The generator matrix of S_k^β is the concatenation of $\frac{(2^k-1)(3^k-1)}{2}$ copies of the generator matrix of the ternary simplex code $S_{3,k}^\beta$ and $\frac{(3^k-1)}{2}$ copies of the generator matrix of the simplex code $S_{6,k}^\beta$ over $\mathbb{Z}_6$, given by*

$$\mathfrak{G}^\beta = \left[\begin{array}{c|c} 1_{\frac{(2^k-1)(3^k-1)^2}{2}} \otimes T_{3,k}^\beta & 1_{\frac{(3^k-1)}{2}} \otimes G_{6,k}^\beta \end{array} \right], \text{for } k \geq 1, \tag{7}$$

where

$$T_{3,k}^\beta = \begin{pmatrix} 11\cdots1 & 00\cdots0 \\ T_{3,k-1}^\alpha & T_{3,k-1}^\beta \end{pmatrix}, \text{ for } k \geq 3, \text{ with } T_{3,2}^\beta = \begin{pmatrix} 111 & 0 \\ 012 & 1 \end{pmatrix} \tag{8}$$

and

$$G_{6,k}^\beta = \begin{pmatrix} 11\cdots1 & 00\cdots0 & 22\cdots2 & 33\cdots3 \\ G_{6,k-1}^\alpha & G_{6,k-1}^\beta & \Lambda_{k-1} & \mu_{k-1} \end{pmatrix}, G_{6,2}^\beta = \begin{pmatrix} 111111 & 0 & 222 & 33 \\ 012345 & 1 & 135 & 12 \end{pmatrix}, \tag{9}$$

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

$$\Lambda_k = \begin{pmatrix} 00\cdots0 & 11\cdots1 & 22\cdots2 & 33\cdots3 & 44\cdots4 & 55\cdots5 \\ \Lambda_{k-1} & G_{6,k-1}^\alpha & \Lambda_{k-1} & G_{6,k-1}^\alpha & \Lambda_{k-1} & G_{6,k-1}^\alpha \end{pmatrix}, \tag{10}$$

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

$$\mu_k = \begin{pmatrix} 00\cdots0 & 11\cdots1 & 22\cdots2 & 33\cdots3 \\ \mu_{k-1} & G_{6,k-1}^\alpha & G_{6,k-1}^\alpha & \mu_{k-1} \end{pmatrix}. \tag{11}$$

In the following we define the simplex code S_k^γ of type γ over $\mathbb{Z}_3\mathbb{Z}_6$. As in [12], let $G_{6,k}^\gamma$ be the $k\times 2^{k-1}(3^k-2^k)$ matrix defined inductively by

$$G_{6,k}^\gamma = \begin{pmatrix} 11\cdots 1 & 00\cdots 0 & 22\ldots 2 & 33\cdots 3 & 44\cdots 4 \\ G_{6,k-1}^\alpha & G_{6,k-1}^\gamma & G_{6,k-1}^\gamma & G_{6,k-1}^\gamma & G_{6,k-1}^\gamma \end{pmatrix}, \tag{12}$$

with

$$G_{6,2}^\gamma = \begin{pmatrix} 111111 & 0 & 2 & 3 & 4 \\ 012345 & 1 & 1 & 1 & 1 \end{pmatrix}. \tag{13}$$

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.

Proposition 3.5. *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 $2^{k-1}(3^k-2^k)$.*

Definition 3.6. *The generator matrix of the simplex code S_k^γ over $\mathbb{Z}_3\mathbb{Z}_6$ is the concatenation of $2^{k-1}(3^k-2^k)$ copies of the generator matrix of $S_{3,k}^\alpha$ and 2×3^k copies of the generator matrix of $S_{6,k}^\gamma$, given by*

$$\mathfrak{G}^\gamma = \left[\ 1_{2^{k-1}(2^k-3^k)}\otimes T_{3,k}^\alpha \ \middle|\ 1_{3^k}\otimes G_{6,k}^\gamma\ \right], \text{for } k\geq 2, \tag{14}$$

Note that the length of the simplex code S_k^γ over $\mathbb{Z}_3\mathbb{Z}_6$ of type γ is $6^k(3^k-2^k)$.

3.1. The Different Weight Distribution of $\mathbb{Z}_3\mathbb{Z}_6$-Simplex Codes of Types α, β and γ

From the structure of the generator matrices associated with the linear codes $\mathbb{Z}_3\mathbb{Z}_6$-linear codes S_k^α, S_k^β and S_k^γ, we can deduce the ensuing outcomes, shedding light on the different distribution weights.

	Hamming Weight
S_k^α	$0, 3^{k-1}\left(3\times 2^{k-1}+1\right), 3^{k-1}\left(4\times 2^{k-1}+1\right), 3^{k-1}\left(5\times 2^{k-1}+1\right)$
S_k^β	$0, \left(2^{k-2}+1\right)\left(3^k-1\right), \frac{6^k}{3}+\frac{2\times 3^k}{3}-1, \frac{5\times 6^k}{2}+\frac{2\times 3^k}{3}-2^{k-2}-1$
S_k^γ	$0, 5\times 6^{k-1}-3\times 2^{2k-2}+3^k-1$

Table 1: Hamming Weight of S_k^α, S_k^β, and S_k^γ.

