Bol. Soc. Paran. Mat.
©SPM – E-ISSN-2175-1188
SPM: www.spm.uem.br/bspm

(3s.) **v. 2026 (44)** : 1–11.
ISSN-0037-8712
doi:10.5269/bspm.77446

Employing Non-Binary Simplex Codes Over $\mathbb{F}_p(\mathbb{F}_p + v\mathbb{F}_p)$ within Various Applications

Karima Chatouh* and Mohammed. M. Al-Ashker

ABSTRACT: This article examines simplex codes categorized as types α and β over $\mathbb{F}_p(\mathbb{F}_p + v\mathbb{F}_p)$, along with exploring the p-array Gray representations of simplex codes of types α and β over the same field. Additionally, the article investigates the covering radius of simplex codes of types α and β over $\mathbb{F}_p(\mathbb{F}_p + v\mathbb{F}_p)$. Lastly, the article delves into the construction of secret sharing schemes utilizing simplex codes over the finite field $\mathbb{F}_p$.

Key Words: Simplex codes, finite non chain rings, additive codes, covering radius, hamming and lee weights.

Contents

1. Introduction

The exploration of simplex codes of types α and β over finite rings presents a compelling avenue within the realm of coding theory, where the refinement of algebraic structures intersects with the imperatives of error-correcting codes. Within the confines of a finite ring, these simplex codes emerge as versatile and effective tools for encoding and decoding information, providing a robust defense against errors during data transmission. The finite ring environment introduces a distinctive array of challenges and possibilities that significantly shape the design and efficacy of simplex codes. Researchers, in delving into the complexities of these codes over finite rings, strive to unveil not just theoretical insights into the algebraic foundations but also practical methodologies for constructing resilient communication systems in settings prone to errors and interruptions, see [1,2,3,11,4,12,13].

The aim of this article is to comprehensively explore and elucidate various aspects of simplex codes, with a particular focus on types α and β over finite ring $\mathbb{F}_p(\mathbb{F}_p + v\mathbb{F}_p)$. The investigation encompasses a detailed examination of the p-array Gray images associated with simplex codes of types α and β over this ring, shedding light on their unique properties and applications. Additionally, the article aims to delve into the covering radius of simplex codes of types α and β over $\mathbb{F}_p(\mathbb{F}_p + v\mathbb{F}_p)$, unraveling the intricacies of

[*] Corresponding author.
2020 *Mathematics Subject Classification:* 16P10, 11T71, 94B05, 11H71, 94B65.
Submitted June 22, 2025. Published December 29, 2025

their error-correcting capabilities. Moreover, the discussion extends to the construction of secret sharing schemes utilizing simplex codes over finite fields $\mathbb{F}_p$, exploring the practical implications of these codes in safeguarding sensitive information through distributed cryptographic mechanisms. Through this comprehensive exploration, the article seeks to contribute to the broader understanding of simplex codes and their diverse applications in coding theory, cryptography, and information security.

The article's structure is outlined as follows: In Section 2, foundational information is presented with two key subsections. Subsection "Hamming and Lee Weights of Linear Codes over $R = \mathbb{F}_p(\mathbb{F}_p + v\mathbb{F}_p)$" elucidates Hamming and Lee weights concepts within linear codes over the ring $\mathbb{F}_p(\mathbb{F}_p + v\mathbb{F}_p)$. The subsequent subsection, "Bounds on the Covering Radius: Upper and Lower Limits," explores covering radius boundaries for linear codes over the same ring. Section 3 focuses on developing simplex codes (types α and β) within $\mathbb{F}_p(\mathbb{F}_p+v\mathbb{F}_p)$. Section 4 computes Gray images for simplex codes of types α and β over $\mathbb{F}_p(\mathbb{F}_p+v\mathbb{F}_p)$. Section 5 scrutinizes the covering radius of simplex codes types α and β over the same ring, exploring related properties, computational techniques, and bounds. Section 6 delves into access structures inherent in secret sharing schemes based on Gray images from $\mathbb{F}_p(\mathbb{F}_p + v\mathbb{F}_p)$-simplex codes of type β, highlighting their functionality and interaction in secret sharing contexts.

2. Context and Preliminaries

In this section, we present our initial findings drawing from references [16], [17], and [19]. We focus on introducing the rings of integers modulo p, denoted as $\mathbb{F}_p$, where p is an odd prime. Additionally, we establish the concept of $\mathbb{F}_p+v\mathbb{F}_p$, a collection comprising elements such as $0, 1, 2, \cdots, (p-1), v, 2v, \cdots, (p-1) + v(p-1)$, where the condition $v^2 = v$ holds. Sets of n-tuples within these rings are denoted by $\mathbb{F}_p^n$ and $(\mathbb{F}_p + v\mathbb{F}_p)^n$. We recall that the ring $\mathbb{F}_p(\mathbb{F}_p + v\mathbb{F}_p)$ can be written in the following set form

$$\mathbb{F}_p(\mathbb{F}_p + v\mathbb{F}_p) = \{\, a + vb \mid a, b \in \mathbb{F}_p,\ v^2 = v \,\}.$$

For instance, when $p = 3$, the elements are explicitly

$$\mathbb{F}_3(\mathbb{F}_3 + v\mathbb{F}_3) = \{\, 0, 1, 2, v, 2v, 1 + v, 2 + v, 1 + 2v, 2 + 2v \,\}.$$

We introduce the ring $R = \mathbb{F}_p(\mathbb{F}_p+v\mathbb{F}_p)$ and define a non-empty set C as an R-additive code, forming a subgroup of $\mathbb{F}_p^\gamma \times (\mathbb{F}_p + v\mathbb{F}_p)^\delta$, demonstrating its isomorphism to $\mathbb{F}_p^\lambda \times (\mathbb{F}_p + v\mathbb{F}_p)^\mu$. The group type attributed to C is denoted as $p^{\lambda+2\mu}$, signifying that C encompasses $|C| = p^{\lambda+2\mu}$ codewords. Moreover, within C, the count of distinct orders for any two codewords also equals $|C| = p^{\lambda+2\mu}$. We introduce the concept of a linear code C with length n over R.

