République Algérienne Démocratique Et Populaire

Ministère de L'enseignement Superieur Et de

La Recherche Scientifique

Université de Batna 2 - Mostefa Ben Boulaid -

Faculté des Mathématiques et D'informatique

Département des Mathématiques

THESE

Présentée pour l'obtention du titre de

Docteur en Sciences

Option : **Mathématiques Appliquées**

Sous le thème

Étude et Construction de Certaines Classes de Codes linéaires sur les anneaux finis

Présentée par

Ouarda HADDOUCHE

Devant le jury composé de:

Mr Guedjiba Said	Prof. Université de Batna 2	Président
Mme Zekraoui Hanifa	Prof. Université d' O. E. Bouaghi	Directrice de thèse
Mr Noui Lemnouar	Prof. Université de Batna 2	Co-encadreur
Mme Guenda Kenza	Prof. USTHB	Examinatrice
Mr Milles Soheyb	MCA. Centre universitaire de Barika	Examinateur
Mme Chatouh Karima	MCA. Université de Batna 1	Invitée

2023/2024

Remerciements

Dans ces lignes, j'ai l'occasion de remercier les gents qui m'ont aidé d'une manière ou d'une autre dans le développement de ma thèse, je voudrais commencer par exprimer toute ma gratitude envers ma soeur Chatouh Karima. Après m'avoir suggéré ce beau sujet, elle a toujours été présente pour guider mon travail.Son écoute, ses connaissances, sa disponibilité et ses conseils m'ont autorisé d'entamer bien ce travail. Je le remercie du fond du coeur.

Ensuite, je veux remercier ma directrice de thèse le professeur Zekraoui Hanifa d'avoir accepté de travailler sous sa direction.

Je remercie mon collaborateur le professeur Noui Lemnouar pour sa disponibilité et sa compréhension durant ma recherche.

Je tiens à remercier également Monsieur Guedjiba Said Professeur à l'université de Batna 2 pour l'honneur qu'il m'a fait en acceptant la présidence du jury de ma soutenance.

J'adresse mes sincères remerciements á madame Guenda Kenza Professeur à l'université de USTHB pour avoir accepté la lourde charge d'évaluer cette thése et d'en être examinatrice de plus son soutien moral.

Je remercie Monsieur Milles Soheyb pour son acceptation comme membre de jury.

Il est important que j'exprime ma gratitude â mes amies: Widad, Lila, Mouna et les autres son cité les noms.

Dédicace

Je dédie cet humble travail à : Mes parents qui ont toujours soutenu dans mes efforts et m'ont appris à faire de mon mieux.

Mon mari a été un grand soutien moral pour moi.

Mes enfants: Aymen, Dhia Eddine, Emma.

Mes frères: Hadjira, Hawas, Adam, Rabah.

Mes nièces et mes neveux.

À tous ceux qui ont participé de près ou de loin à la réalisation de cette thèse.

Chère famille et amis.

Abstract

The aim of this thesis is to establish a foundation for linear codes over a class of finite rings. This research was conducted following numerous national and international conferences, resulting in the publication of two papers, with one already published and the other currently under review.

The first paper, titled "Homogeneous Weights over the ring $\mathcal{R}_{5,3} = \mathbb{F}_5 + u_1\mathbb{F}_5 + u_2\mathbb{F}_5 + u_3\mathbb{F}_5$," was published in volume 11 of Advances in Mathematics: Scientific Journal (2022), no.11. This paper explores homogeneous weights as a generalization of Hamming weights for finite rings. A significant portion of our work focuses on studying this weight on $\mathcal{R}_{5,3}$, and to define the homogeneous weight on $\mathcal{R}_{5,3}$, we utilize a homogeneous weight definition on $\mathbb{F}_5$.

The second paper, currently under review, is titled "Homogeneous Weight and its Applications in Some Linear codes over $\mathcal{R}_{p^s,\theta} = \mathbb{F}_{p^s} + u_1\mathbb{F}_{p^s} + \ldots + u_\theta\mathbb{F}_{p^s}$" submitted to The Jordanian Journal of Mathematics and Statistics.

In the first conference, "Simplex and MacDonald codes over $\mathfrak{R}_{5,3}$", presented at the Mini-Congress of Algerian Mathematicians in 2021, we focus on constructing simplex and MacDonald codes over $\mathfrak{R}_{5,3} = \mathbb{F}_5 + u_1\mathbb{F}_5 + u_2\mathbb{F}_5 + u_3\mathbb{F}_5$, expressed as the sum of MacDonald and simplex codes over $\mathbb{F}_5$.

The second conference, "Some Construction of Linear codes over $\mathfrak{R} = \mathcal{R}_1\mathcal{R}_2$," held at the National Conference of Mathematics and Applications CNMA 2021, introduces a new type of linear codes defined over the ring $\mathfrak{R} = \mathcal{R}_1\mathcal{R}_2$. Here, $\mathcal{R}_1 = \mathbb{Z}_4 + u\mathbb{Z}_4$ is a commutative ring with $u^2 = 1$, and $\mathcal{R}_2 = \mathbb{Z}_4 + v_1\mathbb{Z}_4 + v_2\mathbb{Z}_4 + v_3\mathbb{Z}_4$ is the second commutative ring with

specified properties $v_i^2 = \xi_i v_i$, $\xi_i \in \mathbb{Z}_4^*$ and $v_i v_j = v_j v_i$, for $1 \leq i \neq j \leq 3$. We define simplex and MacDonald linear codes over $\mathfrak{R} = \mathcal{R}_1\mathcal{R}_2$.

The third conference, "Simplex and MacDonald LCD Linear Codes over $\mathfrak{R}$," presented at the First National Conference on Mathematics and its Applications CNMA 2021 in Bordj Bou Arreidj, focuses on determining the construction of simplex and MacDonald linear codes as LCD codes over $\mathfrak{R} = \mathbb{F}_9 + w_1\mathbb{F}_9 + w_2\mathbb{F}_9 + w_3\mathbb{F}_9 + w_4\mathbb{F}_9 + w_5\mathbb{F}_9$. The codes are defined with specific properties $w_i^2 = (2 + 2\varrho)\, w_i$ and $w_i w_j = w_j w_i = 0$, $1 \leq i \neq j \leq 5$, and families of linear codes over the finite field $\mathbb{F}_9$ are established, which are Gray images.

