K. Chatouh

LINEAR CODES OVER $\mathbb{Z}_p\mathcal{R}_1\mathcal{R}_2$ AND THEIR APPLICATIONS

K. Chatouh. *Linear codes over $\mathbb{Z}_p\mathcal{R}_1\mathcal{R}_2$ and their applications*, Mat. Stud. **62** (2024), 3–10.

In the paper, we explore the simplex and the MacDonald codes over the finite ring $\mathbb{Z}_p\mathcal{R}_1\mathcal{R}_2$. Our investigation focuses on the unique properties of these codes, with the particular attention to their weight distributions and Gray images. The weight distribution is a crucial aspect as it provides insights into the error-detection and error-correction capabilities of the codes. Gray images play a significant role in understanding the structure and behavior of these codes. By examining the dual Gray images of simplex and MacDonald codes over $\mathbb{Z}_p\mathcal{R}_1\mathcal{R}_2$, we aim to develop efficient secret sharing schemes. These schemes benefit from the inherent properties of the codes, such as minimal weight and redundancy, which are essential for secure and reliable information sharing. Understanding the access structure of these schemes is vital, as it determines which subsets of participants can reconstruct the secret. Our study draws on various properties to elucidate this access structure, ensuring that the schemes are secure and efficient. Through this comprehensive analysis, we contribute to the field of coding theory by demonstrating how simplex and MacDonald codes over $\mathbb{Z}_p\mathcal{R}_1\mathcal{R}_2$ can be effectively utilized in cryptographic applications, particularly in designing robust and reliable secret sharing mechanisms.

1. Introduction. The linear simplex and the MacDonald codes are integral components of the theoretical framework in coding theory, serving as powerful tools for ensuring the accuracy and security of data transmission and storage. As linear block codes, they systematically encode data into fixed-size blocks, allowing for efficient error detection and correction mechanisms. These codes find extensive application across diverse fields like telecommunications, where reliable communication is paramount, and digital data storage, where maintaining the accuracy and consistency of data is essential over prolonged durations. In cryptography, they contribute significantly to securing sensitive information against unauthorized access and malicious tampering. Furthermore, in network coding, they play a crucial role in optimizing bandwidth usage and enhancing resilience against network disruptions. The study and optimization of linear simplex and MacDonald codes are essential for advancing the capabilities of error-correcting codes, enabling researchers to develop increasingly sophisticated techniques for combating transmission errors and ensuring robust data integrity. By continually refining their properties and exploring new applications, researchers contribute to the ongoing evolution of coding theory, bolstering the foundation of secure and efficient data communication systems, see [2, 4–9, 11–13].

This article aims to provide an in-depth study of advanced topics in coding theory and cryptography, specifically over the finite ring $\mathbb{Z}_p\mathcal{R}_1\mathcal{R}_2$. This includes investigating the structure and properties of Linear Simplex and MacDonald Codes over $\mathbb{Z}_p\mathcal{R}_1\mathcal{R}_2$, exploring the concept and utility of Gray Images of linear codes over $\mathbb{Z}_p\mathcal{R}_1\mathcal{R}_2$, and analyzing the

2020 *Mathematics Subject Classification:* 94B05, 11T71, 14G50.
Keywords: linear codes; simplex codes; Macdonald codes; secret-sharing schemes.
doi:10.30970/ms.62.1.3-10

Hamming weight distributions of these Gray Images to understand their error-detection and correction capabilities. Additionally, the article aims to construct and examine the properties of a minimal linear code over $\mathbb{Z}_p\mathcal{R}_1\mathcal{R}_2$, emphasizing its efficiency and reliability. Finally, the study aims to develop secret sharing schemes based on the minimal linear simplex and MacDonald codes over $\mathbb{Z}_p\mathcal{R}_1\mathcal{R}_2$, demonstrating how these codes can be effectively utilized to create secure and robust methods for sharing confidential information among multiple parties. Through this comprehensive analysis, the article seeks to advance the understanding and practical application of these coding theory concepts in cryptography.