	Lee Weight
S_k^α	$0, 2^{k+2}\times 3^{2k-2}, 2^{k-1}\times 3^{2k}$
S_k^β	$0, 3\times 2^{k-2}\left(3^k-1\right)^2, 2\times 3^{k-1}\left(2^k-1\right)\left(3^k-1\right),$ $\left(3^k-1\right)\left[3\times 2^{k-2}\left(3^k-1\right)+2\times 3^{k-1}\left(2^k-1\right)\right]$
S_k^γ	$0, 2^{k-2}\left(3^{k+1}-7\times 2^{k-1}\right)+3^{k-1}$

Table 2: Lee Weight of S_k^α, S_k^β, and S_k^γ.

	Euclidean Weight
S_k^{α}	$0, 2^{k-1}\times 3^{2k+1}, 2^{k+3}\times 3^{2k-2}, 19\times 2^{k-1}\times 3^{2k-2}$
S_k^{β}	$0, 9\times 2^{k-2}\left(3^k-1\right)^2, 4\times 3^{k-1}\left(2^k-1\right)\left(3^k-1\right),$ $\left(3^k-1\right)\left[3^{k-1}\left(19\times 2^{k-2}-4\right)-9\times 2^{k-2}\right]$
S_k^{γ}	$0, 2^{k-2}\left(19\times 3^{k-1}-17\times 2^{k-1}\right)+3^{k-1}$

Table 3: Euclidean Weight of S_k^{α}, S_k^{β}, and S_k^{γ}.

	Chinese Euclidean Weight
S_k^{α}	$0, 2^k\times 3^{2k-1}$
S_k^{β}	$0, \left(2^k+1\right)\left(3^k-1\right), 6^k-1, 2^k\left(3^k-1\right)-1$
S_k^{γ}	$0, 6^k-5\times 4^{k-1}+3^{k-1}$

Table 4: Chinese Euclidean Weight of S_k^{α}, S_k^{β}, and S_k^{γ}.

4. The Covering Radius of $\mathbb{Z}_3\mathbb{Z}_6$-Simplex Codes of Types α, β and γ

In this section, we explore the calculation of the covering radius for these specific codes. To achieve this, it is crucial to have a thorough understanding of the covering radius of repetition codes, see [4, 10, 12]. This knowledge forms the foundation for determining the covering radius of simplex codes of types α, β and γ.

Theorem 4.1. *The covering radii of the $\mathbb{Z}_3\mathbb{Z}_6$-simplex codes of type α are given by*

1. $r_L(S_k^{\alpha}) \leq 31\times 2^k\times 3^{2k-1}-3^{k+2}$,
2. $(13\times 2^{k+2}\times 3^{2k-1}-2^4\times 3^k \leq r_E(S_k^{\alpha}) \leq 85\times 2^k\times 3^{2k-1}-3^{k+3}$,
3. $r_{CE}(S_k^{\alpha}) \leq 5\times 2^{k+1}\times 3^{2k-1}-2\times 3^k$.

Proof. According to [4, 10, 12], from Definition 2.1 and Proposition 2.3 the the covering radius $r_L(S_k^{\alpha}), r_E(S_k^{\alpha})$ and $r_{CE}(S_k^{\alpha})$ are given by

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

$$\begin{aligned} r_L(S_k^{\alpha}) &\leq r_L(6^kS_{3,k}^{\alpha})+r_L(3^kS_{6,k}^{\alpha}) \\ &\leq 6^kr_L(S_{3,k}^{\alpha})+3^kr_L(S_{6,k}^{\alpha}) \\ &\leq 6^kr_H(S_{3,k}^{\alpha})+3^kr_L(S_{6,k}^{\alpha}) \\ &\leq 6^k\left(\frac{4\times 3^k}{3}\right)+3^k\left(5\times 9\times 6^{k-1}+5\times 9\times 6^{k-2}+\ldots+5\times 9\times 6^0\right) \\ &\leq 2^{k+2}3^{2k-1}+3^{k+2}\left(6^k-1\right) \\ &\leq \leq 31\times 2^k\times 3^{2k-1}-3^{k+2}. \end{aligned}$$

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

$$\begin{aligned} r_E(S_k^{\alpha}) &\geq 4\times 3^{k-1}\times 6^k+16\times 3^k(6^k-1) \\ &\geq 13\times 2^{k+2}\times 3^{2k-1}-2^4\times 3^k. \end{aligned}$$

On the other hand,

$$\begin{aligned} r_E(S_k^{\alpha}) &\leq 4\times 3^{k-1}\times 6^k+3^3\times 3^k(6^k-1) \\ &\leq 85\times 2^k\times 3^{2k-1}-3^{k+3}. \end{aligned}$$

3. In reference to the code S_k^α and its correlation with the Chinese Euclidean weight, we have

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

□

The following theorem presents the covering radius of $\mathbb{Z}_3\mathbb{Z}_6$-simplex codes of type β.

Theorem 4.2. *The covering radius of the $\mathbb{Z}_3\mathbb{Z}_6$-simplex codes of type β is given by*

(1) $r_L(S_k^\beta) \leq (3^k-1)\left[\frac{(2^k-1)^2(3^k-1)^2}{3} + \left[2^{k-2}(3^{k+2}-15)-6\right]\right]$,

(2) $r_E(S_k^\beta) \leq (3^k-1)\left[\frac{(2^k-1)^2(3^k-1)^2}{3} + \left[2^{k-2}(3^{k+2}-45)-36\right]\right]$,

(3) $r_{CE}(S_k^\beta) \leq (3^k-1)\left[\frac{(2^k-1)^2(3^k-1)^2}{3} + \left[2^k(3^{k+1}-5)-8\right]\right]$.