In the final conference, "Some Constructions of Linear Codes over a ring $\mathfrak{R}$," presented at the International Conference on Research in Applied Mathematics and Computer Science ICRAMCS 2022, a new ring is introduced, represented as the Cartesian product of three finite commutative rings, $\mathfrak{R} = \mathcal{R}_1\mathcal{R}_2\mathcal{R}_3$, with $\mathcal{R}_1 = \mathbb{Z}_q + v_1\mathbb{Z}_q$ is commutative ring and $v_1^2 = 1, \mathcal{R}_2 = \mathbb{Z}_q + v_1\mathbb{Z}_q + v_2\mathbb{Z}_q, \mathcal{R}_3 = \mathbb{Z}_q + v_1\mathbb{Z}_q + v_2\mathbb{Z}_q + v_3\mathbb{Z}_q$ are two other commutatives rings. The construction of codes on this ring involves the creation of generator matrices in another way. Notably, the Gray Map is defined [21–23], and examples of this construction include α-simplex and α-MacDonald codes over the new ring $\mathfrak{R}$. Additionally, Multi-Secret Sharing Schemes are applied to the Gray images of α-MacDonald codes.

Key words: Lee weight, Homogeneous weight, Gray map, Simplex codes, Hamming weight, The covering radius, MacDonald codes.

Résumé

Cette thèse a pour objectif d'établir les bases des codes linéaires sur une classe d'anneaux finis. Cette recherche a été menée à la suite de plusieurs conférences nationales et internationales, aboutissant à la publication de deux articles, l'un déjà publié et l'autre actuellement en cours de révision.

Le premier est intitulé, " Hommogenous on weights on the ring $\mathfrak{R}_{5,3} = \mathbb{F}_5 + u_1\mathbb{F}_5 + u_2\mathbb{F}_5 + u_3\mathbb{F}_5$", Advances in Mathematics: Scientific Journal 11 (2022), no.11. Cet article explore les poids homogènes en tant que généralisation des poids de Hamming pour les anneaux finis. Une partie significative de notre travail se concentre sur l'étude de ce poids sur $\mathcal{R}_{5,3}$, et pour définir le poids homogène sur $\mathcal{R}_{5,3}$, nous utilisons une définition du poids homogène sur $\mathbb{F}_5$.

Le deuxiéme article, actuellement en cours de révision, s'intitule "Homogeneous Weight and its Applications in Some Linear codes over $\mathcal{R}_{p^s,\theta} = \mathbb{F}_{p^s} + u_1\mathbb{F}_{p^s} + \ldots + u_\theta\mathbb{F}_{p^s}$",soumis à The Jordanian Journal of Mathematics and Statistics.

La premiere conférence intitulé "Simplex and MacDonald codes over $\mathfrak{R}_{5,3}$", Mini-Congrès des Mathématiciens Algériens 2021. Nous sommes intéressés à construire des codes simplex et MacDonald sur $\mathfrak{R}_{5,3} = \mathbb{F}_5 + u_1\mathbb{F}_5 + u_2\mathbb{F}_5 + u_3\mathbb{F}_5$, qui sont écrits par la somme des codes simplex et MacDonald sur $\mathbb{F}_5$.

La deuxième conférence intitulé "Some Construction of Linear codes over $\mathcal{R} = \mathcal{R}_1\mathcal{R}_2$", Conférence Nationale de Mathématiques et Applications CNMA 2021. Dans la quelle, nous introduisons un nouveau type de codes linéaires définis sur l'anneau $\mathfrak{R} = \mathcal{R}_1\mathcal{R}_2$ ou $\mathcal{R}_1 = \mathbb{Z}_4 + u\mathbb{Z}_4$ est un anneau commutatif avec $u^2 = 1$ et $\mathcal{R}_2 = \mathbb{Z}_4 + v_1\mathbb{Z}_4 + v_2\mathbb{Z}_4 + v_3\mathbb{Z}_4$, est

le deuxième anneau commutatif, avec $v_i^2 = \xi_i v_i$, $\xi_i \in \mathbb{Z}_4^*$ et $v_i v_j = v_j v_i$, pour $1 \leq i \neq j \leq 3$. Nous donnons les définitions de ces codes, les codes linéaires simplex et MacDonald sur $\mathfrak{R} = \mathcal{R}_1\mathcal{R}_2$.

La troisieme conference intitulé "Simplex and MacDonald LCD Linear Codes over $\mathfrak{R}$ " , First National Conference on Mathematics and its Applications. La mise au point a été placée dans ce travail pour déterminer la construction des linéaires simplex et MacDonald codes pour etre un code LCD sur $\mathfrak{R} = \mathbb{F}_9 + w_1\mathbb{F}_9 + w_2\mathbb{F}_9 + w_3\mathbb{F}_9 + w_4\mathbb{F}_9 + w_5\mathbb{F}_9$, avec $w_i^2 = (2 + 2\varrho)\, w_i$ et $w_i w_j = w_j w_i = 0$, $1 \leq i \neq j \leq 5$, et définir des familles de codes linéaires sur le corps fini $\mathbb{F}_9$ qui constituent des images de Gray des codes Simplex et MacDonald sur $\mathfrak{R}_{5,3}$.

Finalement, la conférence intitulé " Some Constructions of Linear Codes over a ring $\mathfrak{R}$", the International Conference on Research in Applied Mathematics and Computer Science ICRAMCS 2022, nous avons introduit un nouvel anneau qui est donné par le produit cartésien de trois anneaux commutatifs finis, $\mathfrak{R} = \mathcal{R}_1\mathcal{R}_2\mathcal{R}_3$, avec $\mathcal{R}_1 = \mathbb{Z}_q + v_1\mathbb{Z}_q$ est un anneau commutatif et $v_1^2 = 1, \mathcal{R}_2 = \mathbb{Z}_q + v_1\mathbb{Z}_q + v_2\mathbb{Z}_q, \mathcal{R}_3 = \mathbb{Z}_q + v_1\mathbb{Z}_q + v_2\mathbb{Z}_q + v_3\mathbb{Z}_q$ sont deux autres anneaux commutatifs. Notre construction de ce code est donnée par la création de matrices génératrices d'une autre manière. Un autre aspect intéressant des codes sur cet anneau est de définir la Gray Map [21–23]. Nous utilisons deux exemples de cette construction, les codes α-simplex et α-MacDonald sur le nouvel anneau $\mathfrak{R}$. Apres on a utilisé les images Gray des codes α-MacDonald pour definir les schémas de partage multi-secrets.

