Montes Taurus J. Pure Appl. Math. 8 (1), 47–62, 2026

Montes Taurus Journal of Pure and Applied Mathematics

https://www.mtjpamjournal.com

MTJPAM
ISSN: 2687-4814

Exploring minimal linear codes defined over $\mathfrak{R}$ and their application in secret sharing and multi-secret sharing schemes

Karima Chatouh [a]

[a] *Laboratoire D´applications des Mathématiques à L´informatique et à L´électronique Faculty of Economic, Commercial and Management Sciences University of Batna 1, Batna, Algeria*

Abstract

This study explores the development of minimal linear codes over the ring $\mathfrak{R}$, with their potential applications in cryptographic systems. Motivated by the need for efficient and secure information distribution mechanisms, we construct new classes of linear codes whose Gray images over $\mathbb{Z}_7$ exhibit minimality. Our approach leverages algebraic structures such as simplex and MacDonald codes defined over $\mathfrak{R}$, and we examine their weight distributions to establish sufficient conditions for minimality. These minimal codes serve to design secret and multi-secret sharing schemes, demonstrating substantial access control and security properties. The schemes are analyzed for their robustness and practicality in various cryptographic settings, offering insights into the effective use of linear code theory in secure communications.

Keywords: Minimal linear codes, secret sharing schemes, multi-secret-sharing schemes, simplex and Macdonald codes, minimal access sets

2020 MSC: 11Txx, 11T71, 14G50, 15Axx, 15B33

1. Introduction

Linear codes over finite rings contribute significantly to various fields, such as information theory, cryptography, and error correction (*cf.* [3], [8]-[10]). This study focuses on the algebraic properties and applications of minimal linear codes defined over the ring $\mathfrak{R} = \mathbb{Z}_7\mathcal{A}_7\mathcal{R}_7$, specifically their use in secret-sharing and multi-secret-sharing schemes (*cf.* [1], [4]-[6], [11, 14]). These codes, characterized by distinct algebraic properties, form the backbone of secure cryptographic constructions, enabling efficient and secure information distribution (*cf.* [12]).

The motivation for exploring minimal linear codes arises from their ability to support cryptographic protocols where confidentiality and integrity are paramount (*cf.* [15]). We investigate their application in secret-sharing schemes, where a secret is divided into shares distributed to participants, and only authorized subsets can reconstruct the original secret (*cf.* [3]). Furthermore, we extend these concepts to multi-secret-sharing schemes, where multiple secrets are distributed simultaneously, ensuring enhanced security (*cf.* [1, 15]).

This paper examines the Gray images of simplex and MacDonald codes over $\mathfrak{R} = \mathbb{Z}_7\mathcal{A}_7\mathcal{R}_7$ and presents their properties, weight distributions, and minimality (*cf.* [5, 7, 8]). Through these explorations, we aim to advance the understanding of the practical implications of minimal linear codes in cryptography, addressing challenges such as computational complexity, error correction, and resilience against cryptographic attacks (*cf.* [11, 12]).

†*Article ID:* MTJPAM-D-23-00059

Email address: karima.chatouh@univ-batna.dz (Karima Chatouh)

Received:17 December 2023, Accepted:4 August 2025, Published:5 March 2026

⋆*Corresponding Author:* Karima Chatouh

The subsequent sections of the paper are described in the following manner: Section 2 encompasses the fundamental properties utilized throughout our manuscript. In Section 3, we introduce simplex and MacDonald codes over $\mathfrak{R} = \mathbb{Z}_7\mathcal{A}_7\mathcal{R}_7$, where $\mathcal{A}_7 = \mathbb{Z}_7 + u\mathbb{Z}_7$ and $\mathcal{R}_7 = \mathbb{Z}_7 + v\mathbb{Z}_7 + w\mathbb{Z}_7 + vw\mathbb{Z}_7$. We thoroughly investigate the properties of these codes, focusing specifically on the Gray images of simplex and MacDonald codes over the ring $\mathfrak{R}$. Additionally, we compute the weight distributions of these Gray images. Furthermore, we introduce minimal linear codes over $\mathbb{Z}_7$. Section 4 is dedicated to the examination of properties and applications of secret sharing and multi-secret sharing schemes based on minimal linear codes over $\mathbb{Z}_7$.

2. Some background and preliminaries

In this section, we outline our approach to substantiate the presented results. First, we provide an exposition of the properties of the ring $\mathfrak{R}$. Following that, we establish a Gray map and elucidate the Gray images of linear codes over $\mathfrak{R}$. Additionally, we expound upon the methodology employed for computing secret-sharing schemes utilizing linear codes defined over this ring.

The ring $\mathfrak{R} = \{c = (\lambda, \mu, \nu) \ | \lambda \in \mathbb{Z}_7,\ \mu \in \mathcal{A}_7 = \mathbb{Z}_7 + u\mathbb{Z}_7, \nu \in \mathcal{R}_7 = \mathbb{Z}_7 + v\mathbb{Z}_7 + w\mathbb{Z}_7 + vw\mathbb{Z}_7\}$, is defined as the direct product $\mathfrak{R} = \mathbb{Z}_7 \times \mathcal{A}_7 \times \mathcal{R}_7$, where each component has a specific algebraic structure. The first component, $\mathbb{Z}_7$, is the finite field consisting of the integers modulo 7, i.e., $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$. The second component, $\mathcal{A}_7$, is the ring $\mathbb{Z}_7 + u\mathbb{Z}_7$, where u is a nilpotent element satisfying $u^2 = 0$. Each element in $\mathcal{A}_7$ is expressed as $a + ub$, with $a, b \in \mathbb{Z}_7$, giving $\mathcal{A}_7$ a total of 49 elements. The third component, $\mathcal{R}_7$, is defined as $\mathbb{Z}_7 + v\mathbb{Z}_7 + w\mathbb{Z}_7 + vw\mathbb{Z}_7$, where v and w are a nilpotents elements satisfying $v^2 = w^2 = 0$ and $vw = wv$. Elements of $\mathcal{R}_7$ take the form $a + vb + wc + vwd$, with $a, b, c, d \in \mathbb{Z}_7$, so $\mathcal{R}_7$ contains $7^4 = 2401$ elements.

Thus, each element of $\mathfrak{R}$ is an ordered triple $\varsigma = (\eta_1, \eta_2, \eta_3)$, where $\eta_1 \in \mathbb{Z}_7$, $\eta_2 \in \mathcal{A}_7$, and $\eta_3 \in \mathcal{R}_7$. The total number of elements in $\mathfrak{R}$ is therefore $|\mathfrak{R}| = 7 \times 49 \times 2401 = 7^7$, where $\times$ denotes the classical multiplication. An example of an element in $\mathfrak{R}$ is $(3, 2 + 4u, 1 + 2v + 5w + 6vw)$.

It is established that $\mathbb{Z}_7$ is a subring of $\mathcal{A}_7$, and $\mathcal{A}_7$ is a subring of $\mathcal{R}_7$. A code C is considered a $\mathbb{Z}_7\mathcal{A}_7\mathcal{R}_7$-additive code if it is a subgroup of $\mathbb{Z}_7^{\gamma}\mathcal{A}_7^{\delta_1}\mathcal{R}_7^{\delta_2}$. Specifically, a code C is termed separable when it is the direct product of C_γ, C_{δ_1}, and C_{δ_2}, denoted as $C = C_\gamma \times C_{\delta_1} \times C_{\delta_2}$. The Lee weight of an element $c = (\lambda, \mu, \nu) \in \mathfrak{R} = \mathbb{Z}_7\mathcal{A}_7\mathcal{R}_7$ is then defined as

$$w_{Lee}\left((\lambda, \mu, \nu)\right) = w_{Lee}(\lambda) + w_{Lee}(\mu) + wt_{Lee}(\nu).$$