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

$$\begin{aligned} r_L(S_k^\beta) &\leq r_L\left(\frac{(2^k-1)(3^k-1)}{2}S_{3,k}^\beta\right) + r_L\left(\frac{(3^k-1)}{2}S_{6,k}^\beta\right) \\ &\leq \frac{(2^k-1)(3^k-1)}{2}r_L(S_{3,k}^\beta) + \frac{(3^k-1)}{2}r_L(S_{6,k}^\beta) \\ &\leq \frac{(2^k-1)(3^k-1)}{2}r_H(S_{3,k}^\beta) + \frac{(3^k-1)}{2}r_L(S_{6,k}^\beta) \\ &\leq \frac{(2^k-1)^2(3^k-1)^3}{3} + \left[\frac{540}{20}\left(6^{k-1}-1\right) - \frac{60}{4}\left(2^{k-1}-1\right)\right] \\ &\leq (3^k-1)\left[\frac{(2^k-1)^2(3^k-1)^2}{3} + \left[2^{k-2}(3^{k+2}-15)-6\right]\right]. \end{aligned}$$

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

$$\begin{aligned} r_E(S_k^\beta) &\leq r_E\left(\frac{(2^k-1)(3^k-1)}{2}S_{3,k}^\beta\right) + r_E\left(\frac{(3^k-1)}{2}S_{6,k}^\beta\right) \\ &\leq \frac{(2^k-1)(3^k-1)}{2}r_E(S_{3,k}^\beta) + \frac{(3^k-1)}{2}r_E(S_{6,k}^\beta) \\ &\leq \frac{(2^k-1)(3^k-1)}{2}r_H(S_{3,k}^\beta) + \frac{(3^k-1)}{2}r_E(S_{6,k}^\beta) \\ &\leq \frac{(2^k-1)^2(3^k-1)^3}{3} + \left[3^4\left(6^{k-1}-1\right) - 45\left(2^{k-1}-1\right)\right] \\ &\leq (3^k-1)\left[\frac{(2^k-1)^2(3^k-1)^2}{3} + \left[2^{k-2}(3^{k+2}-45)-36\right]\right]. \end{aligned}$$

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

$$\begin{aligned} r_{CE}(S_k^\beta) &\leq r_{CE}\left(\frac{(2^k-1)(3^k-1)}{2}S_{3,k}^\beta\right) + r_{CE}\left(\frac{(3^k-1)}{2}S_{6,k}^\beta\right) \\ &\leq \frac{(2^k-1)(3^k-1)}{2}r_{CE}(S_{3,k}^\beta) + \frac{(3^k-1)}{2}r_{CE}(S_{6,k}^\beta) \\ &\leq \frac{(2^k-1)(3^k-1)}{2}r_H(S_{3,k}^\beta) + \frac{(3^k-1)}{2}r_{CE}(S_{6,k}^\beta) \\ &\leq \frac{(2^k-1)^2(3^k-1)^3}{3} + \left[36\left(6^{k-1}-1\right) - 20\left(2^{k-1}-1\right)\right] \\ &\leq (3^k-1)\left[\frac{(2^k-1)^2(3^k-1)^2}{3} + \left[2^k(3^{k+1}-5)-8\right]\right]. \end{aligned}$$

□

Theorem 4.3. *The covering radius of the simplex codes of types γ is given by*

(1) $r_L(S_k^\gamma) \leq 6^k\left(\frac{32}{15}3^k - \frac{21}{3}2^k\right) - \frac{194}{5}3^k$,

(2) $r_E(S_k^\gamma) \leq 3^k\left[\frac{85}{3}6^k - 2^k\left(\frac{4}{3}2^k + 45\right) - 72\right]$,

(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. Regarding the code S_k^γ and its association with the Lee weight, we have

$$\begin{aligned} r_L(S_k^\gamma) &\leq r_L(2^{k-1}\left(3^k-2^k\right)S_{3,k}^\gamma) + r_L(2\times 3^k S_{6,k}^\gamma) \\ &\leq 2^{k-1}\left(3^k-2^k\right)r_L(S_{3,k}^\gamma) + 2\times 3^k r_L(S_{6,k}^\gamma) \\ &\leq 2^{k-1}\left(3^k-2^k\right)r_H(S_{3,k}^\gamma) + 2\times 3^k r_L(S_{6,k}^\gamma) \\ &\leq 8\times 6^{k-1}\left(3^k-2^k\right) + 2\times 3^k\left[\frac{27}{5}\left(6^{k-1}-1\right) - 14\left(2^{2k-2}\right)\right] \\ &\leq 6^k\left(\frac{32}{15}3^k - \frac{21}{3}2^k\right) - \frac{194}{5}3^k. \end{aligned}$$

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

$$\begin{aligned} r_E(S_k^\gamma) &\leq r_E(2^{k-1}\left(3^k-2^k\right)S_{3,k}^\gamma) + r_E(2\times 3^k S_{6,k}^\gamma) \\ &\leq 2^{k-1}\left(3^k-2^k\right)r_E(S_{3,k}^\gamma) + 2\times 3^k r_E(S_{6,k}^\gamma) \\ &\leq 2^{k-1}\left(3^k-2^k\right)r_H(S_{3,k}^\gamma) + 2\times 3^k r_E(S_{6,k}^\gamma) \\ &\leq 8\times 6^{k-1}\left(3^k-2^k\right) + \frac{45}{2}\times 3^k\left[36\left(\frac{6^{k-1}-1}{5}\right) - 4\left(2^{k-1}-1\right)\right] \\ &\leq 3^k\left[\frac{85}{3}6^k - 2^k\left(\frac{4}{3}2^k + 45\right) - 72\right]. \end{aligned}$$