2.1. Weights of Linear codes over $\mathbb{F}_p(\mathbb{F}_p + v\mathbb{F}_p)$

The Hamming weight and Lee weight play pivotal roles in characterizing vector attributes within the ring framework, holding vital importance in coding and error-correction methodologies. In $(\mathbb{F}_p + v\mathbb{F}_p)^n$, the Hamming weight quantifies the count of non-zero elements, while the Lee weight, tailored to the ring structure of $R = \mathbb{F}_p(\mathbb{F}_p + v\mathbb{F}_p)$, focuses on elements not equal to zero. The Gray (or Lee) weight, introduced in [20], further refines these concepts for elements within $(\mathbb{F}_p + v\mathbb{F}_p)$.

The Gray(or Lee) weight for the codeword $x = (x_1, x_2, \ldots, x_n) \in (\mathbb{F}_p + v\mathbb{F}_p)^n$ is defined by,

$$wt_L(x) = \sum_{i=1}^{n} wt_L(x_i), \tag{2.1}$$

where the Gray(or Lee) weight on $(\mathbb{F}_p + v\mathbb{F}_p)$ is a weight function on $(\mathbb{F}_p + v\mathbb{F}_p)$ defined as

$$wt_L(x_i = t_i + vq_i) = \begin{cases} 0 & \text{if} \quad x_i = 0 \\ 1 & \text{if} \quad t_i \neq 0, q_i = 0 \\ 1 & \text{if} \quad q_i \neq 0, 2t_i + q_i \equiv\ 0\ (mod\ p) \\ 2 & \text{if} \quad q_i \neq 0, 2t_i + q_i \not\equiv\ 0\ (mod\ p) \end{cases} \tag{2.2}$$

The minimum Hamming weight $wt_H(C)$ and the minimum Lee weight $wt_L(C)$ of code C are defined analogously. For $x = (x_1, x_2, \dots, x_n), (y_1, y_2, \dots, y_n) \in (\mathbb{F}_p + v\mathbb{F}_p)^n$, $d_H(x, y) = |\{i|x_i \neq y_i\}|$ is called distance between x and $y \in R^n$ is denoted, $d_H(x, y) = wt_H(x - y)$. The minimum Hamming distance between distinct pairs of codewords of a code C is called the minimum Hamming distance of C and denoted by $d_H(C)$ or shortly d_H. The Gray (or Lee) distance distance between x and $y \in (\mathbb{F}_p + v\mathbb{F}_p)^n$ is defined by,

$$d_L(x, y) = wt_L(x - y) = \sum_{i=1}^{n} wt_L(x_i - y_i).$$

The minimum Lee distance between distinct pairs of codewords of a code C are called the minimum Lee distance of C and denoted by $d_L(C)$ or shortly d_L. If C is a linear code, $d_H(C) = wt_H(C)$, $d_L(C) = wt_L(C)$. A generator matrix of C is a matrix whose rows generate C. Two codes are equivalent if one can be obtained from the other by permuting the coordinates.

The Gray map ϕ from $(\mathbb{F}_p + v\mathbb{F}_p)^n$ to $\mathbb{F}_p^{2n}$ is defined in [20] as:

$$\phi : (\mathbb{F}_p + v\mathbb{F}_p)^n \rightarrow F_p^{2n}, \tag{2.3}$$

$$x + vy \rightarrow (-y, 2x + y)$$

where $x, y \in \mathbb{F}_p^n$. The Gray(or Lee) weight of $x + vy$ is the Hamming weight of its Gray image. Note that ϕ is $\mathbb{F}_p$ linear.

The extension of the Gray map $\rho : \mathbb{F}_p^\gamma \times (\mathbb{F}_p + v\mathbb{F}_p)^\delta \rightarrow \mathbb{F}_p^n$, where $n = \gamma + 2\delta$ is given by $\rho(u, w) = (u, \phi(w_1), \cdots, \phi(w_\delta)), \forall u \in \mathbb{F}_p^\gamma$ and $(w_1, \cdots, w_\delta) \in (\mathbb{F}_p + v\mathbb{F}_p)^\delta$. Then the image of a R-additive code under the extended Gray map is a $\mathbb{F}_p$ linear code of length $n = \gamma + 2\delta$. The Hamming weight of u denoted by $w_H(u)$ and $w_L(w)$ be the Lee weight of w, where $u \in \mathbb{F}_p^\gamma$ and $w \in (\mathbb{F}_p + v\mathbb{F}_p)^\delta$.

Here, D refers to the Lee weight function defined on $(\mathbb{F}_p + v\mathbb{F}_p)$. Thus, for $x = (u, w) \in \mathbb{F}_p^\gamma \times (\mathbb{F}_p + v\mathbb{F}_p)^\delta$, we define

$$w_D(x) = w_H(u) + w_L(w),$$

where $w_H(u)$ is the Hamming weight of $u \in \mathbb{F}_p^\gamma$, and $w_L(w)$ is the Lee weight of $w \in (\mathbb{F}_p + v\mathbb{F}_p)^\delta$. The Gray map defined above is a ring isomorphism.

2.2. Investigating and Expanding Limits on the Covering Radius of Codes over $\mathbb{F}_p(\mathbb{F}_p + v\mathbb{F}_p)$

Within this section, our journey sets sail into an in-depth exploration of both the upper and lower thresholds on the covering radius within a code established over the ring $\mathbb{F}_p(\mathbb{F}_p + v\mathbb{F}_p)$. The covering radius, a pivotal parameter within the realm of coding theory, assumes a substantial role in quantifying the utmost distance separating any given codeword and its nearest counterpart located outside the code. References such as [9] and [15] have already laid down the foundation by furnishing covering radii for a code denoted as C, encompassing distances such as the Lee, Euclidean, and Chinese Euclidean measures. Now, our specific focus lies in the articulation of the covering radii within codes C over $\mathbb{F}_p(\mathbb{F}_p + v\mathbb{F}_p)$, with particular attention directed towards the Lee and Bachoc distances.