2.1. A Gray map and Gray images

We will establish the Gray map and formulate the weight function. To guarantee a distance-preserving isometry. The Gray map is defined as

$$\begin{array}{rccc} \Phi & : & \mathbb{Z}_7\mathcal{A}_7\mathcal{R}_7 & \to & \mathbb{Z}_7^7 \\ & & (\lambda, \mu, \nu) & \mapsto & \Phi\left(\lambda, \mu, \nu\right), \end{array} \tag{2.1}$$

where

$$\Phi\left(\lambda, \mu, \nu\right) = \left(\lambda, \mu_0, \mu_0 + \mu_1, \nu_4, \nu_2 + \nu_4, \nu_3 + \nu_4, \nu_1 + \nu_2 + \nu_3 + \nu_4\right),$$

with $\mu = \mu_0 + u\mu_1 \in \mathcal{A}_7 = \mathbb{Z}_7 + u\mathbb{Z}_7$ and $\nu = \nu_1 + v\nu_2 + w\nu_3 + vw\nu_4 \in \mathcal{R}_7 = \mathbb{Z}_7 + v\mathbb{Z}_7 + w\mathbb{Z}_7 + vw\mathbb{Z}_7$, where $u^2 = v^2 = w^2 = 0$ and all variables commute. Each element of the ring $\mathfrak{R} = \mathbb{Z}_7\mathcal{A}_7\mathcal{R}_7$ is therefore of the form (λ, μ, ν). If we extend the map Φ component-wise to the entire space $\mathbb{Z}_7^{\gamma} \times \mathcal{A}_7^{\delta_1} \times \mathcal{R}_7^{\delta_2}$, then Φ becomes a map into $\mathbb{Z}_7^n$, where $n = \gamma + 2\delta_1 + 4\delta_2$. We now prove that this Gray map Φ is a linear isometry. Linearity of Φ follows from the fact that the operations in all components are performed over the field $\mathbb{Z}_7$ and that Φ is defined using linear combinations of the individual coefficients of μ and ν. That is, for any $x, y \in \mathfrak{R}$ and $a \in \mathbb{Z}_7$, we have $\Phi(x + y) = \Phi(x) + \Phi(y)$ and $\Phi(ax) = a\Phi(x)$. Furthermore, the Lee weight on $\mathfrak{R}$ is defined as $w_{\mathrm{Lee}}(\lambda, \mu, \nu) = w_{\mathrm{Lee}}(\lambda) + w_{\mathrm{Lee}}(\mu) + w_{\mathrm{Lee}}(\nu)$, where each weight counts the number of nonzero components in the $\mathbb{Z}_7$ expansion of λ, μ, and ν. Because the map Φ sends each of these components to separate coordinates in $\mathbb{Z}_7^7$, the Lee weight of (λ, μ, ν) is equal to the Hamming weight of $\Phi(\lambda, \mu, \nu)$. That is, $w_{\mathrm{Lee}}(\lambda, \mu, \nu) = w_H(\Phi(\lambda, \mu, \nu))$. Therefore, Φ is a distance-preserving map and hence a linear isometry from $\mathfrak{R}^n$ to $\mathbb{Z}_7^{7n}$.

Theorem 2.1. *If C represents a linear code over $\mathfrak{R} = \mathbb{Z}_7\mathcal{A}_7\mathcal{R}_7$ with length n and a minimum Lee weight d, then $\Phi(C)$ forms a linear code characterized by parameters $[7n, k, d_{Lee} = d_H]$.*

Example 2.2. Consider the element $c \in \mathbb{Z}_7^5 \times \mathcal{A}_7^3 \times \mathcal{R}_7^2$, where

$$c = (1, 5, 4, 2, 0, 5 + 2u, 1 + 3u, u, 3 + 5v + w + 6vw, 5 + 2v + 3w + 2vw).$$

In alignment with the expression in Equation (2.1), we obtain:

$$\Phi(c) = 1542050140164012455.$$

2.2. Minimal linear codes

The conditions guaranteeing the minimality of a linear code are precisely defined in the following lemma, which outlines sufficient weight-related criteria. This lemma serves as a valuable guide, clearly specifying the conditions that, once satisfied, ensure the minimality of the given linear code.

Lemma 2.3 (*cf.* [11])**.** *Let C be an $[n, k, p]$ linear code over $\mathbb{F}_p$, and let w_{min} and w_{max} be the minimum and maximum nonzero weights of C, respectively. If*

$$\frac{w_{min}}{w_{max}} \geqslant \frac{p-1}{p},$$

then all nonzero codewords of C are minimal.

To determine the minimal access sets, we necessitate the concept of minimal codewords.

Definition 2.4 (*cf.* [11])**.** The support of a codeword $c = (c_0, c_1, \cdots, c_{n-1}) \in \mathbb{Z}_q^n$ is defined as

$$supp(c) = \{0 \leqslant i \leqslant n-1; c_i \neq 0\}.$$

Let c_1 and c_2 be two codewords of the code C. We say that c_1 covers c_2 if

$$supp(c_2) \subseteq supp(c_1).$$

Remark 2.5. A nonzero codeword c belonging to the code C is termed minimal if the only codewords that contain it are scalar multiples of c.

Consider a systematic code $C[n, k, d]$ capable of correcting $t = \lfloor \frac{d-1}{2} \rfloor$ errors, where its generator matrix takes the form $G = [I_k|A]$. In this case, the parity-check matrix is given by $H = [-A^t|I_{n-k}]$. Such a code proves useful in constructing secret-sharing schemes.

2.3. Secret sharing schemes based on linear codes

Consider a dealer P_0 who wishes to securely distribute a secret $s \in \mathbb{F}_p$ among a set of $n-1$ participants denoted by $P = \{P_1, P_2, \ldots, P_{n-1}\}$. Let $\mathfrak{A}_p$ represent the collection of all possible access structures, i.e., subsets of participants authorized to reconstruct the secret. The secret-sharing scheme is based on a linear code C over the finite field $\mathbb{F}_p$ with a generator matrix $G = [g_0 \mid g_1 \mid \cdots \mid g_{n-1}]$, where each $g_i \in \mathbb{F}_p^k$ is a column vector.

To distribute the secret, the dealer randomly selects an information vector $u = (u_0, u_1, \ldots, u_{k-1}) \in \mathbb{F}_p^k$ such that the inner product of u with the first column of G, denoted g_0, yields the secret: $s = ug_0$. Since there are p^{k-1} such vectors $u \in \mathbb{F}_p^k$ satisfying this constraint, the scheme ensures randomness in share generation while keeping s fixed.

The codeword corresponding to the chosen vector u is computed as $v = uG = (v_0, v_1, \ldots, v_{n-1})$, a vector in $\mathbb{F}_p^n$. Each share v_i is then distributed to participant P_i for $1 \leq i \leq n-1$, while the component $v_0 = s$ represents the secret.

Reconstructing the secret is possible only by those subsets of participants whose associated columns in the generator matrix can linearly generate g_0. Specifically, a subset of participants

$$\{P_{i_1}, P_{i_2}, \ldots, P_{i_m}\} \subset P$$

forms a qualified set if the column g_0 can be expressed as a linear combination of their corresponding columns:

$$g_0 = \sum_{j=1}^{m} \eta_j g_{i_j}, \quad \eta_j \in \mathbb{F}_p.$$

Under this condition, the secret s can be recovered from the associated shares using the same linear combination:

$$s = \sum_{j=1}^{m} \eta_j v_{i_j}.$$

The reconstruction process is deterministic and guaranteed by the linearity of the code, ensuring that only qualified access sets can recover from the secret unauthorized subsets and obtain no information about s. This coding-theoretic framework provides efficiency and security and forms the foundation for the secret-sharing schemes developed in this work.

3. Linear simplex and MacDonald codes over $\mathfrak{R}$

In this section, we embark on the development of various constructions for linear codes over $\mathfrak{R}$. These constructions hold significant importance in the context of implementing secret sharing schemes. As delineated in [5, 7, 8], it becomes imperative to define the following concepts, setting the groundwork for the subsequent exploration of linear codes and their applications in secure information sharing.

Definition 3.1. The generator matrix of $\mathcal{S}_k^{\alpha}$, simplex codes of type α over $\mathfrak{R}$, as the concatenation of 7^{6k} copies of the generator matrix of $S^{\alpha}_{\mathbb{Z}_7,k}$, 7^{5k} copies of the generator matrix of $S^{\alpha}_{\mathcal{A}_7,k}$ and 7^{3k} copies of the generator matrix of $S^{\alpha}_{\mathcal{R}_7,k}$ is given by

$$\Omega_k^{\alpha} = \left[\; 1_{7^{6k}} \otimes G^{\alpha}_{\mathbb{Z}_7,k} \;\middle|\; 1_{7^{5k}} \otimes G^{\alpha}_{\mathcal{A}_7,k} \;\middle|\; 1_{7^{3k}} \otimes G^{\alpha}_{\mathcal{R}_7,k} \; \right], \quad \text{for } k \geq 1. \tag{3.1}$$

Definition 3.2. The generator matrix of $\mathcal{S}_k^{\beta}$ is the concatenation of 7^{k+1} copies of the generator matrix of $S^{\beta}_{\mathbb{Z}_7,k}$, 7^k copies of the generator matrix of $S^{\beta}_{\mathcal{A}_7,k}$ and 7^{k-1} copies of the generator matrix of $S^{\beta}_{\mathcal{R}_7,k}$ given by

$$\Omega_k^{\beta} = \left[\; 1_{7^{k+1}} \otimes G^{\beta}_{\mathbb{Z}_7,k} \;\middle|\; 1_{7^{k}} \otimes G^{\beta}_{\mathcal{A}_7,k} \;\middle|\; 1_{7^{k-1}} \otimes G^{\beta}_{\mathcal{R}_7,k} \; \right], \quad \text{for } k \geq 2. \tag{3.2}$$

These findings result in the following implications.