Mots clés: Lee weight, Homogeneous weight, Gray map, Simplex codes, Hamming weight, The covering radius, MacDonald codes.

Notations

$\mathbb{F}_q$ =: A finite field of q elements.

$r(C)$ =: The covering radius of a code C over $\mathbb{F}_q$. $\widehat{C}$ =: The extended code.

$\mathcal{R}$ =: A finite ring.

$S_k(q)$ =: The simplex code over finite fiels $\mathbb{F}_q$.

$M_{k,u}(q)$ =: The Macdonald code over finite fiels $\mathbb{F}_q$.

wt_{Lee} =: The Lee weight.

wt_{Ham} =: the Hamming weight.

wt_{hom} =: The homogeneous weight.

$C^{\sum_{j=1}^{7} n_j}$ =: The repetition code en bloc on $\mathbb{F}_q$.

$S_k^{\alpha}(q)$ =: The simplex code of type α over $\mathbb{F}_q$.

$\mathcal{M}_{k,u}^{\alpha}(q)$ =: The Macdonald code of type α over $\mathbb{F}_q$.

$S_k^{\alpha,\theta}$ =: The simplex code of type α over $\mathcal{R}_{p^s,\theta}$.

$\mathcal{M}_{k,u}^{\alpha,\theta}$ =: The Macdonald code of type α over $\mathcal{R}_{p^s,\theta}$.

S_k^{α}=: The simplex code of type α over $\mathbb{F}_{p^s}$.

$\mathcal{M}_{k,u}^{\alpha}$ =: The Macdonald code of type α over $\mathbb{F}_{p^s}$.

G_k^{α}=: The generator matrix of simplex code of type α over $\mathbb{F}_{p^s}$.

$\mathcal{G}_k^{\alpha,\theta}$=: The generator matrix of simplex code of type α over $\mathcal{R}_{p^s,\theta}$.

$G_{k,t}^{\alpha}$=: The generator matrix of Macdonald code of type α over $\mathbb{F}_{p^s}$.

$\mathcal{G}_{k,t}^{\alpha,\theta}$=: The generator matrix of type α over $\mathcal{R}_{p^s,\theta}$.

$\Phi(C)$=: Gray imge of C.

Contents

Introduction

The transmission of digital information is pervasive in today's technology, encompassing texts, sounds, images, videos flowing through the Internet, satellites, or the playback of media like DVDs, BluRays, barcodes, or credit card numbers. The flow of information must adhere to stringent constraints: optimization of message size to prevent channel overload, mitigation of channel errors, ensuring the secrecy and authentication of transmissions, and swift calculations for transformations requiring passage through a channel.

The theory of error-correcting codes aims to develop codes that can detect and, if possible, correct errors occurring during message transmission.

At the conclusion of the Second World War in 1948 [38, 39, 65, 66, 73], Claude Shannon laid the foundational principles of information theory by publishing the article "A Mathematical Theory of Communication." However, this theory merely anticipates the existence of codes without providing any means of constructing them. Despite substantial progress in the design of digital communication systems since the 1950s, the challenge of constructing effective codes remains pertinent. The codes initially explored in this narrative predominantly focused on binary codes, representing subsets of $\mathbb{Z}_2^n$, which are codeword spaces of length n. Numerous studies [20,31,32,70] have delved into $\mathbb{Z}_4$ rings, with notable contributions by Sloane, Hammons, Solé, Calderbank, and Kumar in their 1990 publication [54, 63]. This work highlights the correlation between the family of nonlinear binary codes and linear codes on $\mathbb{Z}4$. The latter exhibit an algebraic structure known as $\mathbb{Z}_4$-linear codes, while linear codes defined as additive subgroups of $\mathbb{Z}_4$ are termed quaternary linear codes [54]. In recent years, the field of code theory has expanded, bridging mathematics

and engineering, enabling the introduction of codes on various finite fields and even on rings [12, 13, 60, 62, 69].

The objective of this work is to establish the foundational principles of linear codes over specific classes of finite rings [48], defined by the following form: $\mathcal{R}_{p^s,\theta} = \mathbb{F}_{p^s} + u_1\mathbb{F}_{p^s} + \ldots + u_\theta\mathbb{F}_{p^s}$, where $u_i^2 = u_i$, $u_iu_j = u_ju_j = 0$ and $1 \leq i \neq j \leq \theta$, $\mathfrak{R}_{5,3} = \mathbb{F}_5 + u_1\mathbb{F}_5 + u_2\mathbb{F}_5 + u_3\mathbb{F}_5$, $\mathcal{R} = \mathcal{R}_1\mathcal{R}_2$, where $\mathcal{R}_1 = \mathbb{Z}_4 + u\mathbb{Z}_4$ is a commutative ring with $u^2 = 1$ and $\mathcal{R}_2 = \mathbb{Z}_4 + v_1\mathbb{Z}_4 + v_2\mathbb{Z}_4 + v_3\mathbb{Z}_4$, is the second commutative ring, with $v_i^2 = \xi_i v_i$, $\xi_i \in \mathbb{Z}_4^*$ and $v_iv_j = v_jv_i$, for $1 \leq i \neq j \leq 3$, $\mathfrak{R} = \mathbb{F}_9 + w_1\mathbb{F}_9 + w_2\mathbb{F}_9 + w_3\mathbb{F}_9 + w_4\mathbb{F}_9 + w_5\mathbb{F}_9$, where $w_i^2 = (2 + 2\varrho)\, w_i$ and $w_iw_j = w_jw_i = 0$, $1 \leq i \neq j \leq 5$ and $\mathfrak{R} = \mathcal{R}_1\mathcal{R}_2\mathcal{R}_3$, with $\mathcal{R}_1 = \mathbb{Z}_q + v_1\mathbb{Z}_q$ is commutative ring and $v_1^2 = 1, \mathcal{R}_2 = \mathbb{Z}_q + v_1\mathbb{Z}_q + v_2\mathbb{Z}_q, \mathcal{R}_3 = \mathbb{Z}_q + v_1\mathbb{Z}_q + v_2\mathbb{Z}_q + v_3\mathbb{Z}_q$.