The covering radius of a code C over $\mathbb{F}_p(\mathbb{F}_p + v\mathbb{F}_p)$ is defined as follows:

$$r_D(C) = \max_{x \in \mathbb{F}_p^\gamma \times (\mathbb{F}_p + v\mathbb{F}_p)^\delta} \left\{ \min_{c \in C} d_L(x, c) \right\}, \tag{2.4}$$

where $r_D(C)$ represents the covering radius, $\mathbb{F}_p^\gamma \times (\mathbb{F}_p + v\mathbb{F}_p)^\delta$ denotes the Cartesian product of $\mathbb{F}_p^\gamma$ and $(\mathbb{F}_p + v\mathbb{F}_p)^\delta$, and $d_L(x, c)$ represents the Lee distance between a vector x and a codeword c.

Moreover, the set $\mathbb{F}_p^\gamma \times (\mathbb{F}_p + v\mathbb{F}_p)^\delta$ can be expressed as the union of spheres centered around each codeword in C with a radius equal to the covering radius $r_D(C)$, as given by:

$$\mathbb{F}_p^\gamma \times (\mathbb{F}_p + v\mathbb{F}_p)^\delta = \cup_{c \in C} S_{r_D}(c), \tag{2.5}$$

where $S_{r_D}(x)$ denotes the sphere of vectors in $\mathbb{F}_p^{\gamma} \times (\mathbb{F}_p + v\mathbb{F}_p)^{\delta}$ with a distance at most r_D from a given codeword c.

The exploration into these limits on covering radii holds paramount importance in comprehending the error-correction potential inherent in codes over $\mathbb{F}_p(\mathbb{F}_p + v\mathbb{F}_p)$. In the ensuing sections, we will plunge deeper into the ramifications stemming from these boundaries and their influence on the effectiveness of diverse coding methodologies. Additionally, we will investigate approaches to streamline the design of codes within real-world applications, thereby striving to augment both the dependability and effectiveness of coding systems predicated on the adopted ring configuration.

Definition 2.1 *For a binary linear code C without a zero coordinate, $r_D(C) = \lfloor \frac{n(C)}{2} \rfloor$.*

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

The subsequent outcome holds great significance as it offers a method to ascertain the covering radius for codes established over the ring $\mathbb{F}_p(\mathbb{F}_p + v\mathbb{F}_p)$.

Proposition 2.3 *If C_0 and C_1 are codes over $\mathbb{F}_p(\mathbb{F}_p + v\mathbb{F}_p)$ has length n_0 and n_1, of minimum distance d_0 and d_1, generated by matrices G_0 and G_1, respectively, and if C is the code generated by*

$$G = \left(\begin{array}{c|c} 0 & G_1 \\ \hline G_0 & A \end{array} \right),$$

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

$$r_d(C_c) \geq r_d(C_0) + r_d(C_1),$$

for all distances d over $\mathbb{F}_p(\mathbb{F}_p + v\mathbb{F}_p)$.

2.3. Utilizing Linear Codes in the Context of Secret Sharing Schemes

Consider a generator matrix $G = (g_0, g_1, \ldots, g_{n-1})$ for an $C = [n, k, d; p]$-code. This matrix G consists of row vectors that effectively create the linear subspace C. In a secret sharing arrangement based on C, the confidential value is an element taken from $\mathbb{F}_p$. This sharing setup involves a dealer P_0 and $n-1$ parties, namely $P_1, P_2, \ldots, P_{n-1}$.

For the purpose of computing shares associated with a secret value s, the dealer employs a random selection of a vector denoted as $u = (u_0, u_1, \ldots, u_{k-1})$ originating from $\mathbb{F}_p^k$, ensuring that s can be represented as the result of ug_0. Within $\mathbb{F}_p^k$, there exist p^{k-1} such vectors u conforming to this criterion. Subsequently, the dealer treats the vector u as information and proceeds to compute the corresponding codeword $v = uG = (v_0, v_1, \ldots, v_{n-1})$. This computed codeword's components are then distributed to the respective parties, with P_i receiving v_i as their designated share, where $1 \leq i \leq n-1$. In cases where $s = v_0 = ug_0$ holds true, a collection of shares $(v_{i_1}, v_{i_2}, \ldots, v_{i_m})$ is capable of uniquely determining the secret s if and only if the column g_0 within matrix G can be expressed as a linear combination of columns $g_{i_1}, g_{i_2}, \ldots, g_{i_m}$ within the same matrix G. This leads to the establishment of the ensuing proposition as detailed in [14].

Proposition 2.4 *Let G be a generator matrix of an $[n; k; d]$ code C over $\mathbb{F}_p$. In the secret sharing scheme based on C, a set of shares $(v_{i_1}, v_{i_2}, \cdots, v_{i_m})$ determines the secret if and only if there is a codeword*

$$(1, 0, \cdots, 0, c_{i_1}, 0, \cdots, c_{i_m}, 0, \cdots, 0),$$

in $C^{\perp}$ with $c_{i_j} \neq 0$ for at least one j, $1 \leqslant i_1 \leqslant \cdots \leqslant i_m \leqslant n-1$ and $1 \leqslant m \leqslant n-1$.

When presented with a codeword as outlined in Proposition 2.4, the scenario arises where g_0 can be expressed as the summation $\sum_{j=1}^{m} a_j g_{i_j}$. As a result of this configuration, the retrieval of the secret value s is accomplished through the calculation given by

$$s = \sum_{j=1}^{m} a_j v_{i_j}. \tag{2.6}$$

Theorem 2.5 ([8]) *Let C be an $[n;k;d]$ linear code over $\mathbb{F}_p$ with generator matrix*

$$G = [g_0, g_1, \cdots, g_{n-1}],$$

and let $C^\perp$ be its dual code with minimum distance $d^\perp$. If each nonzero codeword of C is minimal, then in the secret sharing scheme based on $C^\perp$ there are p^{k-1} minimal access sets. in addition, we have the following.