The structure of this paper is organized to lead the reader for the complexities of secret-sharing schemes and the application of advanced coding theory over the finite ring $\mathbb{Z}_p\mathcal{R}_1\mathcal{R}_2$. Section 2 begins by laying the groundwork with a comprehensive discussion on the fundamentals of secret sharing schemes. These include a study of the basic principles and essential requirements that underpin these cryptographic protocols. Additionally, we provide a thorough overview of linear codes over $\mathbb{Z}_p\mathcal{R}_1\mathcal{R}_2$, with a particular emphasis on the properties and significance of linear Gray image codes. These Gray image codes are crucial for understanding the encoding and error-correction capabilities inherent in the linear codes used throughout our study. Moving forward, Section 3 delves into the specifics of simplex and MacDonald codes over $\mathbb{Z}_p\mathcal{R}_1\mathcal{R}_2$. Here, we examine the properties of these codes in detail, with a special focus on their weight distributions and Gray images. The weight distribution analysis provides insight into the error detection of these codes. At the same time, the study of Gray images helps to visualize and understand the structural nuances of the codes in question. In Section 4, we introduce the core of our research: the proposed secret sharing scheme that leverages the minimal linear simplex and MacDonald codes over $\mathbb{Z}_p\mathcal{R}_1\mathcal{R}_2$. This section outlines the encoding process, demonstrating how linear simplex and MacDonald codes generate shares from the original secret. We then explain the methodology for constructing the minimal access secret set of the secret sharing scheme. This involves detailing the criteria and processes that ensure only authorized subsets of participants can reconstruct the original secret, thereby maintaining the confidentiality and integrity of the information shared. Overall, this paper aims to provide a cohesive and detailed exposition on applying linear coding theory to enhance the security and efficiency of secret sharing schemes, with each section building upon the previous to offer a comprehensive understanding of the subject matter.

2. Preliminaries. The purpose of this section is to equip the reader with a solid understanding of the preliminaries needed to appreciate the subsequent analysis of the ring

$$\mathbb{Z}_p\mathcal{R}_1\mathcal{R}_2 = \mathbb{Z}_p\left(\mathbb{Z}_p + v_1\mathbb{Z}_p\right)\left(\mathbb{Z}_p + v_2\mathbb{Z}_p + v_3\mathbb{Z}_p + v_2v_3\mathbb{Z}_p\right).$$

By establishing these fundamentals, we set the stage for exploring profound properties, examples, and applications of this ring in coding theory. Let the ring

$$\mathbb{Z}_p\mathcal{R}_1\mathcal{R}_2 = \mathbb{Z}_p\left(\mathbb{Z}_p + v_1\mathbb{Z}_p\right)\left(\mathbb{Z}_p + v_2\mathbb{Z}_p + v_3\mathbb{Z}_p + v_2v_3\mathbb{Z}_p\right),$$

then

$$\begin{aligned}\mathbb{Z}_p\mathcal{R}_1\mathcal{R}_2 = \big\{\varsigma = (\eta_1,\eta_2,\eta_3)\colon \eta_1 \in \mathbb{Z}_p, \eta_2 \in \mathcal{R}_1 = \mathbb{Z}_p + v_1\mathbb{Z}_p,\\ \eta_3 \in \mathcal{R}_2 = \mathbb{Z}_p + v_2\mathbb{Z}_p + v_3\mathbb{Z}_p + v_2v_3\mathbb{Z}_p, v_i^2 = 0 \ \text{ for } \ 1 \le i \le 3\big\},\end{aligned}$$

it is known that the ring $\mathbb{Z}_p$ is a subring of the ring $\mathcal{R}_1$ and the ring $\mathcal{R}_1$ is a subring of the ring $\mathcal{R}_2$. We say that C is a $\mathbb{Z}_p\mathcal{R}_1\mathcal{R}_2$-additive code if it is a subgroup of $\mathbb{Z}_4^{\gamma} \times \mathcal{R}_1^{\delta_1} \times \mathcal{R}_2^{\delta_2}$. A code C is called separable if C is the direct product of C_γ, C_{δ_1} and C_{δ_2}, i.e.,

$$C = C_\gamma \times C_{\delta_1} \times C_{\delta_2}.$$

The *Lee weight* of $c = (\lambda, \mu, \nu) \in \mathbb{Z}_p\mathcal{R}_1\mathcal{R}_2$ is defined as

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

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

$$\Phi\colon \mathbb{Z}_p \times \mathcal{R}_1 \times \mathcal{R}_2 \to \mathbb{Z}_p^7$$
$$(\lambda,\mu,\nu) \mapsto \Phi\left(\lambda,\mu,\nu\right),$$

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 $\mu = \mu_0 + v_1\mu_1$ and $\nu = \nu_1 + v_2\nu_2 + v_3\nu_3 + v_2v_3\nu_4$.