(i) The simplex codes $\mathcal{S}_k^{\alpha}$ is of length $n = 3 \times 7^{7k}$, and distance minimal $d = 6\left(7^{k-1} + 2 \times 7^{2(k-1)} + 4 \times 7^{4(k-1)}\right)$.

(ii) The simplex codes $\mathcal{S}_k^{\beta}$ is of length $n = \left(\dfrac{7^k - 1}{6}\right)\left[7^{k+1} + 7^{2k-1} + 7^{4(k-1)}\right]$, and distance minimal

$$d = 6\left(7^{k-1} + 2 \times 7^{2(k-1)} + 4 \times 7^{4(k-1)}\right).$$

Presently, we introduce the following definition pertaining to linear MacDonald codes over $\mathfrak{R}$.

Definition 3.3. The MacDonald code $\mathcal{M}_{k,t}^{\alpha}$ is a linear code over $\mathfrak{R}$ of length

$$n = 3 \times 7^{7k} - \left(7^{6k+t} + 7^{5k+2t} + 7^{3k+4t}\right) \tag{3.3}$$

generated by, for $k > 1$ and $1 \leq t \leq k-1$,

$$\Omega_{k,t}^{\alpha} = \left[\; 1_{7^{6k}} \otimes G^{\alpha}_{\mathbb{Z}_7,k,t} \;\middle|\; 1_{7^{5k}} \otimes G^{\alpha}_{\mathcal{A}_7,k,t} \;\middle|\; 1_{7^{3k}} \otimes G^{\alpha}_{\mathcal{R}_7,k,t} \; \right] \tag{3.4}$$

and the MacDonald code $\mathcal{M}_{k,t}^{\beta}$ is a linear code over $\mathfrak{R}$ of length

$$n = \left(\frac{7^k}{6}\right)\left[\left(7^k - 1\right)\left(7 + 7^{k-1} + 7^{3k-4}\right) - \left(7^t - 1\right)\left(7 + 7^{t-1} + 7^{3t-4}\right)\right] \tag{3.5}$$

generated by

$$\Omega_{k,t}^{\beta} = \left[\; 1_{7^{k+1}} \otimes G^{\beta}_{\mathbb{Z}_7,k,t} \;\middle|\; 1_{p^{k}} \otimes G^{\beta}_{\mathcal{A}_7,k,t} \;\middle|\; 1_{7^{k-1}} \otimes G^{\beta}_{\mathcal{R}_7,k,t} \; \right]. \tag{3.6}$$

3.1. Gray images of simplex and MacDonald codes over $\Re$

Our initial discovery centers around the identification of the Gray images for simplex and MacDonald codes over $\mathbb{Z}_7$. This accomplishment is underpinned by the construction of linear simplex and MacDonald codes over $\Re$.

Theorem 3.4. *Let $\mathcal{S}_k^\alpha$ be a $\Re$-simplex code of type α with minimum Lee weight d_L. Then $\Phi(\mathcal{S}_k^\alpha)$ is a simplex code over $\mathbb{Z}_7$ with parameters*

$$\left[7^{7k+1}; k\right]. \tag{3.7}$$

Proof. The code $\mathcal{S}_k^\alpha$ is constructed over the ring $\Re = \mathbb{Z}_7\mathcal{A}_7\mathcal{R}_7$ as a concatenation of generator matrices over its component subrings. The Gray map $\Phi : \Re \to \mathbb{Z}_7^7$ is an isometry with respect to the Lee weight on $\Re$ and the Hamming weight on $\mathbb{Z}_7$. Applying Φ to each codeword in $\mathcal{S}_k^\alpha$, we obtain a linear code $\Phi(S_k^\alpha) \subseteq \mathbb{Z}_7^n$, where $n = 7\times\text{length}(\mathcal{S}_k^\alpha)$. The structure of the generator matrix ensures that $\Phi(\mathcal{S}_k^\alpha)$ spans a subspace of dimension k, and the distance is preserved due to the isometric property. Therefore, $\Phi(\mathcal{S}_k^\alpha)$ is a simplex code over $\mathbb{Z}_7$ with parameters $\left[7^{k+1}, k\right]$. □

Theorem 3.5. *Let $\mathcal{S}_k^\beta$ be a $\Re$-simplex code of type β with minimum Lee weight d_L. Then $\Phi(\mathcal{S}_k^\beta)$ is a simplex code over $\mathbb{Z}_7$ with parameters*

$$\left[\frac{7}{18}\left(7^k - 1\right)\left[7^{k+1} + 7^{2k-1} + 7^{4(k-1)}\right]; k\right]. \tag{3.8}$$

Proof. The generator matrix Ω_k^β of S_k^β over $\Re$ is formed by repeating generators over $\mathbb{Z}_7$, $\mathcal{A}_7$, and $\mathcal{R}_7$ according to the weight distribution scheme:

$$\Omega_k^\beta = \left[\ 1_{7^{k+1}} \otimes G^\beta_{\mathbb{Z}_7,k} \ \middle|\ 1_{7^k} \otimes G^\beta_{\mathcal{A}_7,k} \ \middle|\ 1_{7^{k-1}} \otimes G^\beta_{\mathcal{R}_7,k}\ \right], \quad \text{for } k \geq 2.$$

Each element is mapped under Φ to 7 coordinates in $\mathbb{Z}_7$, and the resulting image is a linear code. Since the components are linearly independent and the map preserves the Lee weight, the Gray image has the expected parameters calculated from the construction. Hence, $\Phi\left(S_k^\beta\right)$ is a simplex code over $\mathbb{Z}_7$ with the claimed parameters. □

Theorem 3.6. *Let $\mathcal{M}_{k,t}^\alpha$ be a $\Re$-MacDonald code of type α and minimum Lee weight d_L. Then $\Phi(\mathcal{M}_{k,t}^\alpha)$ is a MacDonald code over $\mathbb{Z}_7$, with parameters*

$$\left[\left(7^k + 2\times 7^{2k} + 4\times 7^{4k}\right) - \left(p^t + 2p^{2t} + 4\times 7^{4t}\right); k\right]. \tag{3.9}$$

Proof. The MacDonald code $\mathcal{M}_{k,t}^\alpha$ is constructed by removing rows corresponding to lower-order subcodes from a simplex code. The generator matrix $\Omega_{k,t}^\alpha$ is a reduced form of Ω_k^α. As in the simplex case, the Gray map Φ acts as a linear isometry, ensuring that the weight distribution of $\mathcal{M}_{k,t}^\alpha$ is preserved under mapping. Since the structure of the generator matrix directly determines the dimension and length of the image, and minimality is preserved, $\Phi(\mathcal{M}_{k,t}^\alpha)$ is a MacDonald code over $\mathbb{Z}_7$ with the stated parameters. □

Theorem 3.7. *Let $\mathcal{M}_{k,t}^\beta$ be a $\Re$ MacDonald code of type α and minimum Lee weight d_L. Then $\Phi(\mathcal{M}_{k,t}^\beta)$ is a MacDonald code over $\mathbb{Z}_7$, with parameters*

$$\left[\frac{7}{18}\left(7^k - 1\right)\left[7^{k+1} + 7^{2k-1} + 7^{4(k-1)}\right] - \frac{7}{18}\left(7^t - 1\right)\left[7^{t+1} + 7^{2t-1} + 7^{4(t-1)}\right]; k\right]. \tag{3.10}$$

Proof. The MacDonald code $\mathcal{M}_{k,t}^\beta$ of type β is generated similarly to $\mathcal{M}_{k,t}^\alpha$, but with a different repetition scheme. The generator matrix $\Omega_{k,t}^\beta$ incorporates copies of subcodes over $\mathbb{Z}_7$, $\mathcal{A}_7$, and $\mathcal{R}_7$ arranged in a weighted structure. Applying Φ maps the code into $\mathbb{Z}_7^n$ while preserving linearity and weight. Due to the linear independence of generators and the inherited structure, $\Phi(M_{k,t}^\beta)$ forms a MacDonald code over $\mathbb{Z}_7$ with parameters matching the algebraic derivation from the generator matrix size and structure. □

3.2. The Hamming weights distributions of $\Phi(\mathcal{S}_k^{\alpha})$, $\Phi(\mathcal{S}_k^{\beta})$, $\Phi(\mathcal{M}_{k,t}^{\alpha})$ and $\Phi(\mathcal{M}_{k,t}^{\beta})$

Specifically, our analysis delves into the determination of Hamming weight distributions, a crucial step in characterizing a minimal linear code over $\mathbb{Z}_7$. The obtained results are presented in the Tables 1-3, offering a comprehensive view of the weight distribution patterns within the code. This exploration contributes valuable insights into the fundamental properties of minimal linear codes.