1. *If $d^\perp = 2$ then*

   i) if g_i is a multiple of g_0, $1 \leqslant i \leqslant n-1$, then participant P_i must be in every minimal access set, and

   ii) if g_i is not a multiple of g_0, $1 \leqslant i \leqslant n-1$, then participant P_i must be in $(p-1)p^{k-2}$ minimal access sets.

2. *If $d^\perp \geqslant 2$, for $1 \leqslant t \leqslant min\{k-1, d^\perp - 1\}$, then every group of t participants is involved in $(p-1)^t p^{k-(t+1)}$ minimal access sets.*

The sufficient condition is obtained from the weights as described in the following lemma.

Lemma 2.6 ([8]) *Let C be an $[n;k;d]$ 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.

3. Simplex Codes of Types α and β over $\mathbb{F}_p(\mathbb{F}_p + v\mathbb{F}_p)$

In this segment, we focus on the investigation of simplex code of type α and β. Every type is associated with a specific collection of fundamental vectors, thereby signifying a unique code structure. The formulation of these codes entails a methodical approach of selecting appropriate foundational vectors and systematically generating all potential codewords through linear amalgamations.

Let $T^\alpha_{p,k}$ be the generator matrix of $S^\alpha_{p,k}$, the simplex code of type α over $\mathbb{F}_p$,

$$T^\alpha_{p,k} = \left(\begin{array}{c|c|c|c} 00\cdots0 & 11\cdots1 & \cdots & (p-1)(p-1)\cdots(p-1) \\ \hline T^\alpha_{p,k-1} & T^\alpha_{p,k-1} & \cdots & T^\alpha_{p,k-1} \end{array}\right), \ for\ k \geq 2, \tag{3.1}$$

with $T^\alpha_{p,1} = (012\cdots(p-1))$. In [18] the simplex codes $S^\alpha_{p^2,k}$ of type α over the ring $\mathbb{F}_p + v\mathbb{F}_p$ were defined. The generator matrix $G^\alpha_{p^2,k}$ of $S^\alpha_{p^2,k}$ is a $k \times p^{2k}$ matrix over $\mathbb{F}_p + v\mathbb{F}_p$ defined inductively by,

$$G^\alpha_{p^2,k} = \left(\begin{array}{c|c|c|c} 0\ldots0 & 1\ldots1 & \ldots & (p-1)+v(p-1)\cdots(p-1)+v(p-1) \\ \hline G^\alpha_{p^2,k-1} & G^\alpha_{p^2,k-1} & \ldots & G^\alpha_{p^2,k-1} \end{array}\right), \tag{3.2}$$

where

$$G^\alpha_{p^2,1} = \left(\begin{array}{ccccccccc} 0 & 1 & \ldots & (p-1) & v & \ldots & v(p-1) & \ldots & (p-1)+v(p-1) \end{array}\right)$$

The columns of $G^\alpha_{p^2,k}$ consist of all distinct k-tuples over $(\mathbb{F}_p + v\mathbb{F}_p)$. The code $S^\alpha_{p^2,k}$ generated by $G^\alpha_{p^2,k}$ has length p^{2k}.

We define the generator matrix of S^α_k, the simplex code of type $\mathbb{F}_p(\mathbb{F}_p + v\mathbb{F}_p)$ as the concatenation of p^{2k} copies of the generator matrix of $S^\alpha_{p,k}$ and p^k copies of the generator matrix of $S^\alpha_{p^2,k}$, given by

$$\mathfrak{G}^\alpha_k = \left(\begin{array}{c|c} 1_{p^{2k}} \otimes T^\alpha_{p,k} & 1_{p^k} \otimes G^\alpha_{p^2,k} \end{array}\right), for\ k \geq 1. \tag{3.3}$$

The length of the simplex code of type α over $\mathbb{F}_p(\mathbb{F}_p + v\mathbb{F}_p)$ is equal to $2p^{3k}$ and the number of codewords is equal to p^k for some k.

The type β of the simplex codes S_k^β over $\mathbb{F}_p(\mathbb{F}_p+v\mathbb{F}_p)$ is a punctured version of S_k^α. The number of codewords is p^k and its length is $2\left(\frac{(p^k-1)}{(p-1)}\right)\left(\frac{(p^{2k+1}+p^{2k}-2p^{k+1}-2p^k+p+1)}{(p+1)(p-1)^2}\right)$. The generator matrix of S_k^β is the concatenation of $\frac{(p^{2k+1}+p^{2k}-2p^{k+1}-2p^k+p+1)}{(p+1)(p-1)^2}$ copies of the generator matrix of the simplex code $S_{p,k}^\beta$ over $\mathbb{F}_p$ and $\frac{(p^k-1)}{(p-1)}$ copies of the generator matrix of the simplex code $S_{p^2,k}^\beta$ over $\mathbb{F}_p+v\mathbb{F}_p$, given by

$$\mathfrak{G}_k^\beta=\left(\begin{array}{c|c} 1_{\frac{(p^{2k+1}+p^{2k}-2p^{k+1}-2p^k+p+1)}{(p+1)(p-1)^2}}\otimes T_{p,k}^\beta & 1_{\frac{(p^k-1)}{(p-1)}}\otimes G_{p^2,k}^\beta \end{array}\right), for\ k\geq 1, \tag{3.4}$$

where $T_{p,k}^\beta$ is the generator matrix of the ternary simplex code of type β given by

$$T_{p,k}^\beta=\left(\begin{array}{c|c} 11\cdots 1 & 00\cdots 0\\ \hline T_{p,k-1}^\alpha & T_{p,k-1}^\beta \end{array}\right), \tag{3.5}$$

