**Palestine Journal of Mathematics**

**Vol 13(Special Issue III)(2024)** , 55–62 

# Linear codes over $\mathfrak{R} = \mathbb{Z}_7 \left(\mathbb{Z}_7 + u\mathbb{Z}_7\right) \left(\mathbb{Z}_7 + v\mathbb{Z}_7 + w\mathbb{Z}_7 + vw\mathbb{Z}_7\right)$

Karima Chatouh

Communicated by Kuncham S.P.

MSC 2010 Classifications: Primary 11TXX, 11T71; Secondary 15Axx, 15B33.

Keywords and phrases: Linear Codes, Secret sharing schemes, Simplex and Macdonald codes, Minimal access sets.

**Abstract** In this work, we demonstrate that the Gray images of linear simplex and MacDonald codes over $\mathfrak{R} = \mathbb{Z}_7\mathcal{A}_7\mathcal{R}_7$ are minimal linear codes over $\mathbb{Z}_7$. We have obtained secret-sharing schemes by utilizing these minimal linear codes. Finally, we apply these results to some minimal access sets.

## 1 Introduction

Recently, algebraic coding theory has become very interesting in linear codes over finite rings. These codes have many applications in information coding, strongly regular graphs, secret-sharing schemes, and cryptography. In some of these areas, there has been a lot of research on the use of linear codes over finite commutative rings; see [4, 5, 6, 9].

The class of codes facilitated for study is that of linear codes, which covers some rather good codes and has sufficient structure so that encoding and decoding are not absurdly complicated. Simplex and MacDonald codes are all-important classes of linear codes from both theoretical and practical points of view, being easier to implement due to their rich algebraic structure. These codes are related to the concept of secret-sharing schemes, which have necessary applications in many cryptographic areas, including secure multiparty computations and threshold cryptography, as the secret can be recovered once a subset of the participants shares their information [2, 1, 7, 8, 10, 11, 12, 13].

In this paper, our goal is the application of secret-sharing schemes to some linear 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 $\mathcal{R}_7 = \mathbb{Z}_7 + v\mathbb{Z}_7 + w\mathbb{Z}_7 + vw\mathbb{Z}_7$. Section 2 consists of the basic properties that are used throughout our manuscript. In section 3, we present simplex and MacDonald codes over $\mathfrak{R} = \mathbb{Z}_7\mathcal{A}_7\mathcal{R}_7$. The properties of these codes are studied, particularly the Gray images of simplex and MacDonald codes over the ring $\mathfrak{R} = \mathbb{Z}_7\mathcal{A}_7\mathcal{R}_7$. Additionally, we have calculated the weight distributions of these Gray images. Moreover, we have introduced minimal linear codes over $\mathbb{Z}_7$. Section 4 is devoted to the study of the properties and the applications of secret-sharing schemes based on minimal linear codes over $\mathbb{Z}_7$.

## 2 Some Background and Preliminaries

In this section, we present a strategy to substantiate our results, which is as follows: we provide the properties of the ring $\mathfrak{R}$. Additionally, we determine a Gray Map and Gray images of linear codes over $\mathfrak{R}$. Moreover, we explain the method of computing the secret-sharing schemes using linear codes defined over this ring.

Firstly, the ring $\mathfrak{R}$ can be represented by the following equation:

$$\begin{aligned}\mathfrak{R} = \{\varsigma = (\eta_1, \eta_2, \eta_3) \,|\eta_1 \in \mathbb{Z}_7,\ \eta_2 \in \mathcal{A}_7 = \mathbb{Z}_7 + u\mathbb{Z}_7,\\ \eta_3 \in \mathcal{R}_7 = \mathbb{Z}_7 + v\mathbb{Z}_7 + w\mathbb{Z}_7 + vw\mathbb{Z}_7\},\end{aligned} \tag{2.1}$$

where $u^2 = v^2 = w^2 = 0$, it is known that the ring $\mathbb{Z}_7$ is a subring of the ring $\mathcal{A}_7$ and the ring $\mathcal{A}_7$ is a subring of the ring $\mathcal{R}_7$. We say that $C$ is a $\mathbb{Z}_7\mathcal{A}_7\mathcal{R}_7$-additive code if it is a subgroup of $\mathbb{Z}_7^{\gamma}\mathcal{A}_7^{\delta_1}\mathcal{R}_7^{\delta_2}$. A code $C$ is called separable if $C$ is the direct product of $C_\gamma$, $C_{\delta_1}$ and $C_{\delta_2}$, i.e., $C = C_\gamma \times C_{\delta_1} \times C_{\delta_2}$. The Lee weight of $c = (\lambda, \mu, \nu) \in \mathfrak{R} = \mathbb{Z}_7\mathcal{A}_7\mathcal{R}_7$ is defined as