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

$$\begin{aligned} r_{CE}(S_k^\gamma) &\leq r_{CE}(2^{k-1}\left(3^k-2^k\right)S_{3,k}^\gamma) + r_{CE}(2\times 3^k S_{6,k}^\gamma) \\ &\leq 2^{k-1}\left(3^k-2^k\right)r_{CE}(S_{3,k}^\gamma) + 2\times 3^k r_{CE}(S_{6,k}^\gamma) \\ &\leq 2^{k-1}\left(3^k-2^k\right)r_H(S_{3,k}^\gamma) + 2\times 3^k r_{CE}(S_{6,k}^\gamma) \\ &\leq 8\times 6^{k-1}\left(3^k-2^k\right) + 2\times 5\times 3^k\left[36\left(\frac{6^{k-1}-1}{5}\right) - 4\left(2^{k-1}-1\right)\right] \\ &\leq 2^{k+2}\left(\frac{10}{3}3^{2k} - 5\times 3^k\right) - 3^k\left(\frac{2^{2k+2}}{3} - 32\right). \end{aligned}$$

□

5. Association Schemes for $\mathbb{Z}_6$-Simplex Codes of Types α, β and γ

As indicated by references [11, 15, 16], linear codes find application in the construction of association schemes. An association scheme characterized by d classes, defined on a set $\mathfrak{B}$, entails partitioning the Cartesian product $\mathfrak{B}\times\mathfrak{B}$ into $(d+1)$ distinct classes denoted as $\Sigma = \{\Sigma_0, \Sigma_1, \ldots, \Sigma_d\}$. These classes are subject to the following properties: The pair $(\mathfrak{B}, \Sigma)$ is called a d-class association scheme if

1. $\Sigma_0 = \{(x, x),\ x \in \mathfrak{B}\}$
2. $\mathfrak{B} \times \mathfrak{B}$ is a disjoint union of $\Sigma_0, \Sigma_1, \ldots, \Sigma_d$
3. For each integer $0 \le i \le d$, there exists an integer $0 \le j \le d$ such that $\Sigma_j = \Sigma_i^t$, where $\Sigma_i^t = \{(x, y),\ (y, x) \in \Sigma_i\}$
4. For any $0 \le i, j, k \le d$ and each pair $(x, y) \in \Sigma_k$, assuming that $p_{i,j}^k$ is an integer, then $|\{c \in \mathfrak{B}; (x, z) \in \Sigma_i, (z, y) \in \Sigma_j\}| = p_{i,j}^k$.

Remark 5.1. *[11] For $\mathfrak{B} = \mathbb{Z}_p^n$, define Σ_i as the set $\{(x, y) \in \mathbb{Z}_p^n \times \mathbb{Z}_p^n \mid d(x, y) = i\}$. The pair $(\mathbb{Z}_p^n, \Sigma)$ forms an i-class association scheme known as the Hamming association scheme.*

We have the following lemma that clarifies the relationship between linear codes and association schemes, highlighting their connection.

Lemma 5.2. *[15] Consider a linear code C over $\mathbb{Z}_p$ with nonzero weights w_1 and w_2. Let c_1 and c_2 be two linearly independent codewords of C such that $w(c_1) = w(c_2) = w_1$. For any $a, b \in \mathbb{Z}_p^*$, if $w(ac_1 + bc_2) = w_2$, then the restriction of the Hamming association scheme to C forms a i-class association scheme if and only if $w_2 \ne w_1 + i - 1$.*

While $\mathbb{Z}_3$ is a subset of $\mathbb{Z}_6$, every code defined over $\mathbb{Z}_3\mathbb{Z}_6$ extends naturally to being defined over $\mathbb{Z}_6$. Consequently, the following results hold true.

Theorem 5.3. *Let S_k^α and S_k^β are a linear code over the ring $\mathbb{Z}_6$. Then the restriction to S_k^α and S_k^β of the Hamming association scheme is a 3-class association scheme.*

Proof. By Lemma 5.2, if c_i, c_j be two codewords of S_k^α such that c_i, c_j, for $1 \le i \ne j \le 3^{k_0} \times 6^{k_1}$ are linear independent. According to [6, 12], we have $w(c_i) = w(c_j) = w_1$, for $1 \le i \ne j \le p^k$ and for any $a, b \in \mathbb{F}_p^*$ we have $w(ac_1 + bc_2) = w_2$, for $1 \le i \ne j \le 3^{k_0} \times 6^{k_1}$, where

$$w_1 \wedge w_2 = \begin{cases} 3 \times 6^{k-1} \ if \quad c_i, c_j \in S_k^\alpha, for\ 1 \le i \ne j \le 3^{k_0} \times 6^{k_1}, \\ 4 \times 6^{k-1} \ if \quad c_i, c_j \in S_k^\alpha, for\ 1 \le i \ne j \le 3^{k_0} \times 6^{k_1}, \\ 5 \times 6^{k-1} \ if \quad c_i, c_j \in S_k^\alpha, for\ 1 \le i \ne j \le 3^{k_0} \times 6^{k_1}. \end{cases}$$

It is clear that $w_2 \ne w_1 + 2$.