If extending Φ naturally from $\mathbb{Z}_p^{\gamma} \times \mathcal{R}_1^{\delta_1} \times \mathcal{R}_2^{\delta_2}$ to $\mathbb{Z}_p^{n=\gamma+2\delta_1+4\delta_2}$, we check that Φ is a linear isometry.

Theorem 1. *If C is a linear code over $\mathbb{Z}_p\mathcal{R}_1\mathcal{R}_2$ of length n and minimum Lee weight d, then $\Phi(C)$ is a linear code with the parameters $[7n, k, d_{Lee} = d_H]$.*

The weight perspective provides a sufficient condition for a linear code to be minimal, based on comparing the minimum weight of the code with the minimum nonzero weight of any nonzero codeword. The following lemma establishes that if a linear code is minimal, all codewords of weight equal to the minimum distance are minimal codewords.

Lemma 1 ([3])**.** *Let C be an $[n, k, d_H]$-linear code over $\mathbb{F}_p$, and let w_{min} and w_{max} be the minimum and maximum nonzero weights of C, respectively. If $w_{min}/w_{max} \geqslant (p-1)/p$, then all nonzero codewords of C are minimal.*

We require the idea of minimal codewords in order to find the minimal access sets.

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

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

Let c_1 and c_2 be two codewords of the code C. We say that c_1 covers c_2 if $\mathrm{supp}(c_2) \subseteq \mathrm{supp}(c_1)$.

Remark 1. A non-zero codeword $c \in C$ is said to be minimal if the only codewords that cover it are scalar multiples of c.

Consider the systematic code $C[n, k, d]$ corrects $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ errors, so its generator matrix is $G = [I_k \mid A]$, and its parity-check matrix is $H = [-A^t \mid I_{n-k}]$. This code can be used to establish secret-sharing schemes.

Secret sharing schemes based on linear codes. According to [1], 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 randomly chooses 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, it then 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 $(v_{i_1}, v_{i_2}, \ldots, v_{i_m})$ determines the secret s if and only if column g_0 of G is a linear combination of the columns

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

Then the secret s is recovered by computing $s = \sum_{j=1}^{m} \eta_j v_{i_j}$.

3. Linear simplex and MacDonald codes over $\mathbb{Z}_p\mathcal{R}_1\mathcal{R}_2$. In this section, we delve into the detailed study of linear simplex and MacDonald codes over finite ring $\mathbb{Z}_p\mathcal{R}_1\mathcal{R}_2$.These codes play a pivotal role in coding theory, providing a system for error detection and correction, which are crucial for reliable data transmission. By exploring their concepts and construction, we gain insights into how these codes can be effectively implemented and optimized within the algebraic structure of $\mathbb{Z}_p\mathcal{R}_1\mathcal{R}_2$. The linear simplex codes are renowned for their straightforward construction and effectiveness in simpler coding, while MacDonald codes offer enhanced error-correcting capabilities suitable for more complex applications. This section aims to provide a comprehensive understanding of these coding techniques, demonstrating their adaptability and utility in various applications. Based on the definitions and frameworks established in [4], we have:

Definition 2. The *generator matrix* of $\mathcal{S}_k^\alpha$, simplex codes of type α over $\mathbb{Z}_p\mathcal{R}_1\mathcal{R}_2$, as the concatenation of p^{6k} copies of the generator matrix of $S^\alpha_{\mathbb{Z}_p,k}$, p^{5k} copies of the generator matrix of $S^\alpha_{\mathcal{R}_1,k}$ and p^{3k} copies of the generator matrix of $S^\alpha_{\mathcal{R}_2,k}$, given by

$$\Omega_k^\alpha = \left[\ 1_{p^{6k}} \otimes G^\alpha_{\mathbb{Z}_p,k} \ \middle|\ 1_{p^{5k}} \otimes G^\alpha_{\mathcal{R}_1,k} \ \middle|\ 1_{p^{3k}} \otimes G^\alpha_{\mathcal{R}_2,k} \ \right], \quad \text{for } k \geq 1.$$

