ISSN: 2307-7743
www.scienceasia.asia
©2025 Science Asia

Asian J. Math. Appl. (2025) 2025:9

Secret Sharing Schemes Based on Linear Codes over F_2RS

Rabia Dertli[1], **Senol Eren**[1]

[1]Department of Mathematics, Ondokuz Mayıs University, Samsun, Turkey

Correspondence should be addressed to Rabia Dertli: rabia.alim06@gmail.com

Abstract
In the paper, we give some interesting access structures of secret sharing schemes based on torsion codes of MacDonald codes over $F_2+uF_2+vF_2$. Later, we study Simplex and MacDonald codes over the finite ring F_2RS. We discuss the properties of these codes by giving their weight distributions and Gray images. By studying the binary Gray images of Simplex and MacDonald codes over F_2RS, we aim to construct efficient secret sharing schemes. These schemes exploit the inherent properties of codes, such as minimum weight, which are essential for reliable information sharing. Understanding the access structure of these schemes is vital as it determines which subsets of participants can reconstruct the secret. Through this comprehensive analysis, we contribute to the field of coding theory by showing how Simplex and MacDonald codes over F_2RS can be effectively used in cryptographic applications to design secret sharing schemes.

Keywords: Simplex codes, MacDonald codes, Secret sharing scheme.

1 Introduction

A secret sharing scheme (SSS) is a method by which a dealer distributes shares of a secret to participants such that only qualified subsets of participants can recover the secret from their shares. SSS was introduced in 1979 by Shamir [1] and Blakley [2]. Since then, many applications of SSS to several different kinds of cryptographic protocols have appeared. For example, SSS can be used in a secure key management scheme and multiparty computation. SSS has been an important cryptographic primitive.

There are many approaches to the design of SSSs. One of them is based on linear codes over finite fields. It was first pointed out by McEliece-Sarwate [3] that Shamir's secret sharing scheme is closely related to the Reed-Solomon coding scheme. After that, Massey [4] constructed secret sharing schemes by linear codes. The relationship between a $minimal\ qualified\ set$ and $minimal\ codeword$ of its dual code was also characterized in [4]. However, the access structure of the secret sharing scheme, which is based on a linear code,e is hard to determine in general. Several authors have considered the minimal codewords of certain codes and characterized the access structure of the secret sharing schemes [5–7]. Only well-structured linear codes can have secret sharing schemes with desirable access structures. The access structures based on some linear codes over finite fields have been determined in [8, 9]. Secret sharing schemes from linear codes over finite chain rings were considered in [10, 11].

In [12], A. Dertli and Y. Cengellenmis constructed MacDonald codes over the ring $R = F_2 + vF_2$. Also, in [13], R. Dertli and S. Eren constructed MacDonald codes over the finite non-chain ring $S = F_2 + uF_2 + vF_2$ and then studied the torsion codes. In this paper, we give some interesting access structures of SSS based on torsion codes of MacDonald codes over $F_2 + uF_2 + vF_2$. This paper aims to present a special case of coding theory and

Received: 2025-01-24

cryptography, especially over the finite ring F_2RS. This includes studying the structure and properties of linear simplex and MacDonald codes over F_2RS, studying the properties of gray images of linear codes over F_2RS, and analyzing the Hamming weight distributions of these gray images to understand their error detection and correction capabilities. In addition, the study aims to examine the structure of the minimal linear code over F_2RS, highlighting its efficiency and reliability. Finally, the study aims to construct secret sharing schemes based on the minimal linear simplex and MacDonald codes over F_2RS and shows how these codes can be effectively used to establish reliable and robust methods for secret information sharing between multiple parties. Through this detailed analysis, our work aims to improve the understanding and application of coding theory concepts in cryptography.