The proof for the code $\overset{\beta}{k}$ is obtained using a similar approach. □

Theorem 5.4. *Let S_k^γ is a linear code over the ring $\mathbb{Z}_6$. Then the restriction to S_k^γ of the Hamming association scheme is a 2-class association scheme.*

Proof. According to [6, 12] and Lemma 5.2, if c_i and c_j are two codewords of S_k^γ such that c_i and c_j, for $1 \le i \ne j \le p^k$, are linearly independent, then $w(c_i) = w(c_j) = w_1 = 3 \times 2^{k-2}[5 \times 3^{k-2} - 2^{k-2}]$ for $1 \le i \ne j \le p^k$, and for any $a, b \in \mathbb{F}_p^*$, we have $w(ac_i + bc_j) = w_2 = 3 \times 2^{k-2}[5 \times 3^{k-2} - 2^{k-2}]$ for $1 \le i \ne j \le p^k$. It is evident that $w_2 \ne w_1 + 1$. □

Example 5.5. *Let S_2^β be a linear code over $\mathbb{Z}_6$ with parameters* $[16, 2, 11]$, *generated by*

$$\mathfrak{G}^\beta = \begin{pmatrix} 1110111111022233 \\ 0121012345113512 \end{pmatrix}, \tag{15}$$

all codewords of S_2^β are given by

0000000000000000, 0121012345113512, 0242024024220424, 0303030303333330,
0424042042440242, 0545054321553154, 1110111111022233, 1231123450135145,
1352135135242051, 1413141414355503, 1534153153402415, 1055105432515321,
2220222222044400, 2341234501151312, 2402240240204224, 2523252525311130,
2044204204424042, 2105210543531554, 3330333333000033, 3451345012113545,
3512351351220451, 3033303030333303, 3154315315440215, 3215321054553121,
4440444444022200, 4501450123135112, 4022402402242024, 4143414141355530,
4204420420402442, 4325432105515354, 5550555555044433, 5011501234151345,
5132513513204251, 5253525252311103, 5314531531424015, 5435543210531521.

If, $c_1 = 0545054321553154$ and $c_2 = 1110111111022233$ are linear independent and $w(c_1) = w(c_2) = w_1 = 14$, $w(c_1 + c_2) = w_2 = 14$, we have $w(c_2) \neq w(c_1) + 2$, . Then, the restriction to S_2^β of the Hamming scheme is a 3-class association scheme.

Example 5.6. *Let S_3^γ be a linear code over $\mathbb{Z}_6$ with parameters* $[76, 3, 46]$, *generated by*

$$\begin{pmatrix} 1111111111111111111111111111111111110000000000222222222233333333334444444444 \\ 0000001111112222223333334444445555551111102341111102341111102341111110234 \\ 0123450123450123450123450123450123450123451111012345111101234511110123451111 \end{pmatrix},$$

some codewords of S_3^γ are given by

000000000000000000000000000000000000000000000000000000000000000000000000000000,
111111111111111111111111111111111110000000000222222222233333333334444444444,
000000111111222222333333444444555555111111023411111102341111110234111111023411111110234,
012345012345012345012345012345012345012345111101234511110123451111012345111101234511111,
123450123450123450123450123450123450012345111123450133333450124444450123555 5,
240240513513240240513513240240513513351351225213513500303513512252513513441 4,
351351024024351351024024351351024024351351225235135122520240245525351351251 2,

$$\vdots$$

531531420420315315204204153153042042531531421031531520542042041543153153043 2
543210432105321054210543105432054321543210532132105431052105432054105432154 3.

If,

$$c_1 = 2402405135132402405135132402405135133513512252135135003035135122525135134414$$

and

$$c_2 = 3513510240243513510240243513510240243513512252351351225202402455253513512252$$

are linear independent and $w(c_1) = w(c_2) = w_1 = 68$, $w(c_1 + c_2) = w_2 = 68$, we have $w(c_2) \neq w(c_1) + 1$. Then, the restriction to S_3^γ of the Hamming scheme is a 2-class association scheme.

6. MSSS Based on $\mathbb{Z}_3\mathbb{Z}_6$-Simplex Codes of Types α, β, and γ

In this section, we introduce a multi-secret sharing scheme that relies on linear codes and employs Blakley's method, as outlined in the work by Alahmadi et al. [1]. The steps for this multi-secret sharing scheme are as follows: Consider subcodes of codes S_k^{α}, S_k^{β} and S_k^{γ} denoted as $\widehat{S_k^{\alpha}}$, $\widehat{S_k^{\beta}}$, and $\widehat{S_k^{\gamma}}$ over $\mathbb{Z}_3\mathbb{Z}_6$ with a generator matrix $\widehat{\mathfrak{G}^{\alpha}}$, $\widehat{\mathfrak{G}^{\beta}}$, and $\widehat{\mathfrak{G}^{\gamma}}$ respectively. This approach builds upon the principles presented in [1], offering a robust framework for secret sharing through linear codes. By leveraging the properties of linear codes and Blakley's method, this scheme provides an effective means of securely distributing multiple secrets among authorized parties while ensuring confidentiality and integrity.