$$w_{Lee}\left((\lambda, \mu, \nu)\right) = w_{Lee}(\lambda) + w_{Lee}(\mu) + wt_{Lee}(\nu). \tag{2.2}$$

### 2.1 A Gray Map and Gray Images of Linear Code over $\mathfrak{R}$

We will define the Gray map and then construct the weight in such a way that it will provide us with a distance-preserving isometry.

$$\begin{array}{rccc} \Phi & : & \mathbb{Z}_7\mathcal{A}_7\mathcal{R}_7 & \to & \mathbb{Z}_7^7 \\ & & (\lambda,\mu,\nu) & \mapsto & \Phi(\lambda,\mu,\nu), \end{array} \tag{2.3}$$

where

$$\Phi(\lambda,\mu,\nu) = (\lambda, \mu_0, \mu_0+\mu_1, \nu_4, \nu_2+\nu_4, \nu_3+\nu_4, \nu_1+\nu_2+\nu_3+\nu_4), \tag{2.4}$$

with $\mu = \mu_0 + u\mu_1$ and $\nu = \nu_1 + v\nu_2 + w\nu_3 + vw\nu_4$. If extending $\Phi$ naturally from $\mathbb{Z}_7^{\gamma} \times \mathcal{A}_7^{\delta_1} \times \mathcal{R}_7^{\delta_2}$ to $\mathbb{Z}_7^{n=\gamma+2\delta_1+4\delta_2}$, we check that $\Phi$ is a linear isometry.

**Theorem 2.1.** *If $C$ is a linear code over $\mathfrak{R} = \mathbb{Z}_7\mathcal{A}_7\mathcal{R}_7$ of length $n$ and minimum Lee weight $d$, then $\Phi(C)$ is a linear code with 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

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

according to Equation 2.3, we have

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

### 2.2 Minimal Linear Codes over $\mathfrak{R}$

The sufficient condition on weights for defining a linear code that is minimal is specified in the following lemma.

**Lemma 2.3** ([10]). *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*

$$\frac{w_{min}}{w_{max}} \geqslant \frac{p-1}{p}, \tag{2.5}$$

*then all nonzero codewords of $C$ are minimal.*

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

**Definition 2.4** ([10]). The support of a codeword $c = (c_0, c_1, \cdots, c_{n-1}) \in \mathbb{Z}_q^n$ is defined as

$$supp(c) = \{0 \leqslant i \leqslant n-1; c_i \neq 0\}. \tag{2.6}$$

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

$$supp(c_2) \subseteq supp(c_1). \tag{2.7}$$

**Remark 2.5.** A non-zero codeword $c \in C$ is said to be minimal if the only codewords that cover it are scalar multiples of $c$.

Let a systematic code $C[n;k;d]$ corrects $t = \lfloor \frac{d-1}{2} \rfloor$ errors, so its generator matrix is in the form $G = [I_k|A]$, then $H = [-A^t|I_{n-k}]$ is the parity-check matrix. This code can be used to construct secret-sharing schemes.

### 2.3 Secret Sharing Schemes Based on Linear Codes

Let a dealer $P_0$ and $P = \{P_1, P_2, \ldots, P_{n-1}\}$ be a set of $n-1$ participants. Also, let $\mathfrak{A}p$ be the set of all access elements on $P$. In the secret sharing scheme based on $C$, to compute shares for all the participants, the dealer chooses randomly a vector $u = (u_0, \ldots, u_k) \in \mathbb{F}_p^k$ such that $s = ug_0$. There are $p^{k-1}$ such vectors $u \in \mathbb{F}_p^k$. Therefore, the dealer treats $u$ as an

information vector and calculates the corresponding codeword $v = uG = (v_0, v_1, \ldots, v_{n-1})$, where $G = [g_0, g_1, \ldots, g_{n-1}]$ is a generator matrix of $C$. Consequently, the dealer gives $v_i$ to party $P_i$ as their share for each $1 \leq i \leq n-1$. If $s = v_0 = ug_0$, then a set of shares $(v_{i_1}, v_{i_2}, \cdots, v_{i_m})$ determines the secret $s$ if and only if the column $g_0$ of $G$ is a linear combination of the columns.