for $k\geq 3$, with $T_{p,2}^\beta=\left(\begin{array}{c|c} 11\cdots 1 & 0\\ \hline 01\cdots(p-1) & 1\end{array}\right)$ and $G_{p^2,k}^\beta$ is a generator matrix of the simplex code $S_{p^2,k}^\beta$ over $\mathbb{F}_p+v\mathbb{F}_p$ of type β defined inductively as in [18] by the following,
for $k=2$, Let λ_k be the $k\times\frac{p^{2k}-p^k}{p-1}$ matrix over $\mathbb{F}_p+v\mathbb{F}_p$ defined inductively by $\lambda_1=(12\cdots(p-1)\ v)$ and

$$\lambda_2=\left(\begin{array}{c|c|c|c|c|c|c|c|c} \mathbf{0} & \mathbf{1} & \cdots & \mathbf{p-1} & \mathbf{v} & \mathbf{1+(p-1)v} & \mathbf{2+(p-2)v} & \cdots & \mathbf{p-1+v}\\ \hline \lambda_1 & G_{p^2,1}^\alpha & \cdots & G_{p^2,1}^\alpha & G_{p^2,1}^\alpha & \lambda_1 & \lambda_1 & \cdots & \lambda_1 \end{array}\right) \tag{3.6}$$

λ_k is constructed inductively as follows

$$\lambda_k=\left(\begin{array}{c|c|c|c|c|c|c|c|c|c} \mathbf{0} & \mathbf{1} & \mathbf{2} & \cdots & \mathbf{p-1} & \mathbf{v} & \mathbf{1+(p-1)v} & \mathbf{2+(p-2)v} & \cdots & \mathbf{p-1+v}\\ \hline \lambda_{k-1} & G_{p^2,k-1}^\alpha & G_{p^2,k-1}^\alpha & \cdots & G_{p^2,k-1}^\alpha & G_{p^2,k-1}^\alpha & \lambda_{k-1} & \lambda_{k-1} & \cdots & \lambda_{k-1} \end{array}\right). \tag{3.7}$$

Let δ_k be a matrix of size $k\times\frac{p^{2k}-p^k}{p-1}$ over $\mathbb{F}_p+v\mathbb{F}_p$. Let $\delta_1=[12\cdots p-1\ p-1+v]$ and

$$\delta_2=\left(\begin{array}{c|c|c|c|c|c|c|c|c|c} \mathbf{0} & \mathbf{1} & \mathbf{2} & \cdots & \mathbf{p-1} & \mathbf{p-1+v} & \mathbf{v} & \mathbf{2v} & \cdots & \mathbf{(p-1)v}\\ \hline \delta_1 & G_{p^2,1}^\alpha & G_{p^2,1}^\alpha & \cdots & G_{p^2,1}^\alpha & G_{p^2,1}^\alpha & \delta_1 & \delta_1 & \cdots & \delta_1 \end{array}\right). \tag{3.8}$$

δ_k is constructed inductively as follows

$$\delta_k=\left(\begin{array}{c|c|c|c|c|c|c|c|c|c} \mathbf{0} & \mathbf{1} & \mathbf{2} & \cdots & \mathbf{p-1} & \mathbf{p-1+v} & \mathbf{v} & \mathbf{2v} & \cdots & \mathbf{(p-1)v}\\ \hline \delta_1 & G_{p^2,1}^\alpha & G_{p^2,k-1}^\alpha & \cdots & G_{p^2,k-1}^\alpha & G_{p^2,k-1}^\alpha & \delta_{k-1} & \lambda_{k-1} & \cdots & \lambda_{k-1} \end{array}\right). \tag{3.9}$$

Let $G_{P^2,k}^\beta$ $(k\geq 2)$ be matrix the generator of $S_{P^2,k}^\beta$. The size of $G_{P^2,k}^\beta$ is

$$k\times\frac{(p^{2k+1}+p^{2k}-2p^{k+1}-2p^k+p+1)}{(p+1)(p-1)^2}$$

. The matrix $G_{P^2,2}^\beta$ is as follows

$$G_{P^2,2}^\beta=\left(\begin{array}{c|c|c|c} \mathbf{1} & 0 & \mathbf{v} & \mathbf{(p-1)+v}\\ \hline G_{p^2,1}^\alpha & 1 & 12\cdots(p-1)\ (p-1+v) & 1\cdots(p-1)\ v \end{array}\right). \tag{3.10}$$

$G_{P^2,k}^\beta$ is constructed inductively as follows

$$G^{\beta}_{P^2,k} = \left(\begin{array}{c|c|c|c} \mathbf{1} & \mathbf{0} & \mathbf{v} & \mathbf{(p-1+v)} \\ \hline G^{\alpha}_{p^2,k-1} & G^{\beta}_{p^2,k-1} & \delta_{k-1} & \lambda_{k-1} \end{array}\right). \tag{3.11}$$

Using the induction method, we can readily verify that no two columns within $G^{\beta}_{p^2,k}$ are proportional to each other. This systematic mathematical technique enables us to establish this property in a structured manner. To delve deeper, $G^{\beta}_{p^2,k}$ denotes a particular mathematical entity, and the conclusion drawn through induction applies universally to all instances of this matrix. The proof of this assertion is both straightforward and comprehensive, underscoring the potency and adaptability of the induction principle when addressing such mathematical investigations.

4. The p-array Gray Images of Simplex Codes over $\mathbb{F}_p(\mathbb{F}_p + v\mathbb{F}_p)$ of Types α and β

In this section, we explore the concept of Gray images in the context of simplex codes over the algebraic structure $\mathbb{F}_p(\mathbb{F}_p + v\mathbb{F}_p)$ of types α and β. The fundamental idea behind Gray images lies in representing these simplex codes through a concatenation of simplex codes over $\mathbb{F}_p$, specifically categorized into types α and β. The process of constructing Gray images involves systematically organizing and combining these simplex codes over $\mathbb{F}_p$, resulting in a compact and efficient representation of the original simplex codes. To achieve this, we introduce a significant theorem that precisely outlines the procedure for generating the Gray images corresponding to types α and β.