The homogeneous weight serves as a generalization of the Hamming weight for finite rings, holding significant relevance in this study. In the exploration of this weight on $\mathcal{R}_{p^s,\theta}$ and the determination of the homogeneous weight on $\mathcal{R}_{p^s,\theta}$, we leverage the definition of homogeneous weight on $\mathbb{F}_{p^s}$. Our focus is on constructing linear codes C comprising simplex and MacDonald codes over $\mathcal{R}_{p^s,\theta}$ expressed as the sum of simplex and MacDonald codes over $\mathbb{F}_{p^s}$, i.e., $C = \oplus_{i=1}^{\theta}\xi_iC_i$. We initiate with a straightforward observation that may characterize the properties of C based on those of C_i, where $0 \leq i \leq \theta$. An alternative perspective on these linear codes involves constructing their generator matrices, and we present a new representation for these matrices.

Another intriguing facet of codes over the rings is defining a Gray map from $\mathcal{R}_{p^s,\theta}$ to $\mathbb{F}_{p^s}$ and subsequently obtaining the Gray images of these codes. One of the most challenging problems in coding theory revolves around determining the covering radius of linear codes over a finite ring. Given that the covering radius is a fundamental parameter of the code, we strive to establish bounds on the covering radius for certain classes of linear codes with repeated coordinates and their Gray images. For a specific case, we delve into previous points studied on the ring $\mathfrak{R}_{5,3}$. Finally, we apply multi-secret sharing schemes to MacDonald and Simplex linear codes on $\mathfrak{R} = \mathcal{R}_1\mathcal{R}_2\mathcal{R}_3$.

The structure of this thesis is as follows:

Chapter 1: will be dedicated to providing a general introduction to codes over finite fields. The discussion will commence with the definition of the concept of finite fields codes, followed by the presentation of examples of well-known linear codes.

Chapater 2: This chapter introduces a novel class of rings, $\mathcal{R}_{p^s,\theta}$, forming the foundation for the entirety of this work [21], [23], [25]. The initial step involves defining the ring $\mathcal{R}_{p^s,\theta}$. Subsequently, we present the generator matrices of these codes in a novel manner, along with exploring Gray maps within the ring $\mathcal{R}_{p^s,\theta}$ towards the $\mathbb{F}_{p^s}^n$ and their resulting Gray images. Additionally, we delve into the homogeneous weight, a significant component of this chapter.

Chapter 3: Here, we present some properties and definitions of linear codes over $\mathfrak{R}_{5,3} = \mathbb{F}_5 + u_1\mathbb{F}_5 + u_2\mathbb{F}_5 + u_3\mathbb{F}_5$ [49]. In particular, generator matrix of these codes, the Gray map and the Gray images. Also, We present some homogenous weight results on $\mathfrak{R}_{5,3} = \mathbb{F}_5 + u_1\mathbb{F}_5 + u_2\mathbb{F}_5 + u_3\mathbb{F}_5$, we complete this chapter by some useful examples.

Chapter 4: In Chapter 4, we undertake the computation of the homogeneous weight within this ring. Additionally, we explore a new structure for linear codes and their Gray images over $\mathcal{R}_{p^s,\theta}$ [50], providing potential utility in subsequent applications. The chapter also encompasses the presentation of bounds on the covering radius for these codes. Furthermore, we introduce specific properties of LCD codes within the context of simplex and MacDonald codes over $\mathcal{R}_{p^s,\theta}$ [51, 53].

Chapter 5: We conclude our work by applying Multi-Secret Sharing Schemes to MacDonald and simplex linear codes over $\mathbb{Z}_q$, [48].

Thus, we have concluded this thesis with a comprehensive summary and provided avenues for future perspectives.

Chapter 1

LINEAR CODES OVER FINITE FIELDS

In this chapter, we will review some definitions and examine linear codes whose alphabet is an $\mathbb{F}_q$-field with q elements. The statements provided here are largely inspired by [6, 9, 20, 27, 42, 60, 61], works to which we refer the reader for the complete proofs of the results presented below.

1.1 Some properties of finite fields

Definition 1.1.1 *[61] Let $\mathbb{F}_q$ be the finite field of order q. A vector space (or linear vector space) over $\mathbb{F}_q$ is a nonempty set $\mathcal{V}$. Moreover, some vector addition $(+)$ and scalar multiplication $(.)$ by elements of $\mathbb{F}_q$ it satisfies all of the following conditions. For every $s, t, f \in \mathcal{V}$ and for all $\lambda, \mu \in \mathbb{F}_q$:*

1. *$s + t \in \mathcal{V}$;*
2. *$(s + t) + f = s + (t + f)$;*
3. *For all $0 \in \mathcal{V}$, there is an element 0 with property $0 + t = t = t + 0$;*

4. *There is an element of* $\mathcal{V}$ *named* $-s$ *for every variable* $s \in \mathcal{V}$, *such that* $s + (-s) = 0 = (-s) + s$;

5. $\lambda s \in \mathcal{V}$;

6. $\lambda \cdot (s + t) = \lambda \cdots + \lambda \cdot t, (\lambda + \mu) \cdot t = \lambda \cdot t + \mu \cdot t$;

7. $(\lambda\mu) \cdot s = \lambda(\mu \cdot s)$;

8. *If* 1 *represents the multiplicative identity of* $\mathbb{F}_q$, *than* $1 \cdot s = s$.