	w_H	Number of distinct codewords
$\Phi(\mathcal{S}_k^{\alpha}), \Phi(\mathcal{S}_k^{\beta})$	0	1
$\Phi(\mathcal{S}_k^{\alpha}), \Phi(\mathcal{S}_k^{\beta})$	$6(7^{k-1} + 2 \times 7^{2(k-1)} + 4 \times 7^{4(k-1)})$	$(7^k - 1) + 2(7^{2k} - 1) + 4(7^{4k} - 1)$

Table 1. The Hamming weight distribution of linear codes $\Phi(\mathcal{S}_k^{\alpha})$ and $\Phi(\mathcal{S}_k^{\beta})$

	w_H	Number of distinct codewords
$\Phi(\mathcal{M}_k^{\alpha})$	0	1
$\Phi(\mathcal{M}_k^{\alpha})$	$(7^{k-1} + 2 \times 7^{2k-1} + 4 \times 7^{4k-1}) - (7^{t-1} + 2 \times 7^{2t-1} + 4 \times 7^{4t-1})$	$7^{k+1} - 7^{k+1-t}$
$\Phi(\mathcal{M}_k^{\alpha})$	$7^{k-1} + 2 \times 7^{2k-1} + 4 \times 7^{4k-1}$	$7(7^{k-t} - 1)$

Table 2. The Hamming weight distribution of linear codes $\Phi(\mathcal{M}_{k,t}^{\alpha})$

	w_H	Number of distinct codewords
$\Phi(\mathcal{M}_k^{\beta})$	0	1
$\Phi(\mathcal{M}_k^{\beta})$	$(7^{k-1} + 2 \times 7^{2k-2} + 4 \times 7^{4k-4}) - (7^{t-1} + 2 \times 7^{2t-2} + 4 \times 7^{4t-4})$	$7^{k+1} - 7^{k+1-t}$
$\Phi(\mathcal{M}_k^{\beta})$	$7^{k-1} + 2 \times 7^{2k-2} + 4 \times 7^{4k-4}$	$7(7^{k-t} - 1)$

Table 3. The Hamming weight distribution of linear codes $\Phi(\mathcal{M}_{k,t}^{\beta})$

3.3. A minimal linear code over $\mathfrak{R} = \mathbb{Z}_7\mathcal{A}_7\mathcal{R}_7$

The distinctive category of linear codes known as minimal linear codes holds significant relevance in the realm of secret-sharing schemes. These codes, characterized by specific properties, play a crucial role in ensuring the secure distribution of sensitive information among multiple parties. The unique features inherent in minimal linear codes make them particularly well-suited for applications where confidentiality, integrity, and efficient sharing of secrets are paramount. This family of codes represents a valuable tool in the construction of robust and secure cryptographic systems, contributing to the advancement of information security protocols.

Theorem 3.8. *All nonzero codewords of codes $\Phi(\mathcal{S}_k^{\beta})$, $\Phi(\mathcal{M}_{k,t}^{\alpha})$ and $\Phi(\mathcal{M}_{k,t}^{\beta})$ over $\mathbb{Z}_7$ are minimal.*

Proof. Let $\Phi(\mathcal{M}_{k,t}^{\beta})$ denote the Gray image of the β-MacDonald code over $\mathbb{Z}_7$. Since the Gray map Φ is a linear isometry with respect to the Lee weight over $\mathfrak{R}$ and the Hamming weight over $\mathbb{Z}_7$, the image C is a linear code over $\mathbb{Z}_7$.

We use Table 3 and the Ashikhmin–Barg minimality criterion [3], which states that a linear code over $\mathbb{F}_p$ is minimal if:

$$\frac{w_{\min}}{w_{\max}} > \frac{p-1}{p}.$$

In our case, $p = 7$, so the threshold becomes:

$$\frac{6}{7}.$$

The weights of the Gray images are derived as follows. For fixed $k > t$, the maximum weight of the code is:

$$w_{\max} = 7^{k-1} + 2 \times 7^{2k-2} + 4 \times 7^{4k-4}$$

and the minimum weight is:

$$w_{\min} = w_{\max} - \left(7^{t-1} + 2 \times 7^{2t-2} + 4 \times 7^{4t-4}\right).$$

Thus,

$$\frac{w_{\min}}{w_{\max}} = \frac{w_{\max} - \delta}{w_{\max}},$$

where $\delta = 7^{t-1} + 2 \times 7^{2t-2} + 4 \times 7^{4t-4}$. □

Example 3.9. Take $k = 3$ and $t = 2$ in Equation (3.8). Then

$$w_{\max} = 7^2 + 2 \times 7^4 + 4 \times 7^8 = 49 + 4802 + 23059204 = 23064055,$$

$$\delta = 7^1 + 2 \times 7^2 + 4 \times 7^4 = 7 + 98 + 9604 = 9709,$$

$$w_{\min} = 23064055 - 9709 = 23054346.$$

Hence,

$$\frac{w_{\min}}{w_{\max}} = \frac{23054346}{23064055} \approx 0.9996 > \frac{6}{7} \approx 0.8571.$$

This verifies the inequality explicitly for $k = 3$, $t = 2$. Since the denominator grows faster than the numerator when $k > t$, the ratio becomes even closer to 1 as k increases.

Therefore, for all valid MacDonald code constructions where $t < k$, the inequality:

$$\frac{w_{\min}}{w_{\max}} > \frac{6}{7}$$

holds true, and hence $\Phi(\mathcal{M}^{\beta}_{k,t})$ is minimal linear codes over $\mathbb{Z}_7$.

We use a similar arguments for the codes $\Phi(\mathcal{S}^{\beta}_{k})$ and $\Phi(\mathcal{M}^{\alpha}_{k,t})$.

Theorem 3.8 leads us to the following remark.

Remark 3.10. The Gray images $\Phi(\mathcal{S}^{\beta}_{k})$, $\Phi(\mathcal{M}^{\alpha}_{k,t})$, and $\Phi(\mathcal{M}^{\beta}_{k,t})$ are minimal linear codes over $\mathbb{Z}_7$. Their minimality is ensured by satisfying the Ashikhmin-Barg [3] condition:

$$\frac{w_{\min}}{w_{\max}} > \frac{6}{7},$$

where $w_{\min}$ and $w_{\max}$ are the minimum and maximum nonzero Hamming weights of the code, respectively. This condition is verified in Theorem 3.8.

4. Secret-sharing schemes and multi-secret sharing schemes based on minimal linear simplex and MacDonald codes

This section explores the design and implementation of secret-sharing and multi-secret-sharing schemes derived from minimal linear codes constructed over the ring $\Re = \mathbb{Z}_7\mathcal{A}_7\mathcal{R}_7$. Specifically, we employ the Gray images of linear simplex and MacDonald codes to generate minimal linear codes over $\mathbb{Z}_7$, which serve as the foundation for cryptographic protocols. These minimal codes possess desirable algebraic properties that ensure that each nonzero codeword is minimal, a feature essential for defining efficient and secure access structures. We investigate how the duals of these codes can be applied to construct qualified access sets in secret-sharing schemes and how subsets of these codes can support the secure distribution of multiple secrets simultaneously. Throughout this section, theoretical results are supported by concrete examples that illustrate the construction, participant distribution, and recovery processes in single- and multi-secret-sharing scenarios.

4.1. Secret-sharing schemes based on minimal linear simplex and MacDonald codes

The utilization of minimal linear codes over $\mathbb{Z}_7$ extends to the establishment of secret-sharing schemes. The implementation of this concept will be elucidated in the subsequent theorems, providing specific details on how minimal linear codes play a pivotal role in the formulation and execution of secure information sharing mechanisms.

Theorem 4.1. *Let $\Phi(\mathcal{S}_k^\beta)$ be the linear code over $\mathbb{Z}_7$. Then in the secret-sharing scheme based on $\Phi(\mathcal{S}_k^\beta)^\perp$, there are $\tau_1 = \left(\frac{7^k-1}{6}\right)\left[2\times 7^{k-1} + 4\times 7^{3(k-1)}\right]$ participants. Moreover, each participant P_i is involved in $6\times 7^{(k-2)}$ out of $7^{(k-1)}$ minimal access sets.*

Proof. This result follows directly from the access structure framework introduced by Massey [13], extended to linear codes over finite fields. In a linear secret-sharing scheme, the secret is embedded in the first coordinate, and shares are presented via the remaining coordinates of a codeword.

A subset of participants $A \subseteq \{P_1, \ldots, P_{n-1}\}$ can recover the secret if there exists a codeword in $\Phi(\mathcal{S}_k^\beta)^\perp$ with support contained in $\{0\} \cup A$, and with $c_0 \neq 0$. The minimality condition ensures that the access set is minimal, i.e., no proper subset of A can reconstruct the secret.