$$g_0 = \sum_{j=1}^{m} \eta_j g_{i_j}. \tag{2.8}$$

Then the secret $s$ is recovered by computing

$$s = \sum_{j=1}^{m} \eta_j v_{i_j}. \tag{2.9}$$

## 3 Linear Simplex and MacDonald Codes over $\mathfrak{R}$

In this section, we establish several constructions of linear codes over $\mathfrak{R}$, which are crucial for applying secret sharing schemes. According to [4, 5, 6], we need to define the following.

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

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

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

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

These results lead to the following.

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

Now, we state the following definition concerning 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 $n = 3 \times 7^{7k} - \left(7^{6k+t} + 7^{5k+2t} + 7^{3k+4t}\right)$ generated by, for $k > 1$ and $1 \leq t \leq k-1$,

$$\Omega_{k,t}^{\alpha} = \left[\; 1_{7^{6k}} \otimes G_{\mathbb{Z}_7,k,t}^{\alpha} \;\middle|\; 1_{7^{5k}} \otimes G_{\mathcal{A}_7,k,t}^{\alpha} \;\middle|\; 1_{7^{3k}} \otimes G_{\mathcal{R}_7,k,t}^{\alpha} \;\right], \tag{3.3}$$

and the MacDonald code $\mathcal{M}_{k,t}^{\beta}$ is a linear code over $\mathfrak{R}$ of length $n = \left(\dfrac{7^k}{6}\right)[(7^k - 1)(7 + 7^{k-1} + 7^{3k-4}) - (7^t - 1)(7 + 7^{t-1} + 7^{3t-4})]$ generated by

$$\Omega_{k,t}^{\beta} = \left[\; 1_{7^{k+1}} \otimes G_{\mathbb{Z}_7,k,t}^{\beta} \;\middle|\; 1_{p^k} \otimes G_{\mathcal{A}_7,k,t}^{\beta} \;\middle|\; 1_{7^{k-1}} \otimes G_{\mathcal{R}_7,k,t}^{\beta} \;\right]. \tag{3.4}$$

### 3.1 Gray Images of Simplex and MacDonald Codes over $\mathfrak{R}$

Our initial discovery involves establishing the Gray images of simplex and MacDonald codes over $\mathbb{Z}_7$, a result substantiated by the construction of linear simplex and MacDonald codes over $\mathfrak{R}$.

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

$$\left[7^{7k+1}; k\right]. \tag{3.5}$$

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

$$\left[\frac{7}{18}\left(7^k-1\right)\left[7^{k+1}+7^{2k-1}+7^{4(k-1)}\right]; k\right]. \tag{3.6}$$

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

$$\left[\left(7^k+2\times 7^{2k}+4\times 7^{4k}\right)-\left(p^t+2p^{2t}+4\times 7^{4t}\right); k\right]. \tag{3.7}$$

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

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

### 3.2 The Hamming Weights Distributions of $\Phi(\mathcal{S}_k^{\alpha})$, $\Phi(\mathcal{S}_k^{\beta})$, $\Phi(\mathcal{M}_{k,t}^{\alpha})$ and $\Phi(\mathcal{M}_{k,t}^{\beta})$

In particular, we determine the Hamming weight distributions to characterize a minimal linear code over $\mathbb{Z}_7$, and then we present the following tables:

| | $w_H$ | 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 $\mathfrak{R} = \mathbb{Z}_7\mathcal{A}_7\mathcal{R}_7$

A unique family of linear codes, called minimal linear codes, has important uses in secret-sharing schemes.

**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.* Using Table 3 and Lemma 2.3, for code $\Phi(\mathcal{M}_{k,t}^\beta)$ over $\mathbb{Z}_7$ satisfied

$$\begin{aligned}\frac{w_{min}\left(\Phi(\mathcal{M}_{k,t}^\beta)\right)}{w_{max}\left(\Phi(\mathcal{M}_{k,t}^\beta)\right)} &= \frac{\left((7^{k-1} + 2 \times 7^{2k-2} + 4 \times 7^{4k-4}) - (7^{t-1} + 2 \times 7^{2t-2} + 4 \times 7^{4t-4})\right)}{7^{k-1} + 2 \times 7^{2k-2} + 4 \times 7^{4k-4}} \\ &\geq \frac{6}{7} \geq \frac{1}{2}.\end{aligned}$$

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

This theorem leads us to the following remark.