Theorem 4.1 *Let S^{α}_k represent a $\mathbb{F}_p(\mathbb{F}_p + v\mathbb{F}_p)$-simplex code of type α with a minimum weight denoted as d. When we apply the mapping ρ to S^{α}_k, the resulting code is obtained by combining $6 \cdot p^{(p-1)k+1}$ instances of the p-array simplex code with the following parameters: length $6 \cdot p^{pk+1}$, dimension k, and Hamming distance $d_H = 6 \cdot p^{pk-1}$.*

Proof 4.2 *When considering the generator matrix $\mathfrak{G}^{\alpha}_k$ for the $\mathbb{F}_p(\mathbb{F}_p + v\mathbb{F}_p)$-simplex code S^{α}_k, the formula representing $\rho(\mathfrak{G}^{\alpha}_k)$ takes the following form:*

$$\rho(\mathfrak{G}^{\alpha}_k) = \left(\overbrace{T^{\alpha}_{p,k} \mid T^{\alpha}_{p,k} \mid \cdots \mid T^{\alpha}_{p,k}}^{6 \cdot p^{(p-1)k+1}} \right),$$

where $T^{\alpha}_{p,k}$ signifies the generator matrix of the p-array simplex code $S^{\alpha}_{p,k}$. This relation can be established through an inductive approach with respect to k, validating the uniformity of $\rho(\mathfrak{G}^{\alpha}_k)$ across various values of k. To recapitulate, the provided equation defines the configuration of $\rho(\mathfrak{G}^{\alpha}_k)$ based on the generator matrix $T^{\alpha}_{p,k}$ of the p-array simplex code $S^{\alpha}_{p,k}$. Additionally, the induction performed on k serves to establish the validity of this expression for all conceivable values of k.

Theorem 4.3 *Let S^{β}_k represent a $\mathbb{F}_p(\mathbb{F}_p + v\mathbb{F}_p)$-simplex code of type β with a minimum weight denoted as d. When we apply the mapping ρ to S^{β}_k, the resulting code is obtained by combining*

$$6\left(\frac{(p^{2k+1} + p^{2k} - 2p^{k+1} - 2p^k + p + 1)}{(p+1)(p-1)^2}\right), \tag{4.1}$$

instances of the p-array simplex code with the following parameters: length

$$6\left(\frac{(p^k - 1)}{(p-1)}\right)\left(\frac{(p^{2k+1} + p^{2k} - 2p^{k+1} - 2p^k + p + 1)}{(p+1)(p-1)^2}\right), \tag{4.2}$$

and dimension k.

Proof 4.4 *The proof exhibits similarities to the one outlined in Theorem 4.1.*

5. The Covering Radius of Simplex Codes over $\mathbb{F}_p(\mathbb{F}_p + v\mathbb{F}_p)$ of Types α and β

The following theorems provide the covering radius of simplex codes with types α and β over the ring $\mathbb{F}_p(\mathbb{F}_p + v\mathbb{F}_p)$.

Theorem 5.1 *The covering radii of the $\mathbb{F}_p(\mathbb{F}_p + v\mathbb{F}_p)$-simplex codes of type α and β are determined*

1. $r_L(S_k^{\alpha}) \leq p^{3k}\,(p-1)\left(1+p^k\right)$,
2. $r_L(S_k^{\beta}) \leq \dfrac{p^{3k}\left(p^{k+2}+p^3+1\right)-p^{2k}\left(p^{2k}+2p^3+2p^2\right)+p^3\,(1+p)}{p^3\,(p^2-1)}$.

Proof 5.2 *1. Following [6] and regarding the code S_k^{α} and its association with the Lee weight, there exists certain available information*

$$\begin{aligned} r_L(S_k^{\alpha}) &\leq r_L(p^{2k}S_{p,k}^{\alpha}) + r_L(p^kS_{p^2,k}^{\alpha}) \\ &\leq p^{2k}r_L(S_{p,k}^{\alpha}) + p^kr_L(S_{p^2,k}^{\alpha}) \\ &\leq p^{2k}r_H(S_{p,k}^{\alpha}) + p^kr_L(S_{p^2,k}^{\alpha}) \\ &\leq p^{2k}\left(p^{k-1}\,(p-1)\right) + p^k\left(p^{3k-1}\,(p-1)\right) \\ &\leq p^{3k}\,(p-1)\left(1+p^k\right). \end{aligned}$$

2. The code S_k^{β} and its correlation with the Lee weight have some available information.

$$\begin{aligned} r_L(S_k^{\beta}) &\leq \frac{(p^{2k+1}+p^{2k}-2p^{k+1}-2p^k+p+1)}{(p+1)(p-1)^2}\left(p^{k-1}\,(p-1)\right) + \frac{p^k-1}{p-1}\left(p^{3k-3}\,(p-1)\right) \\ &\leq \frac{p^{3k}\left(p^{k+2}+p^3+1\right)-p^{2k}\left(p^{2k}+2p^3+2p^2\right)+p^3\,(1+p)}{p^3\,(p^2-1)}. \end{aligned}$$

5.1. Covering Radius of Gray Images for these Simplex Codes

Studying simplex codes over $\mathbb{F}_p(\mathbb{F}_p+v\mathbb{F}_p)$ with types α and β involves a key factor called the covering radius of Gray images. This factor decides the smallest radius needed to cover all codewords when they're projected onto the p-array Gray images.

Theorem 5.3 *For the Gray images of $\mathbb{F}_p(\mathbb{F}_p + v\mathbb{F}_p)$-simplex codes of types α and β the values of their covering radii are exclusively determined by the parameters characterizing these codes.*

1. $r_H\left(\rho\left(S_k^{\alpha}\right)\right) = 6 \times p^{6k-1}$,
2. $r_H\left(\rho\left(S_k^{\beta}\right)\right) = 6\left(\dfrac{p^{k-1}}{p-1}\right)\left(p^{2k}-2p^k+1\right)$,

Proof 5.4 *To demonstrate the validity of the statement, leverage the theorems provided in references [5] and [10] as supporting evidence.*

6. Constructing Secret Sharing Schemes Using Simplex Codes over Finite Fields $\mathbb{F}_p$

Within this section, our focus centers on a category of Gray images that pertain to linear codes existing over a finite ring. Notably, we delve into the simplex codes of type β, utilizing these Gray images as a foundational element for the creation of secret sharing schemes.