The secret distribution process occurs within the secret space denoted as $(\mathbb{Z}_3\mathbb{Z}_6)^n$, where each codeword represents a secret $s = (s_1, s_2, \ldots, s_n)$. Executed by the dealer, who possesses knowledge of the secret s, the share ω for a user with the associated codeword c is computed using the scalar product: $\omega = h_c(s) = c \cdot s^t$, where t indicates transposition. For secret recovery, a system is constructed involving the private secret s and the coalition corresponding to the rows of $\widehat{\mathfrak{G}^{\vartheta}}$, where $\vartheta \in \{\alpha, \beta, \gamma\}$. This system of equations is represented as $\widehat{\mathfrak{G}^{\vartheta}} \cdot s^t = \omega^t$, where $\omega = (\omega_1, \omega_2, \ldots, \omega_k)$, and ω_i represents the share linked to the i^{th} row of $\widehat{\mathfrak{G}^{\vartheta}}$, with $\vartheta \in \{\alpha, \beta, \gamma\}$. The solution set forms an affine space with the associated vector spaces $\widehat{S_k^{\alpha}}^{\perp}$, $\widehat{S_k^{\beta}}^{\perp}$, and $\widehat{S_k^{\gamma}}^{\perp}$. Assuming $\widehat{S_k^{\alpha}}$, $\widehat{S_k^{\beta}}$, and $\widehat{S_k^{\gamma}}$ are Linearly Complementary Dual, meaning

$$rank\left(\widehat{\mathfrak{G}^{\vartheta}}\right) = rank\left[\left(\widehat{\mathfrak{G}^{\vartheta}}\right)\left(\widehat{\mathfrak{G}^{\vartheta}}\right)^{\perp}\right] = rank\left[\left(\widehat{\mathfrak{G}^{\vartheta}}\right)^{\perp}\left(\widehat{\mathfrak{G}^{\vartheta}}\right)\right] \neq 0, \tag{16}$$

for $\vartheta \in \{\alpha, \beta, \gamma\}$, the system admits a unique solution within C. The secret retrieval involves solving the linear system:

$$\begin{cases} \widehat{\mathfrak{G}^{\vartheta}} \cdot s^t = \omega^t, & \vartheta \in \{\alpha, \beta, \gamma\} \\ H(\widehat{\mathfrak{G}^{\vartheta}}) \cdot s^t = 0, & \vartheta \in \{\alpha, \beta, \gamma\}, \end{cases} \tag{17}$$

where $H(\widehat{\mathfrak{G}^{\vartheta}})$ signifies the parity-check matrix of $\widehat{\mathfrak{G}^{\vartheta}}$.

6.1. Properties of the System and Information Pertaining to Coalitions

The proposed scheme's characteristics underscore its resilience and efficiency in multi-secret sharing. By harnessing the power of linear codes and Blakley's method, the scheme establishes a sturdy framework for secure information distribution. Particularly, parameters like $C = [n, M, d]$ shed light on the scheme's capacity for error detection and correction. Furthermore, information pertaining to potential coalitions is crucial for assessing the scheme's security implications. Understanding these aspects contributes to a comprehensive evaluation of the scheme's effectiveness and reliability in real-world applications.

Theorem 6.1. *The multi-secret sharing scheme yields the following insights:*

1. *The access structure comprises a M-tuple of codewords that exhibit linear independence.*
2. *A minimum of M elements are required to recover the secret.*

Theorem 6.2. *Consider C as an $C = [n, M, d]$-code over $\mathbb{Z}_3\mathbb{Z}_6$ with a generator matrix $\widehat{\mathfrak{G}^{\vartheta}}$, where $\vartheta \in \{\alpha, \beta, \gamma\}$. In a multi-secret-sharing scheme built upon C, the count of minimal coalitions is determined by:*

$$\frac{6^k \prod_{j=0}^{k-1} (6^k - 6^j)}{k!}. \tag{18}$$

6.2. Applications Examples

Example 6.3. *When $k = 2$, the generator matrix of $\widehat{S_2^{\alpha}}$ is provided as follows:*

$$\mathfrak{G}^{\alpha} = \begin{bmatrix} 10111111333333555555 \\ 01012345012345012345 \end{bmatrix}. \tag{19}$$

Following Equation 16, we have

$$rank\left(\widehat{\mathfrak{G}^{\alpha}}\right) = rank\left[\left(\widehat{\mathfrak{G}^{\alpha}}\right)\left(\widehat{\mathfrak{G}^{\alpha}}\right)^{\perp}\right] = rank\left[\left(\widehat{\mathfrak{G}^{\alpha}}\right)^{\perp}\left(\widehat{\mathfrak{G}^{\alpha}}\right)\right] = 2 \neq 0. \tag{20}$$