**Remark 3.9.** The 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.

## 4 Secret-Sharing Schemes Based on Minimal Linear Simplex and MacDonald codes

Minimal linear codes over $\mathbb{Z}_7$ are used to determine secret-sharing schemes. This concept will be further specified in the following theorems.

**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.*

**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.*

**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.*

**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 7 minimal qualifed 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

$$\Phi\left(\Omega_3^{\beta}\right) = 1_{13496021} \otimes \begin{bmatrix} 10011111111111111111111111111111111111111111111111111110000001 \\ 01000001111111222222233333334444444555555566666661011111 10 \\ 00134560123456012345601234560123456012345601234561123456 2 \end{bmatrix},$$

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

$$\begin{aligned}
\rho_1 &= 1_{13496021} \otimes (10011111111111111111111111111111111111111111111111111110000001), \\
\rho_2 &= 1_{13496021} \otimes (11011112222222333333344444445555555666666600000011111111), \\
\rho_3 &= 1_{13496021} \otimes (12011113333333555555500000002222222444444466666661222222 1), \\
\rho_4 &= 1_{13496021} \otimes (13011114444444000000033333336666666222222255555551333333 1), \\
\rho_5 &= 1_{13496021} \otimes (14011115555555222222266666663333333000000044444441444444 1), \\
\rho_6 &= 1_{13496021} \otimes (15011116666666444444422222220000000555555533333331555555 1), \\
\rho_7 &= 1_{13496021} \otimes (16011110000000666666655555554444444333333322222221666666 1), \\
\rho_8 &= 1_{13496021} \otimes (10145601234560123456012345601234560123456012345602123456 3), \\
\rho_9 &= 1_{13496021} \otimes (11145602345601345601245601235601234601234501234562234560 3), \\
\rho_{10} &= 1_{13496021} \otimes (12145603456012560123401234562345601456012360123452345601 3),
\end{aligned}$$

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

$$\rho_{21} = 1_{13496021} \otimes (16202460246135613502450246134613502350246124613503135024 5),$$
$$\rho_{22} = 1_{13496021} \otimes (10336251403625140362514036251403625140362514036254362514 0),$$
$$\rho_{23} = 1_{13496021} \otimes (12336253625140514036203625142514036403625162514034514036 0),$$
$$\rho_{24} = 1_{13496021} \otimes (13336254036251036251436251406251403251403651403624625140 0),$$
$$\rho_{25} = 1_{13496021} \otimes (14336255140362251403662514033625140036251440362514036251 0),$$
$$\rho_{26} = 1_{13496021} \otimes (15336256251403403625125140360362514514036236251404140362 0),$$
$$\rho_{27} = 1_{13496021} \otimes (16336250362514625140351403624036251362514025140364251403 0),$$
$$\rho_{28} = 1_{13496021} \otimes (11336252514036362514040362515140362625140303625144403625 0),$$
$$\rho_{29} = 1_{13496021} \otimes (10463041526304152630415263041526304152630415263045415263 2),$$
$$\rho_{30} = 1_{13496021} \otimes (11463042630415304152641526305263041630415204152635526304 2),$$

$$\rho_{31} = 1_{13496021} \otimes (12463043041526526304104152632630415415263063041525630415 2),$$
$$\rho_{32} = 1_{13496021} \otimes (13463044152630041526330415266304152263041552630415041526 2),$$
$$\rho_{33} = 1_{13496021} \otimes (14463045263041263041563041523041526041526341526305152630 2),$$
$$\rho_{34} = 1_{13496021} \otimes (15463046304152415263026304150415263526304130415265263041 2),$$
$$\rho_{35} = 1_{13496021} \otimes (16463040415263630415252630414152630304152626304155304152 2),$$
$$\rho_{36} = 1_{13496021} \otimes (11520532053164316420542053165316420642053105316426642053 4),$$
$$\rho_{37} = 1_{13496021} \otimes (12520533164205531642005316422053164420531664205316053164 4),$$
$$\rho_{38} = 1_{13496021} \otimes (13520534205316053164231642056420531205316453164206164205 4),$$
$$\rho_{39} = 1_{13496021} \otimes (13520534205316053164231642056420531205316453164206164205 4),$$
$$\rho_{40} = 1_{13496021} \otimes (14520535316420205316464205313164205053164242053166205316 4),$$