Definition 3. The *generator matrix* of $\mathcal{S}_k^\beta$ is the concatenation of p^{k+1} copies of the generator matrix of $S^\beta_{\mathbb{Z}_p,k}$, p^k copies of the generator matrix of $S^\beta_{\mathcal{R}_1,k}$ and p^{k-1} copies of the generator matrix of $S^\beta_{\mathcal{R}_2,k}$ given by

$$\Omega_k^\beta = \left[\ 1_{p^{k+1}} \otimes G^\beta_{\mathbb{Z}_p,k} \ \middle|\ 1_{p^{k}} \otimes G^\beta_{\mathcal{R}_1,k} \ \middle|\ 1_{p^{k-1}} \otimes G^\beta_{\mathcal{R}_2,k} \ \right], \quad \text{for } k \geq 2.$$

Remark 2. 1. Simplex codes $\mathcal{S}_k^\alpha$ of length $n = 3p^{7k}$ and distance minimal

$$d = (p-1)(p^{k-1} + 2p^{2(k-1)} + 4p^{4(k-1)}).$$

2. Simplex codes $\mathcal{S}_k^\beta$ of length $n = \left(\frac{p^k-1}{p-1}\right)\left[p^{k+1} + p^{2k-1} + p^{4(k-1)}\right]$ and distance minimal

$$d = (p-1)(p^{k-1} + 2p^{2(k-1)} + 4p^{4(k-1)}).$$

Definition 4. *MacDonald codes* $\mathcal{M}^\alpha_{k,t}$ is a linear code over $\mathbb{Z}_p\mathcal{R}_1\mathcal{R}_2$ of length

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

generated by

$$\Omega^\alpha_{k,t} = \left[\ 1_{p^{6k}} \otimes G^\alpha_{\mathbb{Z}_p,k,t} \ \middle|\ 1_{p^{5k}} \otimes G^\alpha_{\mathcal{R}_1,k,t} \ \middle|\ 1_{p^{3k}} \otimes G^\alpha_{\mathcal{R}_2,k,t} \ \right], \ \textit{for } k > 1 \textit{ and } 1 \leq t \leq k-1.$$

MacDonald codes $\mathcal{M}^\beta_{k,t}$ is a linear code over $\mathbb{Z}_p\mathcal{R}_1\mathcal{R}_2$ of length

$$n = \left(\frac{p^k}{p-1}\right)[(p^k-1)(p + p^{k-1} + p^{3k-4}) - (p^t-1)(p + p^{t-1} + p^{3t-4})],$$

generated by $\Omega^\beta_{k,t} = \left[\ 1_{p^{k+1}} \otimes G^\beta_{\mathbb{Z}_p,k,t} \ \middle|\ 1_{p^{k}} \otimes G^\beta_{\mathcal{R}_1,k,t} \ \middle|\ 1_{p^{k-1}} \otimes G^\beta_{\mathcal{R}_2,k,t} \ \right]$.

3.1. Gray images of linear codes over $\mathbb{Z}_p\mathcal{R}_1\mathcal{R}_2$. In this subsection, we explore the concept of gray images of linear simplex and MacDonald codes over the finite ring $\mathbb{Z}_p\mathcal{R}_1\mathcal{R}_2$.

Theorem 2. *Let $\mathcal{S}_k^\alpha$ be a $\mathbb{Z}_p\mathcal{R}_1\mathcal{R}_2$-simplex code of type α with the minimum Lee weight d_L, then $\Phi(\mathcal{S}_k^\alpha)$ is a simplex code over $\mathbb{Z}_p$ with the length $\left[7p^{7k}; k\right]$.*

Proof. If Ω_k^α is generator matrix of the $\mathbb{Z}_p\mathcal{R}_1\mathcal{R}_2$-simplex code S_k^α, then $\Phi(\Omega_k^\alpha)$ has the form

$$\Phi(\Omega_k^\alpha) = \left[\begin{array}{c} 1_{7p^{6k}} \otimes G^\alpha_{\mathbb{Z}_p,k} \end{array}\right],$$

where $G^\alpha_{\mathbb{Z}_p,k}$ is a generator matrix of the simplex code $S^\alpha_{\mathbb{Z}_p,k}$. The result then follows by induction on k. □

Theorem 3. *Let $\mathcal{S}_k^\beta$ be a $\mathbb{Z}_p\mathcal{R}_1\mathcal{R}_2$-simplex code of type β with the minimum Lee weight d_L. Then $\Phi(\mathcal{S}_k^\beta)$ is a simplex code over $\mathbb{Z}_p$ with the parameters*

$$\left[\left(\frac{p^k-1}{p-1}\right)\left[1+2p^{k-1}+4p^{3(k-1)}\right]; k\right].$$