If $s = (45432105054321210543)$ belongs to $\widehat{S_2^{\alpha}}$, we authenticate a multi-secret-sharing framework using Equation 17. This entails computing the shares according to $\widehat{S_2^{\alpha}}$ as described below:

$$\varpi = (12), \tag{21}$$

let $s = (s_1s_2s_3s_4s_5s_6s_7s_8s_9s_{10}s_{11}s_{12}s_{13}s_{14}s_{15}s_{16}s_{17}s_{18}s_{19}s_{20}) \in \widehat{S_2^{\alpha}}$. After closely examining the system of equations presented in Equation 17, we deduce:

$$\begin{pmatrix} 10111111333333555555 \\ 01012345012345012345 \\ 10000000000000000052 \\ 01000000000000000015 \\ 00100000000000000052 \\ 00010000000000000001 \\ 00001000000000000010 \\ 00000100000000000025 \\ 00000010000000000034 \\ 00000001000000000043 \\ 00000000100000000030 \\ 00000000010000000045 \\ 00000000001000000054 \\ 00000000000100000003 \\ 00000000000010000012 \\ 00000000000001000021 \\ 00000000000000100014 \\ 00000000000000010023 \\ 00000000000000001032 \\ 00000000000000000141 \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \\ s_5 \\ s_6 \\ s_7 \\ s_8 \\ s_9 \\ s_{10} \\ s_{11} \\ s_{12} \\ s_{13} \\ s_{14} \\ s_{15} \\ s_{16} \\ s_{17} \\ s_{18} \\ s_{19} \\ s_{20} \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \tag{22}$$

A unique solution exists for the system of equations, yielding $s = (45432105054321210543)$. Additionally, the count of minimal coalitions is 18900.

Example 6.4. *For $k = 4$, the generator matrix of $\widehat{S_4^{\gamma}}$ is presented as follows:*

$$\mathfrak{G}^{\gamma} = \begin{bmatrix} 33333333333333333333333333333333333333333333333333 \\ 11111111110000000000222222222233333333334444444444 \\ 11111102341111102341111102341111102341111110234 \\ 01234511101234511101234511101234511101234511111 \end{bmatrix}. \tag{23}$$

Following Equation 16, we have

$$rank\left(\widehat{\mathfrak{G}^{\alpha}}\right) = rank\left[\left(\widehat{\mathfrak{G}^{\alpha}}\right)\left(\widehat{\mathfrak{G}^{\alpha}}\right)^{\perp}\right] = rank\left[\left(\widehat{\mathfrak{G}^{\alpha}}\right)^{\perp}\left(\widehat{\mathfrak{G}^{\alpha}}\right)\right] = 4 \neq 0. \tag{24}$$

Should the vector $s = (21054344140543212252432105003005432122522105434414)$ *be a member of the code* $\widehat{S_4^{\gamma}}$*, we proceed to authenticate a multi-secret-sharing framework using Equation 17. This process involves computing shares in accordance with* $\widehat{S_4^{\gamma}}$ *as delineated below:*

$$\varpi = (0204),$$

Consider

$$s = (s_1s_2s_3s_4s_5s_6s_7s_8s_9s_{10}s_{11}s_{12}s_{13}s_{14}s_{15}s_{16}s_{17}s_{18}s_{19}s_{20}s_{21}s_{22}s_{23}s_{24}s_{25}s_{26}s_{27}s_{28}s_{29}s_{30}s_{31}s_{32}$$
$$s_{33}s_{34}s_{35}s_{36}s_{37}s_{38}s_{39}s_{40}s_{41}s_{42}s_{43}s_{44}s_{45}s_{46}s_{47}s_{48}s_{49}s_{50}) \in \widehat{S_4^{\gamma}}.$$

Upon thorough analysis of the equations outlined in Equation 17, we infer:

$$\begin{pmatrix}
33333333333333333333333333333333333333333333333333\\
11111111110000000000222222222233333333334444444444\\
11111102341111110234111111023411111102341111110234\\
01234511110123451111012345111101234511110123451111\\
10000000000000000000000000000000000000010000100043\\
01000000000000000000000000000000000000010000020015\\
00100000000000000000000000000000000000010000110015\\
00010000000000000000000000000000000000010000000011\\
00001000000000000000000000000000000000010000120041\\
00000100000000000000000000000000000000010000010043\\
00000010000000000000000000000000000000010000020000\\
00000001000000000000000000000000000000010000020024\\
00000000100000000000000000000000000000010000020033\\
00000000010000000000000000000000000000010000020042\\
00000000001000000000000000000000000000000000100044\\
00000000000100000000000000000000000000000000020010\\
00000000000010000000000000000000000000000000110010\\
00000000000001000000000000000000000000000000000012\\
00000000000000100000000000000000000000000000120042\\
00000000000000010000000000000000000000000000010044\\
00000000000000001000000000000000000000000000020001\\
00000000000000000100000000000000000000000000020025\\
00000000000000000010000000000000000000000000020034\\
00000000000000000001000000000000000000000000020043\\
00000000000000000000100000000000000000000000120022\\
00000000000000000000010000000000000000000000010024\\
00000000000000000000001000000000000000000000100024\\
00000000000000000000000100000000000000000000020050\\
00000000000000000000000010000000000000000000110050\\
00000000000000000000000001000000000000000000000052\\
00000000000000000000000000100000000000000000010015\\
00000000000000000000000000010000000000000000010033\\
00000000000000000000000000001000000000000000010042\\
00000000000000000000000000000100000000000000010051\\
00000000000000000000000000000010000000010000120021\\
00000000000000000000000000000001000000010000010023\\
00000000000000000000000000000000100000010000100023\\
00000000000000000000000000000000010000010000020055\\
00000000000000000000000000000000001000010000110055\\
00000000000000000000000000000000000100010000000051\\
00000000000000000000000000000000000010010000010014\\
00000000000000000000000000000000000001010000010032\\
00000000000000000000000000000000000000110000010041\\
00000000000000000000000000000000000000020000010050\\
00000000000000000000000000000000000000001000110030\\
00000000000000000000000000000000000000000100000032\\
00000000000000000000000000000000000000000010120002\\
00000000000000000000000000000000000000000001010004\\
00000000000000000000000000000000000000000000001023\\
00000000000000000000000000000000000000000000000141
\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_{40}\\ s_{41}\\ s_{42}\\ s_{43}\\ s_{44}\\ s_{45}\\ s_{46}\\ s_{47}\\ s_{48}\\ s_{49}\\ s_{50}
\end{pmatrix}
=
\begin{pmatrix}
0\\ 2\\ 0\\ 4\\ 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} \qquad (25)$$

The system of equations admits a solitary solution, resulting in

$$s = (21054344140543212252432105003005432122522105434414).$$

Furthermore, the tally of minimal coalitions amounts to 171400800.