Thus, participant P_i belongs to some minimal access set if and only if there exists such a codeword with $c_0 = 1$ and $c_i \neq 0$. □

Theorem 4.2. *Let $\Phi(\mathcal{M}_{k,t}^\alpha)$ be the linear torsion code over $\mathbb{Z}_7$. Then in the secret-sharing scheme based on $\Phi(\mathcal{M}_k^\alpha)^\perp$, there are $\tau_2 = \left(7^k + 2\times 7^{2k} + 4\times 7^{4k}\right) - \left(7^t + 2\times 7^{2t} + 4\times 7^{4t}\right) - 1$ participants. Moreover, each participant P_i is involved in $6\times 7^{(k-2)}$ out of $7^{(k-1)}$ minimal access sets.*

Proof. Since $\Phi(\mathcal{M}_{k,t}^\alpha)$ is a minimal code, every nonzero codeword in $\Phi(\mathcal{M}_{k,t}^\alpha)$ is minimal, and its support is not strictly contained within the support of any other codeword that is not a scalar multiple of it. By duality, every such codeword in $\Phi(\mathcal{M}_k^\alpha)^\perp$ with $c_0 = 1$ defines a unique minimal access set.

This uniqueness arises because the support of a minimal codeword is minimal under inclusion. Therefore, each codeword corresponds to a unique subset of participants capable of reconstructing the secret, and no proper subset can do so. □

Theorem 4.3. *Let $\Phi(\mathcal{M}_{k,t}^\beta)$ be the linear torsion code over $\mathbb{Z}_7$. Then in the secret-sharing scheme based on $\Phi(\mathcal{M}_k^\beta)^\perp$, there are*

$$\tau_3 = \left(\frac{7^k-1}{6}\right)\left[1 + 2\times 7^{k-1} + 4\times 7^{3(k-1)}\right] - \left(\frac{7^t-1}{6}\right)\left[1 + 2\times 7^{t-1} + 4\times 7^{3(t-1)}\right] - 1$$

participants. Moreover, each participant P_i is involved in $6\times 7^{(k-2)}$ out of $7^{(k-1)}$ minimal access sets.

Proof. Each minimal access set corresponds to a unique minimal codeword $c \in \Phi(\mathcal{M}_{k,t}^\beta)^\perp$ such that $c_0 = 1$, as established in Theorem 4.1. Since $\Phi(\mathcal{M}_{k,t}^\beta)$ is minimal, all codewords in $\Phi(\mathcal{M}_{k,t}^\beta)^\perp$ with the required condition give rise to distinct access sets by Theorem 4.2.

Therefore, counting the number of such codewords gives the number of minimal access sets. This bijection between minimal codewords (with $c_0 = 1$) in $\Phi(\mathcal{M}_{k,t}^\beta)^\perp$ and minimal access sets proves the result. □

Example 4.4. Let us consider the code $\Phi(\mathcal{M}_2^\beta)$ over $\mathbb{Z}_7$ of length $n = 61705$ generated by

$$\Phi\left(\Omega_{2,1}^\beta\right) = 1_{8815} \otimes \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 \end{bmatrix}.$$

In the access structure, there are $m = 61704$ participants and seven minimal qualified sets given by

$$\begin{aligned}
\Lambda_1 &= 1_{8815} \otimes \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}, \\
\Lambda_2 &= 1_{8815} \otimes \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 0 \end{pmatrix}, \\
\Lambda_3 &= 1_{8815} \otimes \begin{pmatrix} 1 & 5 & 2 & 6 & 3 & 0 & 4 \end{pmatrix}, \\
\Lambda_4 &= 1_{8815} \otimes \begin{pmatrix} 1 & 3 & 5 & 0 & 2 & 4 & 6 \end{pmatrix}, \\
\Lambda_5 &= 1_{8815} \otimes \begin{pmatrix} 1 & 4 & 0 & 3 & 6 & 2 & 5 \end{pmatrix}, \\
\Lambda_6 &= 1_{8815} \otimes \begin{pmatrix} 1 & 6 & 4 & 2 & 0 & 5 & 3 \end{pmatrix}, \\
\Lambda_7 &= 1_{8815} \otimes \begin{pmatrix} 1 & 0 & 6 & 5 & 4 & 13 & 2 \end{pmatrix}.
\end{aligned}$$

Each participant P_i, $1 \leq i \leq 61704$ in the set $\langle 61704 \rangle$ where $\langle 61704 \rangle = \{1, 2, \ldots, 61704\}$ is in 7 minimal access sets.

Example 4.5. The code $\Phi(\mathcal{S}_3^{\beta})$ over $\mathbb{Z}_7$ of length $n = 769273197$ generated by

$$\Phi\left(\Omega_3^{\beta}\right) = 1_{13496021} \otimes \begin{bmatrix} 10011111111111111111111111111111111111111111111111110000001 \\ 01000001111111222222233333334444444555555566666660111111 0 \\ 00134560123456012345601234560123456012345601234561123456 2 \end{bmatrix}.$$

In the access structure, there are $t = 769273196$ participants and 49 minimal qualifed sets given by

$$\begin{aligned}
\rho_1 &= 1_{13496021} \otimes (10011111111111111111111111111111111111111111111111110000001), \\
\rho_2 &= 1_{13496021} \otimes (11011112222222333333344444445555555666666600000001111111), \\
\rho_3 &= 1_{13496021} \otimes (12011113333333555555500000002222222444444466666661222222 1), \\
\rho_4 &= 1_{13496021} \otimes (13011114444444000000033333336666666222222255555551333333 1), \\
\rho_5 &= 1_{13496021} \otimes (14011115555555222222266666663333333000000044444441444444 1), \\
\rho_6 &= 1_{13496021} \otimes (15011116666666444444422222220000000555555533333331555555 1), \\
\rho_7 &= 1_{13496021} \otimes (16011110000000666666655555554444444333333322222221666666 1), \\
\rho_8 &= 1_{13496021} \otimes (10145601234560123456012345601234560123456012345602123456 3), \\
\rho_9 &= 1_{13496021} \otimes (11145602345601345601245601235601234601234501234562234560 3), \\
\rho_{10} &= 1_{13496021} \otimes (12145603456012560123401234562345601456012360123452345601 3),
\end{aligned}$$

$$\begin{aligned}
\rho_{11} &= 1_{13496021} \otimes (13145604560123012345634560126012345234560156012342456012 3), \\
\rho_{12} &= 1_{13496021} \otimes (14145605601234234560160123453456012012345645601232560123 3), \\
\rho_{13} &= 1_{13496021} \otimes (15145606012345456012323456010123456560123434560122601234 3), \\
\rho_{14} &= 1_{13496021} \otimes (16145600123456601234556012344560123345601223456012012345 3), \\
\rho_{15} &= 1_{13496021} \otimes (10202461350246135024613502461350246135024613502463246135 5), \\
\rho_{16} &= 1_{13496021} \otimes (11202462461350350246146135025024613613502402461353350246 5), \\
\rho_{17} &= 1_{13496021} \otimes (12202463502461502461302461352461350461350261350243461350 5), \\
\rho_{18} &= 1_{13496021} \otimes (13202464613502024613535024616135024246135050246133502461 5), \\
\rho_{19} &= 1_{13496021} \otimes (14202465024613246135061350243502461024613546135023613502 5), \\
\rho_{20} &= 1_{13496021} \otimes (15202466135024461350224613500246135502461335024613024613 5),
\end{aligned}$$

$$\rho_{21} = 1_{13496021} \otimes (162024602461356135024502461346135023502461246135031350245),$$
$$\rho_{22} = 1_{13496021} \otimes (103362514036251403625140362514036251403625140362543625140),$$
$$\rho_{23} = 1_{13496021} \otimes (123362536251405140362036251425140364036251625140345140360),$$
$$\rho_{24} = 1_{13496021} \otimes (133362540362510362514362514062514032514036514036246251400),$$
$$\rho_{25} = 1_{13496021} \otimes (143362551403622514036625140336251400362514403625140362510),$$
$$\rho_{26} = 1_{13496021} \otimes (153362562514034036251251403603625145140362362514041403620),$$
$$\rho_{27} = 1_{13496021} \otimes (163362503625146251403514036240362513625140251403642514030),$$
$$\rho_{28} = 1_{13496021} \otimes (113362525140363625140403625151403626251403036251444036250),$$
$$\rho_{29} = 1_{13496021} \otimes (104630415263041526304152630415263041526304152630454152632),$$
$$\rho_{30} = 1_{13496021} \otimes (114630426304153041526415263052630416304152041526355263042),$$