2 Secret Sharing Schemes From Linear Codes

We use P to denote the set of participants. The subset of participants $A \subseteq P$, which can recover the secret, is called a qualified set, while a set $B \subseteq P$ that can't recover the secret is called an unqualified set. Moreover, the secret sharing scheme is perfect if all the unqualified sets cannot get information about the secret in the information theoretic sense. We consider only perfect secret sharing schemes in this paper. A secret sharing scheme is ideal if the shares are the same size as the secret. If $A \subseteq P$ is a qualified set and for all $C \subset A$ with C is an unqualified set, then A is called a minimal qualified set. The set of all qualified sets is called the access structure of the corresponding secret sharing scheme. Let Δ denote the access structure, that is $\Delta = \{A \subseteq P : A\ is\ a\ qualified\ set\}$.

There are many methods to design secret sharing schemes. One of them is to employ linear codes over the finite field Fq. We can construct secret sharing schemes from linear codes with the method in [4]. Let C be an $[n, k]_q$ linear code and $C^{\perp}$ be its dual code. Let $H = (h_0, h_1, \cdots, h_{n-1})$ be the generator matrix of $C^{\perp}$. The dealer choose $u \in F_q^{n-k}$ randomly such that $u \cdot h_0 = s$. Here is the secret to be shared. Let $u \cdot H = (s, c_1, ..., c_{n-1})$, participant P_i receives c_i as his share, $1 \leq i \leq n-1$. The secret sharing scheme constructed in this way is ideal. Generally, we have the following result.

Lemma 1 *[4] Let G be a generator matrix of an* $[n, k]_q$ *linear code C. In the secret sharing scheme based on C, a set of shares* $\{t_{i_1}, t_{i_2}, \cdots, t_{i_m}\}$, $1 \leq i_1 < \cdots < i_m \leq n-1$ *and* $1 \leq m \leq n-1$, *determines the secret if and only if there is a codeword* $(1, 0, \cdots, 0, c_i 1, 0, \cdots, 0, c_{i_m}, 0, \cdots, 0)$ *(in the dual code* $C^{\perp}$*, where* $c_{ij} \neq 0$ *for at least one j).*

In Lemma, the secret sharing scheme is constructed from C, while we construct the scheme from its dual $C^{\perp}$. The support of a vector $(c_0, c_1, ..., c_{n-1})$ is define as the set$\{0 \leq i \leq n-1, c_i \neq 0\}$. The Hamming weight of a vector is the number of its non-zero components. A vector c_1 is covered by a vector c_2 if the support of c_2 contains the support of c_1. If a non-zero codeword c covers only its scalar multiples but no other non-zero codewords, it is called a minimal codeword. The covering problem of a linear code C is to determine all its minimal codewords. This is a tough problem in general. From Lemma, we can see a one-to-one correspondence between the set of minimally qualified sets and the set of minimal codewords with 1 as its first component in the dual code $C^{\perp}$.

It is generally difficult to determine the access structure of a secret sharing scheme constructed from a linear code C. Because the covering problem of a linear code is complex. However, in some special cases, the access structure can be determined.

Lemma 2 *[5] Let C be an* $[n, k]_q$ *linear code and* $G = [g_0, g_1, \cdots, g_{n-1}]$ *be its generator matrix. If each non-zero codeword of C is a minimal codeword, then in the secret sharing scheme based on* $C^{\perp}$*, there are altogether* q^{k-1} *minimal qualified sets. In addition, we have the following:*

1. If g_i is a multiple of g_0, $1 \leq i \leq n-1$, then participant p_i must be in every minimal qualified set.

2. If g_i is not a multiple of g_0, $1 \leq i \leq n-1$, then participant p_i must be in $(q-1)q^{k-2}$ out of q^{k-1} minimal access sets.

The access structure in Lemma is interesting. In Case 1 of Lemma, some participants must be in every minimal access set and thus are dictators. As in Case 2 of Lemma, each participant plays the same role as he is involved in the same number of minimal qualified sets. Such a secret sharing scheme is said to be democratic. Secret sharing schemes like these cases may be required in certain applications. So, it is useful to construct a linear code in which all of its codewords are minimal.

According to [14], let a dealer p_0 and $p = \{p_1, p_2, \ldots\ldots, p_{n-1}\}$ be a set of $n-1$ participants. Also, let μ_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 $u = (u_0, \ldots, u_k) \in F_p^k$ such that $s = ug_0$. There are p^{k-1} such vectors $o \in F_p^k$. 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 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 go of G is a linear combination of the columns; $g_0 = \sum_{j=1}^{m} n_j g_{i_j}$. Then the secret s is recovered by computing $s = \sum_{j=1}^{m} n_j v_{i_j}$.