Theorem 1.1.2 *Let* p *is a prime number, the ring* $\mathbb{Z}/p\mathbb{Z}$ *is a finite field.*

Definition 1.1.3 *Let* K *be a subfield of the field* K_0 *and* k *the dimension of* K_0 *as a* K*-vector space. We say that* K_0 *is an extension of degree* k *of* K.

Theorem 1.1.4

1. *Let* $\mathbb{F}_q$ *be a finite field of cardinal* q, $q > 1$. *So* $q = p^\xi$, *for* $\xi > 1$ *where* p *is a prime number.*

2. *The field of cardinal* $q = p^\xi$, *note* $\mathbb{F}_q$ *is an extension of degree* m *of the prime field* $\mathbb{F}_p$.

Proposition 1.1.5 $\mathbb{F}_{p^\xi}$ *is an extension of degree* m *of* $\mathbb{F}_p$, *for any integer* $\xi > 1$,.

Theorem 1.1.6 *Let* $\mathbb{F}_q^*$ *the multiplicative group of* $\mathbb{F}_q$ *provided with the multiplication is a cyclic group.*

1.2 Linear codes over $\mathbb{F}_q$

We are now ready to present some properties of linear codes over finite fields see [33], [32]. Let $\mathcal{A}$ be an alphabet, k, n and m positive integers [63, 76] .

Definition 1.2.1 ***Corrector code*** *is the image of an injective map defined from* A^k *and with value in* A^n, *the term codeword designates an element of this set.*

Proposition 1.2.2 *Linear codes C of length n over $\mathbb{F}_q$ are a subspace of $\mathbb{F}_q^n$. The codewords are vectors in C.*

Definition 1.2.3 *The generator matrix G of C is the matrix whose rows form a base of C. As C of length n and dimension k, then G has types $k \times n$. The matrix G completely defines the C codes because*

$$C = \{xG \mid x \in \mathbb{F}_q^k\}.$$

Definition 1.2.4 *The information set is a set of coordinates corresponding to the k columns independent of the generator matrix of C.*

Remark 1.2.5 *1. For $[n, k]$ code C, there is many generator matrices.*

2. [20] The code has a unique generator matrix of the form $[I_k \mid A]$, we called G is in form standar or systematic form, with the identity matrix I_k of type $k \times k$, If the first k coordinates form an information set.

Example 1.2.6 *The $[5, 2]$ linear code over $\mathbb{F}_3$ has many genertor matrices,*

$$G_1 = \begin{bmatrix} 2 & 1 & 0 & 1 & 2 \\ 0 & 2 & 1 & 1 & 1 \end{bmatrix},$$

also

$$G_2 = \begin{bmatrix} 1 & 0 & 2 & 1 & 0 \\ 0 & 1 & 2 & 2 & 2 \end{bmatrix}.$$

Example 1.2.7 *Generator matrix of the $[4, 2]$ linear over $\mathbb{F}_7$ is,*

$$G_2 = \begin{bmatrix} 1 & 0 & 6 & 3 \\ 0 & 1 & 2 & 6 \end{bmatrix}.$$

Example 1.2.8 *1. The sets $\{0\}, \mathbb{F}_q^k$ are trivial linear codes.*

2. Let C is $[6, 3]$ linear code over $\mathbb{F}_2$, whith $\mid C \mid = 2^3$. Then,
$C = \{000000, 010101, 110011, 001111, 100110, 011010, 111100, 101001\}$ is generated by the set $S = \{010101, 110011, 001111\}$
and the standard generator matrix G of C is

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Definition 1.2.9 *[75] Given a linear $[n, k]$ code over $\mathbb{F}_q$.*

(i) The dual code of C denoted by $C^{\perp}$, or the orthogonal complement of the subspace C of $\mathbb{F}_q^n$ for the usual scalar product defined in $\mathbb{F}_q^n \times \mathbb{F}_q^n$ by,

$$< x, y >= \sum_{i=1}^{n} x_i y_i,\ (x, y) \in \mathbb{F}_q^n \times \mathbb{F}_q^n$$

This code is definded by,

$$C^{\perp} = \{x \in \mathbb{F}_q^n, < x, y >= 0, \forall y \in C\}.$$

Then $C^{\perp}$ is an $[n, n-k]$-linear code.

(ii) The matrix H for $C^{\perp}$ is called the parity-check matrix of C, because

$$C = \{x \in \mathbb{F}_q^n \mid Hx^{\perp} = 0\}.$$

Lemma 1.2.10 *If G is a generator matrix in systematic form $[I_k \mid A]$ then parity-check matrix of C is, $[I_{n-k} \mid -A^{\top}]$.*

Example 1.2.11 *The parity-check matrix of C for the example 1.2.6 is*

$$H = \begin{bmatrix} 1 & 0 & 0 & 2 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

Example 1.2.12 *Let C be $[11, 2]$ linear code over $\mathbb{F}_5$ with generator matrix*

$$G = \begin{bmatrix} 1 & 0 & 3 & 1 & 0 & 0 & 4 & 2 & 2 & 1 & 0 \\ 0 & 1 & 4 & 1 & 2 & 3 & 4 & 1 & 2 & 3 & 4 \end{bmatrix}.$$

then parity-check matrix of C is,

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 2 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 4 & 3 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 3 & 1 \end{bmatrix}.$$

Definition 1.2.13 *Assume that C is a linear code over $\mathbb{F}_q$ and let $C^{\perp}$ be the duel of C. So*

1. *The code C is self-duel if $C = C^{\perp}$.*

2. *The code C is self-orthogonl if $C \subset C^{\perp}$.*

Remark 1.2.14 *To describe linear codes, three main parameters are used. The first is the length (n) of the code. The following parameter to consider is k, which indicates the dimension. The third parameter estimates the distance between codeword pairs. To thoroughly comprehend, it must be known:*
We note C is $[n, k, d]$ linear code of length n with k dimension and minimal distance d.