The importance of applying the covering radius of $\mathbb{Z}_3\mathbb{Z}_6$-Simplex Codes of types α, β, and γ, association schemes for $\mathbb{Z}_6$-Simplex Codes of the same types, and the multi-secret sharing scheme based on these codes lies in their collective ability to ensure reliability, efficiency, and security in various communication and information sharing scenarios. The covering radius serves as a fundamental measure of the error-correction capabilities of these codes, providing crucial insights into their robustness against noise and interference in communication channels. By accurately assessing the maximum distance between codewords, it enables the design and evaluation of codes optimized for specific error-correction requirements, thus enhancing the overall performance of communication systems. Association schemes complement this by offering a

structured framework for analyzing the relationships and symmetries within the codes, facilitating the development of efficient encoding and decoding algorithms tailored to exploit these properties. Moreover, association schemes aid in identifying subsets of codewords with desirable properties, which can further optimize error-correction performance and decoding efficiency. Additionally, the multi-secret sharing scheme based on $\mathbb{Z}_3\mathbb{Z}_6$-Simplex Codes of types α, β, and γ leverages their inherent error-correction capabilities and algebraic structure to securely distribute multiple secrets among participants while ensuring confidentiality and resilience against eavesdropping and malicious attacks. By integrating these concepts and techniques, communication systems can achieve enhanced reliability, efficiency, and security, thereby addressing the diverse needs of modern information exchange and storage applications.

7. Conclusion

In conclusion, this article has explored the properties and applications of simplex codes of types α, β, and γ over the ring $\mathbb{Z}_3\mathbb{Z}_6$. It has investigated various aspects including the covering radius of these codes, association schemes for $\mathbb{Z}_6$-simplex codes, and a multi-secret sharing scheme based on them. The analysis of the covering radius provides insights into the error-correcting capabilities of these codes, crucial for their practical implementation in communication systems. Understanding association schemes for $\mathbb{Z}_6$-simplex codes aids in constructing efficient encoding and decoding algorithms, enhancing their performance in various applications. Moreover, the development of a multi-secret sharing scheme demonstrates the versatility and security potential of these codes beyond traditional error correction. By leveraging the algebraic structure of $\mathbb{Z}_3\mathbb{Z}_6$-simplex codes, novel cryptographic primitives can be designed for secure multi-party communication and data storage. Overall, the study of simplex codes over $\mathbb{Z}_3\mathbb{Z}_6$ offers valuable contributions to both theoretical coding theory and practical cryptography, paving the way for advanced communication systems and secure information exchange protocols.

References

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

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

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

[4] K. Chatouh, K. Guenda, T.A. Gulliver, L. Noui, On some classes of linear codes over $\mathbb{Z}_2\mathbb{Z}_4$ and their covering radii, J. Appl. Math. Comput., **53**(1) (2017), 201-222.

[5] K. Chatouh, L. Noui, M. Bin Mamat, Codes over and their covering radii, J. Algebra Number Theory Appl., **16**(1) (2016), 25-39.

[6] K. Chatouh, Some codes over $\mathcal{R} = \mathcal{R}_1\mathcal{R}_2\mathcal{R}_3$ and their applications in secret sharing schemes, Afr. Mat., **35** (2024), 1, https://doi.org/10.1007/s13370-023-01143-8

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

[8] K. Chatouh, K. Guenda, T.A. Gulliver, New Classes of Codes Over $R_{q,p,m} = \mathbb{Z}_{p^m}[u_1, u_2, \cdots, u_q]/\left\langle u_i^2 = 0, u_iu_j = u_ju_i \right\rangle$ and Their Applications, Comp. Appl. Math., **39**(3) (2020), 152.

[9] G.D. Cohen, M.G. Karpovsky, H.F. Mattson, J.R. Schatz, Covering radius-Survey and recent results, IEEE Trans. Inf. Theory., **31**(3) (1985), 328–343.

[10] M. Cruz, C. Durairajan, P. Solé, On the covering radius of codes over $\mathbb{Z}_{p^k}$, Mathematics **8** (2020), 328.

[11] P. Delsarte, An algebraic approach to the association schemes of coding theory, Philips Res. Rep. Suppl., **10** (1973), 97.

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

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

[14] A. Melakhessou, K. Chatouh, and K. Guenda, DNA multi-secret sharing schemes based on linear codes over $\mathbb{Z}_4 \times R$, J. Appl. Math. Comput., **96**(6) (2023), 4833-4853.

[15] G. Luo, X. Cao, G. Xu, S. Xu, A new class of optimal linear codes with flexible parameters, Discr. Appl. Math., **237** (2018), 126-131.

[16] Y. Wang, J. Gao, MacDonald codes over the ring $\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p$, Comp. Appl. Math., **38** (2019), 1-15.