3 Secret Sharing Schemes over $F_2 + uF_2 + vF_2$

3.1 MacDonald code over $F_2 + uF_2 + vF_2$

In [13] constructed MacDonald codes of type α over the ring $F_2 + u\ F_2 + vF_2$, where $u^2 = u$, $v^2 = v$, $uv = vu = 0$, $F_2 = \{0, 1\}$ is the field of two elements and investigate their properties such as torsion codes and weight distributions. From this point of view;

Definition 3 *[13] The code $C_{k,u}^{\alpha}$ generated by $G_{k,u}^{\alpha}$ is called a type α MacDonald code. We can see that the code $C_{k,t}^{\alpha}$ is a linear code over the ring $F_2 + u\ F_2 + vF_2$ of length $n = 2^{3k} - 2^{3t}$. Let $C_{k,u,T}^{\alpha}$ be the torsion code of $C_{k,u}^{\alpha}$. That is the generator matrix of $C_{k,u,T}^{\alpha}$ is obtained by replacing $(1-v)$ by 1 in the matrix of $(1-v)G_{k,u}^{\alpha}$. Similarly, we can get another torsion code of $C_{k,u}^{\alpha}$ by replace v by 1 in $vG_{k,u}^{\alpha}$. We know that the two torsion codes are equivalent. Therefore, we only consider the former case, i.e., we only study $C_{k,u,T}^{\alpha}$. We give the Hamming weight distributions of $C_{k,u,T}^{\alpha}$ in the following result.*

Theorem 4 *[13] The torsion code of $M_{k,u}^{\alpha}$ is binary linear $[2^{3k} - 2^{3u}, k, 2^{3k-1} - 2^{3u-1}]$ code with weight distribution $A_H(0) = 1$, $A_H(2^{3k-1} - 2^{3u-1}) = [2^{k-u}(2^u - 1)]$ and $A_H(2^{3k-1}) = [2^{k-u} - 1]$.*

Proof. Since the torsion code of $M_{k,u}^{\alpha}$ is the set of codewords obtained by replacing u by 1 in all u-linear combination of the rows of the matrix, $u.G_{k,u}^{\alpha}$.

We prove by induction with respect to k and t. For $k = 2$ and $u = 1$ the result holds. Suppose the result holds for $k-1$ and $1 \leq u \leq k-2$. Then for k and $1 \leq u \leq k-1$ the matrix $u.G_{k,u}^{\alpha}$ takes the form, $u.G_{k,u}^{\alpha} = [u.G_k^{\alpha} | \frac{0}{u.G_t^{\alpha}}]$. Each non-zero codeword of $u.M_{k,u}^{\alpha}$ has Hamming weight either $2^{3k-1} - 2^{3u-1}$ or 2^{3k-1} and the dimension of the torsion code of $M_{k,t}^{\alpha}$ is k, than there will be $[2^{k-u}(2^u - 1)]$ codewords of Hamming weight $2^{3k-1} - 2^{3u-1}$ and the number of codewords with Hamming weight 2^{3k-1} is $2^{k-u} - 1$. ■

3.2 Secret sharing schemes based on Torsion codes

The access structure of a secret sharing scheme constructed from a linear code is complex. However, since the codewords of a linear code are minimal, we can construct an interesting secret sharing scheme based on its dual code. In the following, we will prove that all the codewords of the torsion codes $C_{k,u,T}^{\alpha}$ are minimal. First, we need the following Lemma to character the minimal codewords of a linear code.