Proof. The proof follows a similar approach as that of Theorem 2. □

Theorem 4. *Let $\mathcal{M}_{k,t}^\alpha$ be a $\mathbb{Z}_p\mathcal{R}_1\mathcal{R}_2$ MacDonald code of type α and minimum Lee weight d_L. Then $\Phi(\mathcal{M}_{k,t}^\alpha)$ is a MacDonald code over $\mathbb{Z}_p$, with the parameters*

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

Proof. The proof employs a similar methodology to that of Theorem 2. □

Theorem 5. *Let $\mathcal{M}_{k,u}^\beta$ be a $\mathbb{Z}_p\mathcal{R}_1\mathcal{R}_2$ MacDonald code of type α and minimum Lee weight d_L. Then $\Phi(\mathcal{M}_{k,t}^\beta)$ is the MacDonald code over $\mathbb{Z}_p$, with the parameters*

$$\left[\left(\frac{p^k-1}{p-1}\right)\left[1+2p^{k-1}+4p^{3(k-1)}\right]-\left(\frac{p^t-1}{p-1}\right)\left[1+2p^{t-1}+4p^{3(t-1)}\right]; k\right].$$

Proof. The proof utilizes a comparable methodology to that of Theorem 2. □

Using the format of the generator matrices of the linear codes $\Phi(\mathcal{S}_k^\alpha)$, $\Phi(\mathcal{S}_k^\beta)$, $\Phi(\mathcal{M}_{k,t}^\alpha)$ and $\Phi(\mathcal{M}_{k,t}^\alpha)$, we have the following results that give the Hamming weights distributions.

3.2. Hamming weights distributions of $\Phi(\mathcal{S}_k^\alpha)$, $\Phi(\mathcal{S}_k^\beta)$, $\Phi(\mathcal{M}_{k,t}^\alpha)$ and $\Phi(\mathcal{M}_{k,t}^\alpha)$. To gain a deeper understanding of the linear codes $\Phi(\mathcal{S}_k^\alpha)$, $\Phi(\mathcal{S}_k^\beta)$, $\Phi(\mathcal{M}_{k,t}^\alpha)$ and $\Phi(\mathcal{M}_{k,t}^\alpha)$, as well as the distances between their codewords, we analyze their Hamming weight distributions. These distributions provide critical information about the number of non-zero elements in the codewords, which directly relates to their error detection and error correction capabilities. By examining the Hamming weights, we can construct tables that summarize the distribution of these weights, offering valuable insights into the structure and performance of the codes. This detailed analysis allows us to evaluate the efficiency and reliability of the codes in various applications, ensuring they meet the desired criteria for effective data transmission and storage.

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

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
$\Phi(\mathcal{M}_k^\alpha)$	$(p^{k-1}+2p^{2k-1}+4p^{4k-1})-(p^{t-1}+2p^{2t-1}+4p^{4t-1})$	$7p^k-7p^{k-t}$
$\Phi(\mathcal{M}_k^\alpha)$	$p^{k-1}+2p^{2k-1}+4p^{4k-1}$	$7(p^{k-t}-1)$

Table 2: The Hamming Weight Distribution of Linear Codes $\Phi(\mathcal{M}_k^\alpha)$.

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

Table 3: The Hamming Weight Distribution of Linear Codes $\Phi(\mathcal{M}_k^\beta)$.

3.3. A minimal linear code over $\mathbb{Z}_p\mathcal{R}_1\mathcal{R}_2$. In this subsection, we investigate the concept of a minimal linear code over the ring $\mathbb{Z}_p\mathcal{R}_1\mathcal{R}_2$ and its substantial applications in secret sharing schemes. Minimal linear codes are characterized by their simplicity and optimality in terms of the number of codewords required to achieve specific coding objectives. When applied within the framework of $\mathbb{Z}_p\mathcal{R}_1\mathcal{R}_2$, these codes exhibit unique properties that enhance their effectiveness in secure communications. Specifically, in secret-sharing schemes, minimal linear codes play a crucial role in distributing a secret among multiple participants so that only authorized subsets can reconstruct the secret, while unauthorized subsets gain no information. By exploring these codes' theoretical underpinnings and practical applications, we demonstrate their importance in designing efficient and secure cryptographic protocols.