Definition 1.2.15 *Given C be a linear code over $\mathbb{F}_q$, then*

1. *In $\mathbb{F}_q^n$, the Hamming distance $d(x, y)$ between two vectors $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ is defined as the number of coordinates in which $x \neq y$.*

$$d(x, y) = \{\sigma, x_\sigma \neq y_\sigma\},$$

2. *The minimum distance of a code C is given by,*

$$d(C) = min\{d(x, y) \mid x, y \in C, x \neq y\}.$$

Definition 1.2.16 *The amount of nonzero coordinates in a codeword is its Hamming weight i.e.,*

$$wt(x) = d(x, 0)$$

where $x \in \mathbb{F}_q^n$ *and* 0 *is the zero codeword.*

Definition 1.2.17 *If* $x, y \in \mathbb{F}_q^n$, *then* $d(x, y) = wt(x - y)$.

Theorem 1.2.18 *The Hamming distance is a metric over* $\mathbb{F}_q^n$.

Example 1.2.19 *1. The Hamming weight* (0120) *is* 2.

2. The Hamming distance of $(11233), (01223)$ *is* $wt((11233) - (01223)) = 2$.

Definition 1.2.20 *We say that C possesses a fixed weight if all the codewords have the same weight.*

1.2.1 Some examples of linear codes

By providing some classical linear codes and modifying or combining existing codes, many interesting and important codes emerge. [10, 11] .

1.2.2 Hamming codes

Let $\mathbb{F}_p = GF(p)$ signify a finite field of order p. If p is a prime number, the field $GF(p)$ coincides with $\mathbb{Z}_p$ the ring of integer residues modulo p.

Definition 1.2.21 *[72] For an integer* $\varsigma > 1$, *let* $n = \dfrac{p^\varsigma - 1}{p - 1}$. *The* $[n, n-\varsigma, 3]$ ***Hamming code over*** $\mathbb{F}_p$ *is defined by an* $\varsigma \times n$ *parity-check matrix* $H_\varsigma(p)$ *whose columns range over all nonzero of* $\mathbb{F}_p^\varsigma$, *whose leading nonzero entry again, every two columns in* $H_\varsigma(p)$ *are linearly independent.*

Proposition 1.2.22 *[20, 60] A Hamming code has a minimal distance equal to 3.*

Proof 1.2.23 *Parity-check matrix of any code has non-zero columns (definition), so $d \geq 2$ and has no two identical columns, $d \geq 3$, by adding two columns containing only one 1, we obtain a vector which contains exactly two 1, so $d = 3$.*

Example 1.2.24 *[72] If $\varsigma > 1$. The $[2^{\varsigma}, 2^{\varsigma} - 1 - \varsigma, 3]$-Hamming code over $\mathbb{F}_2$ is defined by an $\varsigma \times (2^{\varsigma} - 1)$ parity-check matrix H whose columns range over all nonzero of $\mathbb{F}_2^{\varsigma}$.*

1.2.3 Simplex linear code

In the context of coding theory, a simplex code is a type of linear error-correcting code that has a particularly simple structure. It is a subset of a larger class of linear codes known as Hamming codes, see [38], [39], and [44].

Definition 1.2.25 *[45] Let $\mathbb{F}_q = \{\alpha_0, \alpha_2, ..., \alpha_{q-1}\}$. The code $S_k(q)$ generated by the matrix $G_k(q)$ of size $k \times \dfrac{q^k - 1}{q - 1}$ over $\mathbb{F}_q$ whose columns are two by two linearly independent is called simplex code and $G_k(q)$ can be determined by*

$$G_k(q) = \left[\begin{array}{c|c|c|c|c|c} 00\cdots0 & 1 & 11\cdots1 & \alpha_3\cdots\alpha_3 & \cdots & \alpha_q\cdots\alpha_q \\ \hline G_{k-1}(q) & 0 & G_{k-1}(q) & G_{k-1}(q) & \cdots & G_{k-1}(q) \end{array}\right], \tag{1.1}$$

with

$$G_2(q) = \left[\begin{array}{c|c|c|ccc|c} 0 & 1 & 1 & \alpha_3 & \cdots & \alpha_{q-1} & \alpha_q \\ \hline 1 & 0 & 1 & 1 & \cdots & 1 & 1 \end{array}\right].$$

.

Theorem 1.2.26 *The $[\dfrac{q^k - 1}{q - 1}, k, q^{k-1}]$-simplexe code over $\mathbb{F}_q$, have weight q^{k-1} for all nonzero codewords.*

Definition 1.2.27 *Any $[\dfrac{q^k - 1}{q - 1}, \dfrac{q^k - 1}{q - 1} - k, 3]$ simplex code monomial equivalent of Hamming code.*

Example 1.2.28 *Let $\mathbb{F}_3 = \{0, 1, 2\}$. The simplex code over $\mathbb{F}_3$ is given by the generator matrix*

$$G_3(3) = \left[\begin{array}{c|c|c|c} 0000 & 1 & 1111 & 2222 \\ \hline G_2(3) & 0 & G_2(3) & G_2(3) \end{array}\right], \tag{1.2}$$

where

$$G_2(3) = \left[\begin{array}{c|c|c} 0 & 1 & 12 \\ \hline 1 & 0 & 11 \end{array}\right]. \tag{1.3}$$

1.2.4 Punctured codes

Definition 1.2.29 *[20]*

Let C represent a $[n, k, d]$ code over $\mathbb{F}_q$. By eliminating the same coordinate i in each codeword, we can puncture C. The generator matrix for C^* is created from the generator matrix of C by eliminating column i

Theorem 1.2.30 *Let C^* the code punctured on the i^{th} coordinate of the code C $[n, k, d]$ linear over $\mathbb{F}_q$.*

(a) When $d = 1$, C^* is an $[n-1, k, 1]$ code if C has no codewords of weight 1 whose nonzero entry is in coordinate i. Otherwise, if $k > 1$, C^* is an $[n-1, k, d^*]$ code with $d^* \geqslant 1$.

(b) If distance $d > 1$, then C^* is an $[n-1, k, d^*]$-linear code where

$$\begin{cases} d^* = d - 1 & w(C) = min\ d(x, y) = i, x, y \in \mathbb{F}_q^n \\ d^* = d & otherwise. \end{cases}$$

Example 1.2.31 *Let C be a ternary Hamming code with*

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{bmatrix}.$$

The C-punctured code at positions 4 and 1, respectively, is denoted by the codes C_4^* and C_1^*, respectively. They have following generator matrices

$$G_4^* = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}. \text{ and } G_1^* = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 2 \end{bmatrix}$$

So, C_4^* is a $[3,2,2]$-code and C_1^* is a $[3,2,2]$-code .