Lemma 5 *In an $[n, k]_q$ linear code C, let $w_{\min}$ and $w_{\max}$ be the minimum and maximum non-zero weights, respectively. If $\frac{w_{\min}}{w_{\max}} > \frac{q-1}{q}$, then all the codewords of C are minial. Let $G^{\alpha}_{k,u,T}$ be the generator matrices of $C^{\alpha}_{k,u,T}$. We have the following result.*

Theorem 6 *In the secret sharing scheme based on $C^{\alpha\,\perp}_{k,u,T}$, there are $2^{3k}-2^{3u}-1$ participants and p^{k-1} minimal qualified sets. If the i-th column of $G^{\alpha}_{k,u,T}$ is a multiple of the 0-th column of $G^{\alpha}_{k,u,T}$, then participant p_i is in every minimal qualified set. Otherwise each participant p_i is involved in exactly $(p-1)p^{k-2}$ out of p^{k-1} minimal qualified sets.*

Proof. Let $w_{\min}$ and $w_{\max}$ be the minimum and maximum nonzero weights in the torsion code $C^{\alpha}_{k,u,T}$. From Theorem 4 in [13] , we know that $w_{\min} = (2^{3k-1} - 2^{3u-1})$ and $w_{\max} = (2^{3k-1})$. Then we have;

$$\frac{w_{\min}}{w_{\max}} = \frac{2^{3k-1} - 2^{3u-1}}{2^{3k-1}} = 1 - \frac{1}{2^{3(k-u)}} > \frac{p-1}{p} = \frac{1}{2}$$

where $1 \leq u \leq k-1$. From Lemma 5, we have that all the codewords of $C^{\alpha}_{k,u,T}$ are minimal. ■

Example 7 *Consider the ring $(F_2 + u\ F_2 + vF_2)$, the code $\phi(M^{\alpha}_{k,t})$ over F_2 of length $n = 56$ generated by $\phi(\Omega^{\alpha}_{2,1})$ defined as follows*

$$1_{56} \otimes \begin{bmatrix} 11111111 & 11111111 & 00000000 & 00000000 & 11111111 & 11111111 & 00000000 \\ 01100110 & 01100110 & 01100110 & 01100110 & 01100110 & 01100110 & 01100110 \end{bmatrix}.$$

The access structure has 55 participants and 2 minimal qualified sets. Each participant P_i, $1 \leq i \leq 55$ in the set $\langle 55 \rangle = \{1, 2, ..., 55\}$ is in 2 minimal access set.

4 Secret Sharing Scheme over F_2RS

The ring $R = FqR_1R_2$ introduced in [15]. We have taken $q = 2$ here. The purpose of this section is to provide the reader with the information necessary to evaluate the analysis of the ring.

$$F_2RS = F_2(F_2 + vF_2)(F_2 + u\ F_2 + vF_2)\ \ .$$

By establishing these foundations, we lay the groundwork for exploring the properties and applications of this ring in coding theory.

$$\begin{aligned} F_2RS &= F_2(F_2 + vF_2)(F_2 + u\ F_2 + vF_2) \\ F_2RS &= \{\sigma = (n_1, n_2, n_3) : n_1 \in F_2, n_2 \in R, n_3 \in S, u^2 = u, v^2 = v, uv = vu = 0\}. \end{aligned}$$

The Lee weight of $c = (\lambda, \mu, v) \in F_2RS$ is defined as $w_{Lee}((\lambda, \mu, v)) = w_{tLee}(\lambda) + w_{tLee}(\mu) + w_{tLee}(v)$.

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

$$\begin{aligned} \phi \quad &: \quad F_2 \times R \times S \longrightarrow F_2^6 \\ (x, y, z) \quad &\longrightarrow \quad \phi(x, y, z) \end{aligned}$$

where $\phi(x, y, z) = (x, a_1, a_1 + b_1, a_2, a_2 + b_2, a_2 + c_2)$, with $y = a_1 + b_1 v$ and $z = a_2 + b_2 u + c_2 v$.

If extending ϕ naturally from $F_2^{\gamma} \times R^{\vartheta_1} \times S^{\vartheta_2}$ to $F_2^{n=\gamma+2\vartheta_1+3\vartheta_2}$, we check that ϕ is a linear isometry.