Theorem 6. *All nonzero codewords of codes $\Phi(\mathcal{S}_k^\beta)$, $\Phi(\mathcal{M}_{k,t}^\alpha)$ and $\Phi(\mathcal{M}_{k,t}^\beta)$ over $\mathbb{Z}_p$ are minimal.*

Proof. Using Table and Lemma 1, the code $\Phi(\mathcal{M}_{k,t}^\beta)$ over $\mathbb{Z}_p$ satisfied

$$\frac{w_{min}\left(\Phi(\mathcal{M}_{k,t}^\beta)\right)}{w_{max}\left(\Phi(\mathcal{M}_{k,t}^\beta)\right)}=\frac{\left((p^{k-1}+2p^{2k-2}+4p^{4k-4})-(p^{t-1}+2p^{2t-2}+4p^{4t-4})\right)}{p^{k-1}+2p^{2k-2}+4p^{4k-4}}\geq\frac{p-1}{p}.$$

□

This theorem leads us to the following remark.

Remark 3. The codes $\Phi(\mathcal{S}_k^\beta)$, $\Phi(\mathcal{M}_{k,t}^\alpha)$ and $\Phi(\mathcal{M}_{k,t}^\beta)$ over $\mathbb{Z}_p$ are minimal.

4. Secret sharing schemes based on the minimal linear simplex and MacDonald codes. We previously noted that identifying the access structure of a secret sharing scheme derived from a linear code can be complex. However, when utilizing minimal linear simplex and MacDonald codes, the construction of secret sharing schemes becomes more manageable and efficient. Minimal linear codes simplify the process by ensuring that each codeword's minimality directly correlates with the scheme's access structure, making it easier to determine which subsets of participants can reconstruct the secret. These specific types of codes, with

their well-defined properties and minimality, provide a structured and reliable foundation for designing robust secret sharing schemes, enhancing both security and ease of implementation.

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

Proof. The result follows from Lemma 1 and Theorem 6. □

Theorem 8. *Let $\Phi(\mathcal{M}_k^{\alpha})$ be the linear torsion code over $\mathbb{Z}_p$. Then in the secret sharing scheme based on $\Phi(\mathcal{M}_k^{\alpha})^{\perp}$, there are $\tau_2 = \left(p^k + 2p^{2k} + 4p^{4k}\right) - (p^t + 2p^{2t} + 4p^{4t}) - 1$ participants. Moreover, each participant P_i is involved in $(p-1)p^{(k-2)}$ out of $p^{(k-1)}$ minimal access sets.*

Proof. By considering Lemma 1 and Theorem 6, we can derive the desired outcome. □

Theorem 9. *Let $\Phi(\mathcal{M}_k^{\beta})$ be the linear torsion code over $\mathbb{Z}_p$. Then in the secret sharing scheme based on $\Phi(\mathcal{M}_k^{\beta})^{\perp}$, there are*

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

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

Proof. The result can be obtained based on the conditions outlined in Theorem 6 and Lemma 1. □

Next, we provide an example showcasing the Gray images of linear simplex and MacDonald codes, along with the corresponding access structure of the secret sharing scheme.

Example 1. Let us consider the ring $\mathbb{Z}_p\mathcal{R}_1\mathcal{R}_2 = \mathbb{Z}_{13}(\mathbb{Z}_{13} + v_1\mathbb{Z}_{13})(\mathbb{Z}_{13} + v_2\mathbb{Z}_{13} + v_3\mathbb{Z}_{13} + v_2v_3\mathbb{Z}_{13})$, the code $\Phi(\mathcal{S}_2^{\beta})$ over $\mathbb{Z}_{13}$ of length $n = 123410$ generated by

$$\Phi\left(\Omega_2^{\beta}\right) = 1_{8815} \otimes \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \end{bmatrix}.$$

In the access structure, there are 123409 participants and 13 minimal qualifed sets. Each participant P_i, $1 \le i \le 123409$ in the set $\langle 123409\rangle$, where $\langle 123409\rangle = \{1, 2, \ldots, 123409\}$ is in 13 minimal access sets.