Definition 1.2.32 ***(The shortened code)*** *Let C an $[n,k]$-linear code systematic over $\mathbb{F}_q$ and $C^{'}$ be the set of words of C whose first j components are zero $(j < k+1)$. $C^{''}$ is sebset of $C^{'}$ obtained by eliminated the first j composants for each words.*
$C^{''}$ an $[n-t, k-t]$ linear code called shortened code of C code.

Proposition 1.2.33 *If C an $[n,k,d]$ linear code over $\mathbb{F}_q$ and $C^{''}$ is $[n-t, k-t, d^{''}]$ shortened code, then $d^{''} \geqslant d-1$.*

Example 1.2.34 *Let the linear code C of length 5 and dimension 2 over $\mathbb{F}_3$ with the generator matrix,*

$$G_1 = \begin{bmatrix} 2 & 1 & 0 & 1 & 2 \\ 0 & 2 & 1 & 1 & 1 \end{bmatrix},$$

$C = \{(00000), (02111), (01222), (21012), (20120), (22201), (12021), (11102), (10210)\}$
The minimal distance of C is $d = 3$, using the definition 1.2.32, we have

$$C^{'} = \{(00000), (02111), (01222)\},$$

so,

$$C^{''} = \{(0000), (2111), (1222)\},$$

is a linear code with lenght $4 = 5-1$, dimension $1 = 2-1$ and minimal distance 4.

Proposition 1.2.35 *The dual of a punctured code is the shortened code of the dual.*

1.2.5 Macdonald linear codes

We can generate new codes by either removing or adding one or more coordinates to a known code.

Definition 1.2.36 *Macdonald linear code $M_{k,\tau}(p)$ is the punctured code of the simplex code $S_k(p)$ with the parameters $[\frac{p^k-p^\tau}{p-1}, k, p^{k-1}-p^{\tau-1}]$, and nonzero codeword has weight either p^{k-1} or $p^{k-1}-p^{\tau-1}$ for any k and $1 \leq \tau \leq k-1$.*

Definition 1.2.37 *[62] Let $1 \leq \tau \leq k-1$ and $G_{k,\tau}(p)$ be the matrix obtained from generator matrix of simplex code $G_k(p)$ by eliminating the columns corresponding to the columns of the matrix $G_\tau(p)$. So*

$$G_{k,\tau}(p) = \left[G_k(p) \setminus \frac{0}{G_\tau(p)} \right], \tag{1.4}$$

where 0 is the null matrix of size $(k-\tau) \times \frac{p^\tau - 1}{p-1}$.

1.2.6 Extended codes

There are numerous methods for extending a code or creating a larger code by adding coordinates, see [56].

Definition 1.2.38 *The extended code $\widehat{C}$ of an C $[n,k,d]$-code over $\mathbb{F}_q$ is defined by*

$$\widehat{C} = \{\varpi_1\varpi_2\ldots\varpi_{n+1} \in \mathbb{F}_q^{n+1} | \varpi_1\varpi_2\ldots\varpi_{n+1} \in C \text{ with } \varpi_1+\varpi_2+\ldots+\varpi_{n+1}=0\}.$$

Proposition 1.2.39 *Extended linear codes is also linear with parametre $[n+1, k, \widehat{d}]$, noted $\widehat{C}$, where $\widehat{d} = d$ or $d+1$.*

Definition 1.2.40 *From the two generators matrices G and H parity check matrix of C can be created as generator matrix $\widehat{G}$ for $\widehat{C}$ by inserting an additional column such that the sum of the coordinates of each row of $\widehat{G}$ is 0. A parity check matrix $\widehat{H}$ of $\widehat{C}$ is given by*

$$\widehat{H} = \begin{bmatrix} 1 & \ldots & 1 & 1 \\ & & & 0 \\ & H & & \vdots \\ & & & 0 \end{bmatrix}.$$

Example 1.2.41 *Consider that the code in Example 1.2.31 is a $[4,2,3]$-ternary Hamming code over $\mathbb{F}_3$ with the generator matrix G and the parity check matrix H given by*

$$G = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 2 \end{bmatrix}, \text{ and } H = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 1 \end{bmatrix}.$$

For the extend code $\widehat{C}$, we have

$$\widehat{G} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 2 & 2 \end{bmatrix}, \text{ and } \widehat{H} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 2 & 0 \end{bmatrix}.$$

Hence $\widehat{d} = d = 3$.

Definition 1.2.42 *Let C_1 is an $[n, k, d_1]$ code and C_2 is an $[m, k, d_2]$ code.* ***The Juxtaposition*** *of C_1 and C_2, denoted $\{C_1|C_2\}$, is the $[n+m, k, d_1+d_2]$ code obtained by writing after C_1 and C_2.*

Definition 1.2.43 *The juxtaposition of the codes C_1 and C_2 is the code which admits as a generator matrix*

$$G = [G_1 G_2].$$

where, G_1 and G_2 are generators matrices of C_1 and C_2, respectively.

1.2.7 Linear complementary dual code

Definition 1.2.44 *The linear code C is denoted by the LCD code, if*

$$C \cap C^{\perp} = \{0\}. \tag{1.5}$$

Definition 1.2.45 *[65] The orthogonal projector $\prod_C$ defined by*

$$\varpi \prod_C = \begin{cases} \varpi & \text{if } \varpi \in C, \\ 0 & \text{if } \varpi \in C^{\perp}, \end{cases}$$

exists if only if C is an LCD code.

Proposition 1.2.46 *[65] If G is the generator matrix for a $[n,k]$-linear code C, the codes C is an LCD if and only if the matrix $GG^\top$ is nonsingular. Furthermore, if C is an LCD code, then $\prod_C = G^\top(GG^\top)^{-1}G$ is the orthogonal projector from $\mathbb{F}_q^n$ to C.*

The codes C is an LCD if and only if the matrix $GG^\top$ is nonsingular, where G is the generator matrix for a $[n,k]$-linear code C.
Additionally, if C is an LCD code, the orthogonal projector from $\mathbb{F}_q^n$ to C is $\prod_C = G^\top(GG^\top)^{-1}G$.