Theorem 8 *If C is a linear code over F_2RS of lenght n and minimum Lee weight d, then $\phi(c)$ is a linear code with the parameters $[6n, k, d_{Lee} = d_H]$.*

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 non-zero weight of any non-zero 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 9 *[16] Let C be an $[n, k, d_H]$-linear code over F_2 and let $w_{\min}$ and $w_{\max}$ be the minimum and maximum nonzero weights of C, respectively. If $w_{\min}/w_{\max} \geq (p-1)/p$, then all nonzero codewords of $c$are minimal. We require the idea of minimal codewords to find the minimal access sets.*

Remark 10 *[18] 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 with parameters $[n, k, d]$ corrects $t = [\frac{d-1}{2}]$ errors, so its generator matrix is $G = [I_k|A]$, and its parity-check matrix is $H = [-A^t|I_{n-k}]$. This code can be used to establish secret sharing schemes.

4.1 Simplex and MacDonald codes over F_2RS

In this section, we delve into the detailed study of linear simplex and MacDonald codes over finite ring F_2RS. These codes play an important role in coding theory by providing an error detection and correction method essential for reliable data transmission. By analyzing its concepts and structures, we gain insight into how these codes can be effectively implemented and optimized within the algebraic structure of F_2RS. While linear simplex codes recognize simple structures, MacDonald codes offer advanced error correction techniques suitable for more complex applications. This chapter aims to provide a detailed understanding of these coding techniques by demonstrating their adaptability and benefits to various applications. Based on the definitions and frameworks established in [17], we have:

Definition 11 *The generator matrix of S_k^α, simplex codes of type α over F_2RS, as the concatenation of 2^{5k} copies of the generator matrix of $S^\alpha_{F_2,k}$, 2^{4k} copies of the generator matrix of $S^\alpha_{R,k}$ and 2^{3k} copies of the generator matrix of $S^\alpha_{S,k}$ given by*

$$\Omega_k^\alpha = \left[\begin{array}{c|c|c} \underbrace{G^\alpha_{F_2,k}\cdots G^\alpha_{F_2,k} \mid}_{2^{5k}} & \underbrace{G^\alpha_{R,k}\cdots G^\alpha_{R,k}}_{2^{4k}} & \underbrace{G^\alpha_{S,k}\cdots G^\alpha_{S,k}}_{2^{3k}} \end{array}\right]$$

for $k \geq 1$.

Definition 12 *MacDonald codes $M^\alpha_{k,t}$ is a linear code over F_2RS of length $n = 3.2^{6k} - (2^{5k+t} + 2^{4k+2t} + 2^{3k+3t})$ generated by*

$$\Omega_{k,t}^\alpha = \left[\begin{array}{c|c|c} \underbrace{G^\alpha_{F_2,k,t}\cdots G^\alpha_{F_2,k,t} \mid}_{2^{5k}} & \underbrace{G^\alpha_{R,k,t}\cdots G^\alpha_{R,k,t}}_{2^{4k}} & \underbrace{G^\alpha_{S,k,t}\cdots G^\alpha_{S,k,t}}_{2^{3k}} \end{array}\right]$$

for $k \geq 1$ and $1 \leq t \leq k-1$.

Gray images of linear codes over F_2RS

In this section, we explore the concept of gray images of linear simplex and MacDonald codes over the finite ring F_2RS.

Theorem 13 *Let S_k^α be a F_2RS-simplex code of type α with the minimum Lee weight d_L, then $\phi(S_k^\alpha)$ is a simplex code over F_2 with the length $[6.2^{6k}; k]$.*

Proof. If Ω_k^α is generator matrix of the F_2RS-simplex code S_k^α, then $\phi(\Omega_k^\alpha)$ has the form

$$\phi(\Omega_k^\alpha) = \left[\begin{array}{c} \underbrace{G^\alpha_{F_2,k}\ldots G^\alpha_{F_2,k}}_{6.2^{5k}} \end{array}\right]$$

where $G^\alpha_{F_2,k}$ is a generator matrix of the simplex code $S^\alpha_{F_2,k}$. The result than follows by induction on k. ■

Theorem 14 *Let $M^\alpha_{k,t}$ be a F_2RS MacDonald code of type α and minimum Lee weight d_L. Then $\phi(M^\alpha_{k,t})$ is a MacDonald code over F_2, with the parameters* $[2^k + 2^{2k+1} + 3.2^{3k} - (2^t + 2^{2t+1} + 3.2^{3t})]$.