$$\rho_{31} = 1_{13496021} \otimes (124630430415265263041041526326304154152630630415256304152),$$
$$\rho_{32} = 1_{13496021} \otimes (134630441526300415263304152663041522630415526304150415262),$$
$$\rho_{33} = 1_{13496021} \otimes (144630452630412630415630415230415260415263415263051526302),$$
$$\rho_{34} = 1_{13496021} \otimes (154630463041524152630263041504152635263041304152652630412),$$
$$\rho_{35} = 1_{13496021} \otimes (164630404152636304152526304141526303041526263041553041522),$$
$$\rho_{36} = 1_{13496021} \otimes (115205320531643164205420531653164206420531053164266420534),$$
$$\rho_{37} = 1_{13496021} \otimes (125205331642055316420053164220531644205316642053160531644),$$
$$\rho_{38} = 1_{13496021} \otimes (135205342053160531642316420564205312053164531642061642054),$$
$$\rho_{39} = 1_{13496021} \otimes (135205342053160531642316420564205312053164531642061642054),$$
$$\rho_{40} = 1_{13496021} \otimes (145205353164202053164642053131642050531642420531662053164),$$

$$\rho_{41} = 1_{13496021} \otimes (155205364205314205316205316405316425316420316420563164204),$$
$$\rho_{42} = 1_{13496021} \otimes (165205305316426420531531642042053163164205205316464205314),$$
$$\rho_{43} = 1_{13496021} \otimes (106543210654321065432106543210654321065432106543206543216),$$
$$\rho_{44} = 1_{13496021} \otimes (116543221065433210654432106554321066543210065432100654326),$$
$$\rho_{45} = 1_{13496021} \otimes (126543232106545432106065432121065434321065654321001065436),$$
$$\rho_{46} = 1_{13496021} \otimes (136543243210650654321321065465432102106543543210602106546),$$
$$\rho_{47} = 1_{13496021} \otimes (146543254321062106543654321032106540654321432106503210656),$$
$$\rho_{48} = 1_{13496021} \otimes (156543265432104321065210654306543215432106321065404321066),$$
$$\rho_{49} = 1_{13496021} \otimes (166543206543216543210543210643210653210654210654305432106).$$

Concerns a secret-sharing scheme derived from a minimal linear code $\Phi(S_3^{\beta})$ over $\mathbb{Z}_7$, which is the Gray image of a code constructed over the ring $\Re = \mathbb{Z}_7\mathcal{A}_7\mathcal{R}_7$. The generator matrix of the code is defined as $\Phi(\Omega_3^{\beta}) = 113496021 \otimes G$, where G is a 3×49 generator matrix specified in this example. This code of length $n = 769273197$ over $\mathbb{Z}_7$. Its minimality is ensured by satisfying Lemma 2.3, which requires the ratio $\frac{w_{\min}}{w_{\max}} > \frac{6}{7}$. Based on the Hamming weight distribution given in the article, namely $w_H = 6(7^{k-1} + 2 \times 7^{2(k-1)} + 4 \times 7^{4(k-1)})$, it is confirmed in Theorem 3.8 that the code is indeed minimal. Consequently, the dual code $\Phi(S_3^{\beta})^{\perp}$ is used to construct the access structure of the secret-sharing scheme. The number of participants is given by $\tau_1 = \left(\frac{7^k-1}{6}\right)\left[2 \times 7^{k-1} + 4 \times 7^{3(k-1)}\right]$, which evaluates to 769273196 for $k = 3$. The scheme defines 49 minimal qualified access sets, each represented by a tensor product of a fixed vector and a row of the generator matrix. Each set corresponds to a subset of participants authorized to reconstruct the secret. In practice, a dealer selects a random information vector $u \in \mathbb{Z}_7^k$ and computes the codeword $v = uG$, distributing the coordinate v_i to participant P_i. A minimal access set makes it possible to recover the secret $s = v_0$ if the corresponding participants can express the first column of G as a linear combination of their

columns. The secret is then recovered using the formula $s = \sum_{j=1}^{m} \eta_j v_{i_j}$, where the coefficients η_j are in $\mathbb{Z}_7$. This approach demonstrates the effectiveness of using minimal codes derived from Gray images for secure and efficient secret-sharing schemes.

Example 4.6. The $\Phi(\mathcal{S}_2^{\alpha})$ code is an α-simplex code, where all nonzero codewords in this code are minimal. It is important to note that while this condition is sufficient, it is not necessarily required. The dual of the α-simplex code possesses parameters $[n, k, d] = [49, 47, 42]$, and its generator matrix is defined by.

$$\Phi\left(H\left(\Omega_2^{\alpha}\right)\right) = 1_{96889010407} \otimes \begin{bmatrix}
1000000000000000000000000000000000000000000000000 \\
0100000000000000000000000000000000000000000000016 \\
0010000000000000000000000000000000000000000000025 \\
0001000000000000000000000000000000000000000000034 \\
0000100000000000000000000000000000000000000000043 \\
0000010000000000000000000000000000000000000000052 \\
0000001000000000000000000000000000000000000000061 \\
0000000100000000000000000000000000000000000000062 \\
0000000010000000000000000000000000000000000000001 \\
0000000001000000000000000000000000000000000000010 \\
0000000000100000000000000000000000000000000000026 \\
0000000000010000000000000000000000000000000000035 \\
0000000000001000000000000000000000000000000000044 \\
0000000000000100000000000000000000000000000000053 \\
0000000000000010000000000000000000000000000000054 \\
0000000000000001000000000000000000000000000000063 \\
0000000000000000100000000000000000000000000000002 \\
0000000000000000010000000000000000000000000000011 \\
0000000000000000001000000000000000000000000000020 \\
0000000000000000000100000000000000000000000000036 \\
0000000000000000000010000000000000000000000000045 \\
0000000000000000000001000000000000000000000000046 \\
0000000000000000000000100000000000000000000000055 \\
0000000000000000000000010000000000000000000000064 \\
0000000000000000000000001000000000000000000000003 \\
0000000000000000000000000100000000000000000000012 \\
0000000000000000000000000010000000000000000000021 \\
0000000000000000000000000001000000000000000000030 \\
0000000000000000000000000000100000000000000000031 \\
0000000000000000000000000000010000000000000000040 \\
0000000000000000000000000000001000000000000000056 \\
0000000000000000000000000000000100000000000000065 \\
0000000000000000000000000000000010000000000000004 \\
0000000000000000000000000000000001000000000000013 \\
0000000000000000000000000000000000100000000000022 \\
0000000000000000000000000000000000010000000000023 \\
0000000000000000000000000000000000001000000000032 \\
0000000000000000000000000000000000000100000000041 \\
0000000000000000000000000000000000000010000000050 \\
0000000000000000000000000000000000000001000000066 \\
0000000000000000000000000000000000000000100000005 \\
0000000000000000000000000000000000000000010000014 \\
0000000000000000000000000000000000000000001000015 \\
0000000000000000000000000000000000000000000100024 \\
0000000000000000000000000000000000000000000010033 \\
0000000000000000000000000000000000000000000001042 \\
0000000000000000000000000000000000000000000000151
\end{bmatrix}.$$

In the secret sharing scheme relying on the dual code $\Phi(\mathcal{S}_2^{\alpha})^{\perp}$, there are 49 participants along with a dealer. The total

number of minimal access sets in this scheme is seven.

$$
\begin{aligned}
P_1 &= \{8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,\\
&\quad 36,37,38,39,40,41,42,43,44,45,46,47,48,49\},\\
P_2 &= \{2,3,4,5,6,7,8,9,10,11,12,13,15,16,17,18,19,21,22,23,24,25,27,28,29,30,31,33,34,35,\\
&\quad 36,37,39,40,41,42,43,45,46,47,48,49\},\\
P_3 &= \{2,3,4,5,6,7,8,9,10,12,13,14,15,16,17,18,19,20,22,23,25,26,27,28,29,30,31,32,33,35,\\
&\quad 36,38,39,40,41,42,43,44,45,46,48,49\},\\
P_4 &= \{2,3,4,5,6,7,8,9,11,12,13,14,15,16,17,18,20,21,22,23,24,25,26,27,29,31,32,33,34,35,\\
&\quad 36,37,38,40,41,42,43,44,45,46,47,49\},\\
P_5 &= \{2,3,4,5,6,7,8,9,10,11,12,14,15,16,17,19,20,21,22,24,25,26,27,28,29,30,31,32,33,34,\\
&\quad 36,37,38,39,41,42,43,44,46,47,48,49\},\\
P_6 &= \{2,3,4,5,6,7,8,9,10,11,13,14,15,17,18,19,21,22,23,24,25,26,28,29,30,32,33,34,35,36,\\
&\quad 37,38,39,40,41,43,44,45,47,48,49\},\\
P_7 &= \{2,3,4,5,6,7,8,10,11,12,13,14,15,16,18,19,20,21,22,23,24,26,27,28,29,30,31,32,34,35,\\
&\quad 36,37,38,39,40,42,43,44,45,46,47,48\},
\end{aligned}
$$

Participant P_1 holds a dictatorial role as they are included in every minimal access set, signifying that any group of participants capable of determining the secret must invariably include P_1. Moreover, each participant within the set

$$
\begin{aligned}
&\{8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,\\
&29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49\}
\end{aligned}
$$

is part of six distinct minimal access sets. Therefore, for any group of participants to successfully recover the secret, it necessitates a minimum of six members, constituting 60% of the total participant count.