Example 2. Consider the ring $\mathbb{Z}_p\mathcal{R}_1\mathcal{R}_2 = \mathbb{Z}_5(\mathbb{Z}_5 + v_1\mathbb{Z}_5)(\mathbb{Z}_5 + v_2\mathbb{Z}_5 + v_3\mathbb{Z}_5 + v_2v_3\mathbb{Z}_5)$, the code $\Phi(\mathcal{M}_{3,2}^{\alpha})$ over $\mathbb{Z}_5$ of length $n = 975030100$ generated by $\Phi\left(\Omega_{3,2}^{\alpha}\right)$ defined as follows

$$1_{9750301} \otimes \begin{bmatrix} 111111111111111111111111 & 222222222222222222222222 & 333333333333333333333333 & 444444444444444444444444 \\ 000001111122222333334444 & 000001111122222333334444 & 000001111122222333334444 & 000001111122222333334444 \\ 012340123401234012340123 & 012340123401234012340123 & 012340123401234012340123 & 012340123401234012340123 \end{bmatrix}.$$

In the access structure, there are 975030099 participants and 25 minimal qualifed sets. Each participant P_i, $1 \le i \le 975030099$ in the set $\langle 975030099\rangle$ is in 25 minimal access sets.

5. Conclusion. In conclusion, this study offered significant insights into the construction and applications of Linear Simplex and MacDonald Codes over $\mathbb{Z}_p\mathcal{R}_1\mathcal{R}_2$. By examining Gray images, Hamming weight distributions, and the concept of minimal codes, we deepened our understanding of these codes' characteristics and their importance in secret-sharing schemes. The findings underscore the role of these codes in enhancing secure data transmission and developing robust cryptographic protocols across various fields. This research lays a foundation for future exploration, aiming to optimize these codes for improved security and efficiency in practical applications, thereby contributing to the ongoing advancement of secure communication technologies.

REFERENCES

1. A. Ashikhmin and A. Barg, *Minimal vectors in linear codes and sharing of secrets*, Proc. EIDMA Winter Meeting on Coding Theory, Information Theory and Cryptology (Veldhoven, Netherlands, 1994), Henk C.A. van Tilborg, Frans M.J. Willems (Eds.), 1994, 41.
2. M.C. Bhandari, M.K. Gupta, A.K. Lal, *On $\mathbb{Z}_4$-simplex codes and their gray images*, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC-13, Lecture Notes Comput. Sc., **1719** (1999), 170–180.
3. J.C. Ku-Cauich, H. Tapia-Recillas, *Secret sharing schemes based on almost-bent functions*, Int. J. Pure Appl. Math., **57** (2009), 87–102.
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** (2017), 201–222.
5. K. Chatouh, K. Guenda, T.A. Gulliver, L. Noui, *Simplex and MacDonald codes over R_q*, J. Appl. Math. Comput., **55** (2017), 455–478.
6. K. Chatouh, K. Guenda, T.A. Gulliver, *New classes of codes over $R_{q,p,m} = \mathbb{Z}_{p^m}[u_1, u_2, \cdots, u_q]/\langle u_i^2 = 0, u_iu_j = u_ju_i\rangle$ and their applications*, Comp. Appl. Math., **39** (2020), №152, 1–39. https://doi.org/10.1007/s40314-020-01181-z
7. K. Chatouh, *Some codes over $\mathcal{R} = \mathcal{R}_1\mathcal{R}_2\mathcal{R}_3$ and their applications in secret sharing schemes*, Afr. Math., **35** (2024), №1. https://doi.org/10.1007/s13370-023-01143-8
8. J. Chen, Y. Huang, B. Fu, J. Li, *Secret sharing schemes from a class of linear codes over finite chain ring*, J. Comput. Inform. Syst., **9** (2013), 2777–2784.
9. C.J. Colbourn, M.K. Gupta, *On quaternary MacDonald codes*, Proc. Int. Conf. on Inform. Tech.: Coding and Computing, 2003, 212–215.
10. D. Ding, D.R. Kohelb, S. Ling, *Secret-sharing with a class of ternary codes*, Theoretical Computer Science, **246** (2000), 285–298.
11. M.K. Gupta, C. Durairajan, *On the covering radius of some modular codes*, arXiv:1206.3038v2 [cs.IT] 25 Jun. 2012, 13. https://doi.org/10.48550/arXiv.1206.3038
12. M.K. Gupta, *On Some Linear Codes over $\mathbb{Z}_{2^s}$*, Ph.D. Thesis, IIT, Kanpur, 1999.
13. A. Melakhessou, K. Chatouh, K. Guenda, *DNA multi-secret sharing schemes based on linear codes over $\mathbb{Z}_4 \times R$*, J. Appl. Math. Comp., **69** (2023), №6, 4833–4853. https://doi.org/10.1007/s12190-023-01941-0

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
karima.chatouh@univ-batna.dz

Received 02.07.2024