Proof. The proof employs a similar methodology to that of Theorem 13. Using the format of the generator matrices of the linear codes $\phi(M^\alpha_{k,t})$, we have the following results that give the Hamming weight distributions. ■

Corollary 15 *$\phi(M^\alpha_{k,t})$ linear code with weight distribution* $A_H(0) = 1$, $A_H((2^{k-1} + 2.2^{2k-1} + 3.2^{3k-1}) - (2^{t-1} + 2.2^{2t-1} + 3.2^{3t-1})) = 6(2^k - 2^{k-t})$ *and* $A_H(2^{k-1} + 2.2^{2k-1} + 3.2^{3k-1}) = 6(2^{k-t} - 1)$.

4.2 A minimal linear code over F_2RS

In this section, we explore the concept of minimal linear code over the F_2RS ring and its 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 F_2RS, 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 16 *All nonzero codewords of codes $\phi(M^\alpha_{k,t})$ over F_2 are minimal.*

Proof. Using Corollary Hamming weights distribution, the code $\phi(M^\alpha_{k,t})$ over F_2 satisfied

$$\frac{w_{\min}}{w_{\max}} = \frac{(2^{k-1} + 2.2^{2k-1} + 3.2^{3k-1}) - (2^{t-1} + 2.2^{2t-1} + 3.2^{3t-1})}{2^{k-1} + 2.2^{2k-1} + 3.2^{3k-1}} \geq \frac{p-1}{p}.$$

This theorem leads us to the following remark. ■

Remark 17 *The codes $\phi(M^\alpha_{k,t})$ over F_2 are minimal.*

4.3 Secret sharing scheme based on the minimal linear MacDonald codes

Previously, we mentioned that identifying the access structure of a secret-sharing scheme based on a linear code can be challenging. However, when minimal linear simplex and MacDonald codes are used, the construction of secret-sharing schemes becomes more organized and efficient. Minimal linear codes simplify the process by directly linking each codeword's minimality to the scheme's access structure. This makes it easier to determine which subsets of participants can reconstruct the secret.

These 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 18 *Let $\phi(M_k^\alpha)$ be the linear torsion code over F_2. Then in the secret sharing scheme based on $\phi(M_k^\alpha)^\perp$, there are $\tau = (2^k + 2^{2k+1} + 3.2^{3k}) - (2^t + 2^{2t+1} + 3.2^{3t}) - 1$ participants. Moreover, each participants p_i is involved in $(p-1)p^{(k-2)}$ out of $p^{(k-1)}$ minimal access sets.*

Proof. We can derive the desired outcome by considering Lemma 9 and Theorem 16. ■

Example 19 *Consider the ring $F_2RS = F_2(F_2+vF_2)(F_2+u\ F_2+vF_2)$, the code $\phi(M^{\alpha}_{2,1})$ over F_2 of length $n = 986$ generated by $\phi(\Omega^{\alpha}_{2,1})$ defined as follows*

$$1_{986} \otimes \left[\begin{array}{c|c|c} \underbrace{G^{\alpha}_{F_2,2,1}\ldots G^{\alpha}_{F_2,2,1}}_{1024} & \underbrace{G^{\alpha}_{R,2,1}\ldots G^{\alpha}_{R,2,1}}_{256} & \underbrace{G^{\alpha}_{S,2,1}\ldots G^{\alpha}_{S,2,1}}_{64} \end{array} \right]$$

where

$$G^{\alpha}_{F_2,2,1} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

$$G^{\alpha}_{R,2,1} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

$$G^{\alpha}_{S,2,1} = \begin{bmatrix} 11111111 & 11111111 & 00000000 & 00000000 & 11111111 & 11111111 & 00000000 \\ 01100110 & 01100110 & 01100110 & 01100110 & 01100110 & 01100110 & 01100110 \end{bmatrix}$$

The access structure has 985 participants and 2 minimal qualified sets. Each participant P_i, $1 \leq i \leq 985$ in the set $\langle 985 \rangle = \{1, 2, ..., 985\}$ is in 2 minimal access set.