4.2. Multi-secret sharing schemes based on minimal linear codes

This subsection explores the realm of multi-secret sharing schemes, with a focus on those built upon minimal linear codes. Secret sharing schemes play a pivotal role in secure communication and data protection, ensuring that sensitive information can only be reconstructed when a predetermined set of participants collaborates. In the context of minimal linear codes, these schemes leverage mathematical structures to enhance the security and efficiency of secret sharing protocols.

Exploring an extension of the concepts presented in [1, 2], our research focuses on implementing multi-secret sharing for the Gray images of sub-simplex and sub-Macdonald codes over $\Re$ due to their minimal code properties. To achieve this, we need the Gray images of sub-simplex and sub-MacDonald codes over $\mathbb{Z}_7$ with generating matrices $sub\left(\Phi(\Omega_k^{\alpha})\right)$, $sub\left(\Phi(\Omega_k^{\beta})\right)$, $sub\left(\Phi(\Omega_{k,t}^{\alpha})\right)$, and $sub\left(\Phi(\Omega_{k,t}^{\beta})\right)$. These matrices are defined by the following equations:

$$
\begin{aligned}
rang\left(sub\left(\Phi(\Omega_k^{\alpha})\right)\right) &= rang\left(sub\left(\Phi(\Omega_k^{\alpha})\right) sub\left(\Phi(\Omega_k^{\alpha})\right)\right)^t\\
&= rang\left(sub\left(\Phi(\Omega_k^{\alpha})\right)^t sub\left(\Phi(\Omega_k^{\alpha})\right)\right) \neq 0, \qquad (4.1)
\end{aligned}
$$

$$
\begin{aligned}
rang\left(sub\left(\Phi(\Omega_k^{\beta})\right)\right) &= rang\left(sub\left(\Phi(\Omega_k^{\beta})\right) sub\left(\Phi(\Omega_k^{\beta})\right)\right)^t\\
&= rang\left(sub\left(\Phi(\Omega_k^{\beta})\right)^t sub\left(\Phi(\Omega_k^{\beta})\right)\right) \neq 0, \qquad (4.2)
\end{aligned}
$$

$$
\begin{aligned}
rang\left(sub\left(\Phi(\Omega_{k,t}^{\alpha})\right)\right) &= rang\left(sub\left(\Phi(\Omega_{k,t}^{\alpha})\right) sub\left(\Phi(\Omega_{k,t}^{\alpha})\right)\right)^t\\
&= rang\left(sub\left(\Phi(\Omega_{k,t}^{\alpha})\right)^t sub\left(\Phi(\Omega_{k,t}^{\alpha})\right)\right) \neq 0 \qquad (4.3)
\end{aligned}
$$

and

$$\begin{aligned} rang\left(sub\left(\Phi(\Omega_{k,t}^{\alpha})\right)\right) &= rang\left(sub\left(\Phi(\Omega_{k,t}^{\alpha})\right) sub\left(\Phi(\Omega_{k,t}^{\beta})\right)\right)^{t} \\ &= rang\left(sub\left(\Phi(\Omega_{k,t}^{\beta})\right)^{t} sub\left(\Phi(\Omega_{k,t}^{\beta})\right)\right) \neq 0. \end{aligned} \tag{4.4}$$

Let $\mathbb{Z}_7^n$ be the secret space, where a codeword encodes the secret $S = (s_1, s_2, \ldots, s_n)$ in $\mathbb{Z}_7^n$. The rows of the matrices $sub\left(\Phi(\Omega_k^{\alpha})\right)$, $sub\left(\Phi(\Omega_k^{\beta})\right)$, $sub\left(\Phi(\Omega_{k,t}^{\alpha})\right)$, and $sub\left(\Phi(\Omega_{k,t}^{\beta})\right)$ represent minimal access elements.

All elements of the codes $sub\left(\Phi(\mathcal{S}_k^{\alpha})\right)$, $sub\left(\Phi(\mathcal{S}_k^{\beta})\right)$, $sub\left(\Phi(\mathcal{M}_{k,t}^{\alpha})\right)$, and $sub\left(\Phi(\mathcal{M}_{k,t}^{\beta})\right)$ are participants in this scheme.

The dealer or concessionaire, knowing the secret s, computes the user's share t with the attached codeword c by taking the dot product of this codeword with the secret $t = \langle c, s\rangle = c \cdot s^{\top}$. Using the previous relation, we have the following equations:

$$t^t = sub\left(\Phi(\Omega_k^{\alpha})\right) \cdot s^t, \quad t^t = sub\left(\Phi(\Omega_k^{\beta})\right) \cdot s^t, \quad t^t = sub\left(\Phi(\Omega_{k,t}^{\alpha})\right) \cdot s^t, \quad \text{and } t^t = sub\left(\Phi(\Omega_{k,t}^{\beta})\right) \cdot s^t. \tag{4.5}$$

Here, $t = (t_1, t_2, \ldots, t_k)$, and t_i is the part attached to the i-th row of the matrices $sub\left(\Phi(\Omega_k^{\alpha})\right)$, $sub\left(\Phi(\Omega_k^{\beta})\right)$, $sub\left(\Phi(\Omega_{k,t}^{\alpha})\right)$ and $sub\left(\Phi(\Omega_{k,t}^{\beta})\right)$. The secret can then be obtained by solving the n equations and n unknowns according to the linear systems:

$$\begin{cases} t^t = sub\left(\Phi(\Omega_k^{\alpha})\right) \cdot s^t \\ 0 = H\left(sub\left(\Phi(\Omega_k^{\alpha})\right)\right) \cdot s^t, \end{cases} \quad \begin{cases} t^t = sub\left(\Phi(\Omega_k^{\beta})\right) \cdot s^t \\ 0 = H(\Phi\left(sub\left(\Omega_k^{\beta}\right)\right) \cdot s^t. \end{cases} \tag{4.6}$$

$$\begin{cases} t^t = sub\left(\Phi(\Omega_{k,t}^{\alpha})\right) \cdot s^t \\ 0 = H\left(sub\left(\Phi(\Omega_{k,t}^{\alpha})\right)\right) \cdot s^t, \end{cases} \quad \begin{cases} t^t = sub\left(\Phi(\Omega_{k,t}^{\beta})\right) \cdot s^t \\ 0 = H\left(sub\left(\Phi(\Omega_{k,t}^{\beta})\right)\right) \cdot s^t. \end{cases} \tag{4.7}$$

Example 4.7. For $k = 2$, the generator matrix of $sub\left(\Phi(\mathcal{S}_2^{\alpha})\right)$ is given by

$$sub\left(\Phi(\Omega_2^{\alpha})\right) = \begin{bmatrix} 1 & 1 & 2 & 2 & 3 & 3 & 4 & 4 & 5 & 5 & 6 & 6 \\ 6 & 2 & 3 & 4 & 5 & 6 & 0 & 1 & 2 & 3 & 4 & 5 \end{bmatrix}.$$

Following Equation (4.1), we have

$$rang\left(sub\left(\Phi(\Omega_2^{\alpha})\right)\right) = rang\left(sub\left(\Phi(\Omega_2^{\alpha})\right) sub\left(\Phi(\Omega_2^{\alpha})\right)^{t}\right) = rang\left(sub\left(\Phi(\Omega_2^{\alpha})\right)^{t} sub\left(\Phi(\Omega_2^{\alpha})\right)\right) = 2 \neq 0.$$

If $s = (266534433221) \in sub\left(\Phi(\mathcal{S}_2^{\alpha})\right)$, using Equation (4.5), we check a multi secret-sharing scheme based on $sub\left(\Phi(\mathcal{S}_2^{\alpha})\right)$ by computing the shares as follows

$$t = (3, 3)\,.$$

Let $s = (s_1\ s_2\ s_3\ s_4\ s_5\ s_6\ s_7\ s_8\ s_9\ s_{10}\ s_{11}\ s_{12}) \in sub\left(\Phi(\mathcal{S}_2^{\alpha})\right)$ be the secret. Consider the system of equations defined in Equation (4.6), we have

$$\begin{pmatrix} 1 & 1 & 2 & 2 & 3 & 3 & 4 & 4 & 5 & 5 & 6 & 6 \\ 6 & 2 & 3 & 4 & 5 & 6 & 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 4 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 6 & 3 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 6 & 4 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 6 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 6 & 6 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 5 \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \\ s_5 \\ s_6 \\ s_7 \\ s_8 \\ s_9 \\ s_{10} \\ s_{11} \\ s_{12} \end{pmatrix} = \begin{pmatrix} 3 \\ 3 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