Proposition 6.1 *Every nontrivial codeword within a code $\rho(S_k^{\beta})$ over $\mathbb{F}_p$ are minimal.*

Proof 6.2 *Following the result from reference [6], it can be observed that $w_{min}(\rho(S_k^{\beta}))$ is equal to $w_{max}(\rho(S_k^{\beta}))$. As a consequence of Lemma 2.6, all non-zero codewords of $\rho(S_k^{\beta})$ are established to be minimal.*

This theorem gives rise to the subsequent observation.

Remark 6.3 *The code $\rho(S_k^\beta)$ over $\mathbb{F}_p$ are minimal.*

Theorem 6.4 *Consider the linear code $\rho(S_k^\beta)$ over $\mathbb{F}_p$. In the secret sharing scheme based on $\rho(S_k^\beta)^\perp$. There are $p^{(k-1)}$ minimal access sets and*

$$6\left(\frac{(p^k-1)}{(p-1)}\right)\left(\frac{(p^{2k+1}+p^{2k}-2p^{k+1}-2p^k+p+1)}{(p+1)(p-1)^2}\right)-1 \tag{6.1}$$

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

Proof 6.5 *The outcome is a consequence of Proposition 6.1 in conjunction with Theorems 2.5 and 4.3.*

6.1. Illustrative Instances of Application

Application 1 In situations where p takes the value 2, we will investigate the ring labeled as $R=\mathbb{F}_2(\mathbb{F}_2+u\mathbb{F}_2)$, and center our attention on the Gray image code $\rho(S_4^\beta)$ where the parameter k is fixed at 4. Subsequently,

$$\rho\left(\mathfrak{G}_4^\beta\right)=\left(\ 1_{1350}\otimes T_{2,4}^\beta\ \right),\ \textit{where}\ T_{2,4}^\beta=\begin{pmatrix}111111110000000\\000011111111000\\001100110011110\\010101010101011\end{pmatrix}.$$

The Gray image code $\rho(S_4^\beta)$ is classified as a binary $[20250;4;10800]$ code. We establish the secret sharing scheme using the dual of $\rho(S_4^\beta)$, denoted as $\rho(S_4^\beta)$. In this context,

$$\rho(S_4^\beta)=\left\{\begin{array}{ll}c_0=1_{1350}\otimes(000000000000000), & c_8=1_{1350}\otimes(011001100110101),\\ c_1=1_{1350}\otimes(111111110000000), & c_9=1_{1350}\otimes(001111001100110),\\ c_2=1_{1350}\otimes(000011111111000), & c_{10}=1_{1350}\otimes(010110101010011),\\ c_3=1_{1350}\otimes(001100110011110), & c_{11}=1_{1350}\otimes(110000111100110),\\ c_4=1_{1350}\otimes(010101010101011), & c_{12}=1_{1350}\otimes(100110010110101),\\ c_5=1_{1350}\otimes(111100001111000), & c_{13}=1_{1350}\otimes(011010011001101),\\ c_6=1_{1350}\otimes(110011000011110), & c_{14}=1_{1350}\otimes(101001011010011),\\ c_7=1_{1350}\otimes(101010100101011), & c_{15}=1_{1350}\otimes(100101101001101)\end{array}\right\}.$$

Within the related access arrangement, there are a total of 20249 participants and a set of 8 minimal qualifying subsets, detailed as follows

$$\begin{array}{lcl}P_1&=&1_{1350}\otimes\{1,2,3,4,5,6,7,8\}\,,\\ P_5&=&1_{1350}\otimes\{1,2,5,6,11,12,13,14\}\,,\\ P_6&=&1_{1350}\otimes\{1,2,3,4,9,10,11,12\}\,,\\ P_7&=&1_{1350}\otimes\{1,3,5,7,10,12,14,15\}\,,\\ P_{11}&=&1_{1350}\otimes\{1,2,7,8,9,10,13,14\}\,,\\ P_{12}&=&1_{1350}\otimes\{1,4,5,8,10,11,13,15\}\,,\\ P_{14}&=&1_{1350}\otimes\{1,3,6,8,9,11,14,15\}\,,\\ P_{15}&=&1_{1350}\otimes\{1,4,6,7,9,12,13,15\}\,.\end{array}$$

Every participant P_i, where $1\le i\le 20249$, belonging to the set $[20249]=\{1,2,\ldots,20249\}$), is included in exactly 8 minimal access sets.

Application 2 For the case where p equals 11, let's examine the ring denoted as $R=\mathbb{F}_{11}(\mathbb{F}_{11}+u\mathbb{F}_{11})$ and focus on the Gray image code $\rho(S_2^\beta)$ with a value of k set to 2. Then

$$\rho\left(\mathfrak{G}_2^\beta\right)=\left(\ 1_{10368}\otimes T_{11,2}^\beta\ \right),\ \textit{where}\ T_{11,2}^\beta=\begin{pmatrix}1&1&1&1&1&1&1&1&1&1&1&1&0\\0&1&2&3&4&5&6&7&8&9&10&11&1\end{pmatrix}.$$