5 Conclusion

In this paper, we give some interesting access structures of SSS based on torsion codes of MacDonald codes over $F_2+uF_2+vF_2$ where $u^2 = u$, $v^2 = v$, $uv = vu = 0$. Hamming weight distributions of simplex codes of type α are given. Moreover, weight distributions of torsion codes of MacDonald codes are given. The result shows that all of these torsion codes are p-ary two-weight linear codes and all non-zero codewords of these torsion codes are minimal. Therefore, the access structure of SSS is based on a dual code of torsion code can be determined. Then, valuable information about the structure and applications of Linear Simplex and MacDonald Codes over F_2RS is provided. By analyzing the concept of Gray images, Hamming weight distributions and minimal codes, a deeper understanding of the properties of these codes and their importance in secret sharing schemes is obtained. The findings highlight the role of these codes in providing secure data transmission and contributing to the development of robust cryptographic protocols in various fields. This research provides a foundation for future work aimed at optimizing these codes for improved security and efficiency, thus playing a key role in the advancement of secure communication technologies.

References

[1] A. Shamir, How to share a secret, Commun. ACM, 22 (1979) 612-613.

[2] G. R. Blakley, Safeguarding cryptographic keys, Nat. Comp. Conf. 48 (1979), 313-317.

[3] R. J. McEliece, D. V. Sarwate, On sharing secrets and Reed-Solomon codes, Commun. ACM, 24 (1981), 583-584.

[4] J. L. Massey, Minimal codewords and secret sharing, Proceedings of the 6th Joint Swedish-Russian Workshop on Information Theory, (1993) 276-279.

[5] C. Ding, J. Yuan, Covering and secret sharing with linear codes, Discrete Mathematics and Theoretical Computer Science, Springer Berlin Heidelberg, LNCS, 2731, (2003) 11-25.

[6] A. Ashikhmin, A. Barg, Minimal vectors in linear codes, IEEE Trans. Inf. Theory, 44 (1998), 2010-2017.

[7] C. Ding, A. Salomaa, Secret sharing schemes with nice access structures, Fundam. Inf. 73 (2006), 51-63.

[8] J. Yuan, C. Ding, Secret sharing schemes from three classes of linear codes, IEEE Trans. Inf. Theory, 52 (2006), 206-212.

[9] K. Ding, C. Ding, A class of two-weight and three-weight codes and their applications in secret sharing, arXiv: 1503.06512v1, (2015).

[10] J. Qian, W. Ma, Secret sharing schemes from linear codes over finite rings, IEICE Transactions on Fundamentals of Electronics, Commun. Comp. Sci. 95 (2012), 1193-1196.

[11] J. Chen, Y. Huang, B. Fu, J. Li, Secret sharing schemes from a class of linear codes over finite chain ring, J. Comp. Inf. Syst. 9 (2013), 2777-2784.

[12] A. Dertli, Y. Cengellenmis, MacDonald codes over the ring $F_2 + vF_2$, Int. J. Algebra, 5 (2011), 985-991.

[13] R. Dertli, S. Eren, MacDonald Codes over the Ring $F_2 + uF_2 + vF_2$, J. Sci. Arts, 20 (2020), 283-290.

[14] 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, Henk C.A. van Tilborg, Frans M. J. Willems (Eds.), 1994, 41.

[15] K. Gowdhaman, C. Mohan, C. Durairajan, S. Çalkavur, P. Solé, Skew Cyclic and Skew Constacyclic Codes over a mixed Alphabet, Axioms, 13 (2024), 360.

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

[17] K. Chatouh, K. Guenda, T. A. Gulliver, L. Noui, On some classes of linear codes over Z_2Z_4 and their covering radii, J. Appl. Math. Comput. 53 (2017), 201–222.

[18] K. Chatouh, Linear Codes over $Z_pR_1R_2$ and their Applications. Mat. Stud. 62 (2024) 3-10.