There is a singular solution to the system of equations, and upon solving it, we find that

$$s = (266534433221).$$

Example 4.8. When $k = 3$, the generator matrix for $sub\left(\Phi(\mathcal{S}_3^{\beta})\right)$ is expressed as follows:

$$sub\left(\Phi(\mathcal{S}_3^{\alpha})\right) = \begin{bmatrix} 11111111111100000000 \\ 11223344556611111110 \\ 62345601234501234561 \end{bmatrix}.$$

In accordance with Equation (4.1), we observe

$$\begin{aligned} rang\left(sub\left(\Phi(\Omega_3^{\beta})\right)\right) &= rang\left(sub\left(\Phi(\Omega_3^{\beta})\right) sub\left(\Phi(\Omega_3^{\beta})\right)^t\right) \\ &= rang\left(sub\left(\Phi(\Omega_3^{\beta})\right)^t sub\left(\Phi(\Omega_3^{\beta})\right)\right) \\ &= 3 \neq 0. \end{aligned}$$

If $s = (26431054216565432106)$ belongs to $sub\left(\Phi(\mathcal{S}_3^{\beta})\right)$, we employ Equation (4.5) to examine a multi-secret-sharing scheme utilizing $sub\left(\Phi(\mathcal{S}_3^{\beta})\right)$. The shares are computed as follows:

$$t = (4, 2, 0).$$

Assume $s = (s_1\ s_2\ s_3\ s_4\ s_5\ s_6\ s_7\ s_8\ s_9\ s_{10}\ s_{11}\ s_{12}\ s_{13}\ s_{14}\ s_{15}\ s_{16}\ s_{17}\ s_{18}\ s_{19}\ s_{20}) \in sub\left(\Phi(\mathcal{S}_3^{\beta})\right)$ represents the secret. Examining the system of equations outlined in Equation (4.6), we get

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 2 & 2 & 3 & 3 & 4 & 4 & 5 & 5 & 6 & 6 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 6 & 2 & 3 & 4 & 5 & 6 & 0 & 1 & 2 & 3 & 4 & 5 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 4 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 6 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 5 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 3 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 6 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 6 & 6 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 6 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 6 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 6 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 6 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 6 & 1 \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \\ s_5 \\ s_6 \\ s_7 \\ s_8 \\ s_9 \\ s_{10} \\ s_{11} \\ s_{12} \\ s_{13} \\ s_{14} \\ s_{15} \\ s_{16} \\ s_{17} \\ s_{18} \\ s_{19} \\ s_{20} \end{pmatrix} = \begin{pmatrix} 4 \\ 2 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

A unique solution exists for the system of equations, and upon its resolution, we determine that

$$s = (26431054216565432106).$$

4.3. Security analysis of a multi-secret sharing scheme

This work presents a comprehensive evaluation of a multi-secret sharing scheme, focusing on various aspects crucial for its security and reliability. The study begins by assessing the scheme's ability to maintain the confidentiality

of shared secrets through an analysis of its resistance against eavesdropping and unauthorized access. The algebraic properties of the minimal linear codes employed in the scheme are thoroughly examined, including linearity, independence, and other factors contributing to overall security. The computational complexity of reconstructing secrets from shares is investigated to gauge the scheme's resilience against brute-force and sophisticated computational attacks. Information-theoretic security aspects, such as perfect secrecy, are considered, with an emphasis on evaluating information leakage and the impact of additional information on shared secret security. The research extends to the scheme's error-handling capabilities during sharing and reconstruction, assessing the impact of errors on both security and correctness. Cryptanalysis is conducted to identify potential vulnerabilities, including an evaluation of resistance against cryptographic attacks such as algebraic attacks and side-channel attacks.

5. Conclusion

The article explores various aspects related to linear simplex and MacDonald codes over the ring $\mathfrak{R}$. It covers the Gray images of simplex and MacDonald codes over $\mathfrak{R}$ and investigates the Hamming weight distributions of specific code constructions, namely $\Phi(\mathcal{S}_k^{\alpha})$, $\Phi(\mathcal{S}_k^{\beta})$, $\Phi(\mathcal{M}_{k,t}^{\alpha})$, and $\Phi(\mathcal{M}_{k,t}^{\beta})$. The second part of the article delves into secret-sharing schemes based on minimal linear simplex and MacDonald codes. This involves exploring the potential applications and security implications of utilizing these codes in secret-sharing scenarios. Furthermore, the third part of the article extends the discussion to multi-secret sharing schemes based on minimal linear codes. The focus is on schemes that involve multiple secrets and their security analysis. In conclusion, the article provides a comprehensive examination of linear simplex and MacDonald codes over the ring $\mathfrak{R}$, shedding light on their properties, constructions, and applications in secret-sharing schemes. The inclusion of the security analysis of multi-secret sharing schemes enhances the practical relevance of the research, making it a valuable contribution to the fields of coding theory and cryptography. The findings presented in the article offer insights into the potential use of these codes in secure communication and data protection, paving the way for further research and development in the domain.

Acknowledgments

The author extends heartfelt gratitude to all individuals who have contributed to the enhancement and publication of this work. Their invaluable efforts and support in improving the manuscript have played a pivotal role in shaping its final form.

Author Contributions: This paper has only one author.

Conflict of Interest: The author declares no conflict of interest.

Funding (Financial Disclosure): There is no funding for this work.

References

[1] A. Alahmadi, A. Altassan, A. AlKenani, S. Çalkavur, et al., *A multisecret-sharing scheme based on LCD codes*, Mathematics **8 (2)**, 2020; Article ID: 272.

[2] N. Al Ebri, J. Baek and C. Y. Yeun, *Study on secret sharing schemes (SSS) and their applications*, In: International Conference for Internet Technology and Secured Transactions, Abu Dhabi, United Arab Emirates, December 11-14, 2011, pp. 40–45.

[3] A. Ashikhmin and A. Barg, *Minimal vectors in linear codes and sharing of secrets*, In: Proceedings of the EIDMA Winter Meeting on Coding Theory, Information Theory and Cryptology, Veldhoven, The Netherlands, December 19-21, 1994.

[4] K. Chatouh, *Some codes over $R = R_1R_2R_3$ and their applications in secret sharing schemes*, Afr. Mat. **35**, 2024; Article ID: 1.

[5] K. Chatouh, K. Guenda and T. A. Gulliver, *New classes of codes over $R_{q,p,m} = \mathbb{Z}_{p^m}[u_1, u_2, \cdots, u_q]/\left\langle u_i^2 = 0, u_iu_j = u_ju_i \right\rangle$ and their applications*, Comput. Appl. Math. **39**, 1–39, 2020.

[6] K. Chatouh, D. Mokhtari and K. Guenda, *Application of multi-secret sharing schemes using LCD codes over $\mathfrak{R} = \mathcal{R}[w]$*, Comput. Appl. Math. **44**, 2025; Article ID: 123.

[7] 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*, J. Appl. Math. Comput. **53**, 201–222, 2017.

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

[9] C. Ding, D. R. Kohelb and S. Ling, *Secret-sharing with a class of ternary codes*, Theor. Comput. Sci. **246**, 285–298, 2000.

[10] J. He and E. Dawson, *Multistage secret sharing based on one-way function*, Electron. Lett. **30**, 1591–1592, 1994.

[11] J. C. Ku-Cauich and H. Tapia-Recillas, *Secret sharing schemes based on almost-bent functions*, Int. J. Pure Appl. Math. **57**, 87–102, 2009.
[12] Z. Li, J. Sun and J. Li, *A novel secret sharing scheme based on minimal linear codes*, Wuhan Univ. J. Nat. Sci. **18**, 407–412, 2013.
[13] J. L. Massey, *Some applications of coding theory in cryptography*, In: Codes and Cyphers: Cryptography and Coding IV (Ed. by P. G. Farrell), Essex, England: Formara Ltd., 1995, pp. 33–47.
[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. **69**, 4833–4853, 2023.
[15] C.-C. Yang, T.-Y. Chang and M.-S. Hwang, *A* (t, n) *multi-secret sharing scheme*, Appl. Math. Comput. **151 (2)**, 483–490, 2004.

How to cite this article: K. Chatouh, *Exploring minimal linear codes defined over* $\mathfrak{R}$ *and their application in secret sharing and multi-secret sharing schemes*, Montes Taurus J. Pure Appl. Math. **8 (1)**, 47–62, 2026; Article ID: MTJPAM-D-23-00059.