$$\rho_{41} = 1_{13496021} \otimes (15520536420531420531620531640531642531642031642056316420 4),$$
$$\rho_{42} = 1_{13496021} \otimes (16520530531642642053153164204205316316420520531646420531 4),$$
$$\rho_{43} = 1_{13496021} \otimes (10654321065432106543210654321065432106543210654321065432 6),$$
$$\rho_{44} = 1_{13496021} \otimes (11654322106543321065443210655432106654321006543210065432 6),$$
$$\rho_{45} = 1_{13496021} \otimes (12654323210654543210606543212106543432106565432100106543 6),$$
$$\rho_{46} = 1_{13496021} \otimes (13654324321065065432132106546543210210654354321060210654 6),$$
$$\rho_{47} = 1_{13496021} \otimes (14654325432106210654365432103210654065432143210650321065 6),$$
$$\rho_{48} = 1_{13496021} \otimes (15654326543210432106521065430654321543210632106540432106 6),$$
$$\rho_{49} = 1_{13496021} \otimes (16654320654321654321054321064321065321065421065430543210 6).$$

## 5 Conclusion

In this work, we have investigated some minimal linear codes over the ring $\mathfrak{R} = \mathbb{Z}_7\mathcal{A}_7\mathcal{R}_7$. We have established the relationship between secret-sharing schemes and these minimal linear codes. In the end, we provided examples that helped demonstrate the effectiveness of the theoretical aspect of the study of the proposed secret-sharing schemes.

## References

[1] A. Alahmadi, A. Altassan, A. AlKenani, S. Çalkavur, H. Shoaib, P. Solé, A multisecret-sharing scheme based on LCD codes, Mathematics **8**, 272 (2020).

[2] A. Ashikhmin, A. Barg, Minimal vectors in linear codes and sharing of secrets, in F. M. J. Willems (Ed.), Proceedings of the EIDMA Winter Meeting on Coding Theory, Information Theory and Cryptology, Veldhoven, The Netherlands, Dec. (1994).

[3] Z. R. Al-Shorbassi and M. M. Al-Ashker, Skew $(\mu_1 + u\mu_2 + v\mu_3 + w\mu_4 + uv\mu_5 + vw\mu_6 + uw\mu_7 + uvw\mu_8)$ Constacyclic Codes over $F_q[u; v; w] =< u^2 - 1; v^2 - 1; w^2 - 1; uv - vu; vw - wv; wu - uw >$, Palestine Journal of Mathematics, **12**, 331-339 (2023).

[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**, 201-222 (2017).

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

[6] 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. Computational and Applied Mathematics **39**, 1-39 (2020).

[7] C. Ding, D. R Kohelb, S. Ling, Secret-sharing with a class of ternary codes, Theoretical Computer Science **246**, 285–298 (2000).

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

[9] N. ur Rehman, M. Azmi and G. Mohammad, Reversible cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + \ldots + u^{k-1}\mathbb{F}_2$, Palestine Journal of Mathematics, **12**, 395-407 (2023).

[10] J.C. Ku-Cauich, H. Tapia-Recillas, Secret sharing schemes based on almost-bent functions. Int. J. Pure and Applied Math **57**, 87-102 (2009).

[11] Z. Li, J. Sun, J. Li, A novel secret sharing scheme based on minimal linear codes, Wuhan University J. Natural Sciences **18**, 407–412 (2013).

[12] J.L. Massey, Some applications of coding theory in cryptography, in Codes and Ciphers: Cryptography and Coding IV, Ed. P. G. Farrell, Formara, Essex, England, 33–47 (1995).

[13] C.C. Yang, T.Y. Chang, M.S. Hwang, A New $(t, n)$- multisecret-sharing scheme. Appl. Math. Comput. **151**, 483-490 (2004).

### Author information

Karima Chatouh, 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., Algeria.
E-mail: karima.chatouh@univ-batna.dz