The Gray image code $\rho(S_2^\beta)$ can be characterized as an 11-ary $[134784; 2; 124416]$-code. We proceed to build the secret sharing scheme utilizing $\rho(S_2^\beta)$. Within the associated access structure, there exist 134783 participants and 11 minimal qualified sets, outlined below

$$\begin{aligned}
P_1 &= 1_{10368} \otimes \{1,2,3,4,5,6,7,8,9,10,11,12\}\,, \\
P_2 &= 1_{10368} \otimes \{1,2,3,4,5,6,7,8,9,10,12,13\}\,, \\
P_3 &= 1_{10368} \otimes \{1,2,3,4,5,7,8,9,10,11,12,13\}\,, \\
P_4 &= 1_{10368} \otimes \{1,2,3,4,5,6,7,9,10,11,12,13\}\,, \\
P_5 &= 1_{10368} \otimes \{1,2,3,4,5,6,7,8,10,11,12,13\}\,, \\
P_6 &= 1_{10368} \otimes \{1,2,4,5,6,7,8,9,10,11,12,13\}\,, \\
P_7 &= 1_{10368} \otimes \{1,2,3,4,5,6,7,8,9,11,12,13\}\,, \\
P_8 &= 1_{10368} \otimes \{1,2,3,5,6,7,8,9,10,11,12,13\}\,, \\
P_9 &= 1_{10368} \otimes \{1,2,3,4,6,7,8,9,10,11,12,13\}\,, \\
P_{10} &= 1_{10368} \otimes \{1,2,3,4,5,6,8,9,10,11,12,13\}\,, \\
P_{11} &= 1_{10368} \otimes \{1,3,4,5,6,7,8,9,10,11,12,13\}\,.
\end{aligned}$$

Each individual P_i, with i ranging from 1 to 134783 and belonging to the set $[134783] = \{1, 2, \ldots, 20249\}$, is a member of precisely 11 minimal access sets.

7. Conclusion

The article explores various aspects of Simplex Codes over the finite ring $\mathbb{F}_p(\mathbb{F}_p + v\mathbb{F}_p)$, focusing on two types, denoted as α and β. The investigation covers the construction and properties of these codes, including their Gray images and covering radius. The p-array Gray images of Simplex Codes of Types α and β over $\mathbb{F}_p(\mathbb{F}_p + v\mathbb{F}_p)$ are analyzed. Furthermore, the study explores the application of Simplex Codes in constructing secret sharing schemes over finite fields $\mathbb{F}_p$. In summary, the article contributes to the understanding of Simplex Codes of Types α and β over $\mathbb{F}_p(\mathbb{F}_p + v\mathbb{F}_p)$ by investigating their Gray images, covering radius, and practical applications in the construction of secret sharing schemes over finite fields $\mathbb{F}_p$.

Acknowledgements

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.

Conflicts of Interest

Conflict of interest All authors declare that there is no conflict of interest in this research.

References

1. M.M. Al Ashker, *Simplex codes over the ring $F_2 + uF_2$*, The Arabian Journal For Science and Engineering, **30** (2005) 277-285.

2. M.M. Al Ashker, *Simplex codes over the ring $\sum_{n=0}^{s} u^n F_2$*, Turk. J. Math, **29** (2005) 221-233.

3. M.M. Al Ashker and I.M Isleem, *Simplex codes over the ring $F_2 + vF_2$*, An-Najah Univ J Res (N.sc),**22** (2008) 25-42.

4. K. Chatouh, K. Guenda, T. Aaron Gulliver and L. Noui, *Simplex and MacDonald codes over R_q*, J. Appl. Math. Comput, **55** (2017) 455-478.

5. K. Chatouh, K. Guenda, T. Aaron Gulliver and L. Noui, *On some classes of linear codes over Z_2Z_4 and their covering radii*, J. Appl. Math. Comput, **53** 201-222 (2017). https://doi.org/10.1007/s12190-015-0964-9.

6. K. Chatouh, K. Guenda and T. Aaron 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** (2020) 1-19.

7. R.Chapman, S.T.Dougherty,P.Gaborit and P.Solé, 2-*modular lattices from ternary codes*, Journal de Theorie des Nombres de Bordeaux, **14** (2002) 73-85.

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

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

10. M. Cruz, C. Durairajan and P. Solé, *On the Covering Radius of Codes over* $\mathbb{Z}_{p^k}$, Mathematics, **8** (2020) 328.

11. I.M Isleem, On Linear codes $F_2 \times F_2$, Master Thesis, Islamic University of Gaza, 2007.

12. Y.Cengellenmis,M. Al-Ashker, *Simplex codes of type* β *over* $F_3 + vF_3$, Proceedings of the Jangjeon Mathematical Society, January 2011.

13. Y.Cengellenmis, M. Al-Ashker, Simplex codes of type γ over $F_3 + vF_3$, International Mathematical Forum, **40** (2010) 1993-2000.

14. E. D. Karnin, J. W. Greene, and M. E. Hellman, *On secret sharing systems*, IEEE Trans. Inf. Theory, **29** (1983) 35–41.

15. M.K. Gupta and C. Durairajan, *On the covering radius of some modular codes*, arXiv:1206.3038 v2 [cs.IT] Jun. 2012.

16. M. Bilal, J. Borges, S. T. Dougherty and C. Fernandez-Cordoba, *Maximum distance separable codes over* Z_4 *and* Z_2Z_4, Des. Codes Cryptogr., **61** (2011) 31–40.

17. J. Borges, S. T. Dougherty and C. Fernandez-Cordoba, *Characterization and constructions of self-dual codes over* Z_2Z_4, Adv. Math. Commun., **6** (2012) 287-303.

18. X. Wang, J. Gao and Fang-Wei Fu, *Secret Sharing Schemes from Linear Codes over* $F_p + vF_p$,International Journal of Foundations of Computer Science, **27** (2016) 595-605.

19. F. Çalişkan, T. Yildirim and R. Aksoy, *Non-Binary Quantum Codes from Cyclic Codes over* $F_p(F_p+vF_p)$, International Journal of Theoretical Physics **62** (2023), 29.

20. S. Zhu, L. Wanga, *A class of constacyclic codes over* $F_p + vF_p$ *and its Gray image*, Discrete Mathematics **311** (2011) 2677-2682

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.
E-mail address: karima.chatouh@univ-batna.dz

and

Mohammed. M. Al-Ashker, Department of Mathematics,
Islamic University of Gaza,
PO Box 108, Gaza, Palestine.
E-mail address: mashker@mail.iugaza.edu