Proof 1.2.47 *[65] Assume that $GG^\top$ is nonsingular. If $v \in C$, we have*

$$v = uG$$

for some u. It follows that

$$vG^\top(GG^\top)^{-1}G = uGG^\top(GG^\top)^{-1}G = uG = v.$$

By addition, if $v \in C^\perp$ i.e., $vC^\perp = 0$, so

$$vG^\top(GG^\top)^{-1}G = 0G^\top(GG^\top)^{-1}G = 0.$$

As a result, $G^\top(GG^\top)^{-1}G$ represents an orthogonal projector $\prod_C$, and C must be an LCD code.

If, on the other hand, $GG^\top$ is a singular, then there is a nonzero vector u in $\mathbb{F}_q^k$ such that $uGG^\top = 0$.

$$(uG)v^\top = (uG)(u^{'}G)^\top = uGG^\top(u^{'})^\top = 0(u^{'})^\top = 0.$$

As a result, uG is also a vector in $C^\perp$. It follows that $C \cap C^\perp \neq \{0\}$, so C is not LCD code.

1.2.8 Repitition codes

The communication of a message follows the principle of encoding the message before transmission, aiming to add information for protection against noise. Upon reception,

errors in transmission are corrected by the decoder. The simplest method for encoding a message is the repetition code, which involves repeating each bit of the message a certain number of times. [1, 43].

Definition 1.2.48 *Let $C = \{(\rho, \rho, \cdots, \rho), \rho \in \mathbb{F}_q\}$ the repetition code of length n , then C is $[n, 1, n]$-linear code.*

Example 1.2.49 *The binary repetition code of length n is the binary linear code of parameters $[n, 1]$, which consists of the two codewords $0 = 00\ldots0$ and $1 = 11\ldots1$ its generator matrix, is*

$$G = [1\ 1\ \ldots 1],$$

And the corresponding parity-check matrix, is

$$H = \begin{bmatrix} & & 1 \\ & & 1 \\ & I_{n-1} & \vdots \\ & & 1 \end{bmatrix}.$$

The last coordinate indicates an information set, while the preceding $n-1$ coordinates represent a redundancy set.

1.2.9 Equivalent linear codes

Definition 1.2.50 *Let C' and C denote two linear codes in $\mathbb{F}_q^n$. We argue that C' and C are equivalents if C' is a permutation of the indices image of C, which means that if there exists σ of $\{1, 2, ..., n\}$ a permutation such that*

$$C' = \{a_{\sigma_{(1)}}, a_{\sigma_{(2)}}, ...a_{\sigma_{(n)}} | a_1 a_2 ... a_n \in C\}.$$

Theorem 1.2.51 *[8] Consider G and G' to be two matrices with coefficients in $\mathbb{F}_q$. If the matrix G' is obtained by a combination of the transformations of G, the code generated by G is equivalent to the code generated by G'.*

1. *Row permutation,*

2. *Multiplying a row by an elemment of* $\mathbb{F}_q^*$,

3. *Adding two rows,*

4. *Column permutation,*

5. *Multiplication of a column by an element of* $\mathbb{F}_q^*$.

Example 1.2.52 *The quaternary codes are* $\mathbb{Z}_4 - modules$. *These,* $\mathbb{Z}_4 - modules$ *not necessarily being free, they do not always admit a base [54]. However, any quaternary code is permutation equivalent to a code C, where generator matrix is of the form,*

$$G = \begin{bmatrix} I_{k_1} & M & N \\ 0 & 2I_{k_2} & 2P \end{bmatrix},$$

where M and P are binary matrices and N a matrix with coefficients in $\mathbb{Z}_4$. *The code C has* $4^{k_1}2^{k_2}$ *codewords and dimension of C over* $\mathbb{Z}_4$ *is given by,*

$$dim(C) = log_4 \mid C \mid = log_4(4^{k_1}2^{k_2}) = k_1 + k_2/2.$$

Example 1.2.53 *Let C is* $\mathbb{Z}_4-$*linear code. The set of codewords of C with lenght 4 is given by,*

$$\begin{aligned} C = \{&0000, 1113, 2222, 3331, 0202, 1311, 2020, 3133, \\ &0022, 1131, 2200, 3313, 0220, 1333, 2002, 3111\}. \end{aligned}$$

If $k_1 = 1, k_2 = 2, so\ k_1 + k_2 = 3$, *we have the generator matrix of C given by,*

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 2 \\ 0 & 0 & 2 & 2 \end{bmatrix}.$$

Remark 1.2.54 *If C and* C' *are equivalent, then the set of distances between the elements of C is the same as that of* C'. *As a result, C and* C' *have the same minimal distance.*

1.2.10 Weights distributions

Definition 1.2.55 *[20] Assume C is a linear code of length n. The weight distribution is defined as the number of codewords of each conceivable weight $0, 1, \ldots n$. The weight distribution of a code C is denoted by $A_0(C), A_1(C), \ldots, A_n(C)$. Otherwise, we can denote them as $A_0, A_1, \ldots, A_n$, where $A_i(C) = i$ is the number of codewords of weight i.*

Remark 1.2.56 *If $A_i(C) = 0$, we omitted this values from the list.*

Example 1.2.57 *Recall the code from Example 1.2.34 is a $[5, 2]$ code over $\mathbb{F}_3$, the codewods are given by*

$$C = \{(00000), (02111), (01222), (21012), (20120), (22201), (12021), (11102), (10210)\}$$

And,

$$A_4(C) = 6, A_3(C) = 2.$$

Remark 1.2.58 *For the important result, we need to know about the weights distributions. The weights distributions is a set how related to the weights distributions of C and $C^{\perp}$. In other words, the weights distributions of C are determined by the weights distributions of $C^{\perp}$, the opposite is true.*

1.3 Conclusion

In this chapter, we have given some basic notions on linear codes over finite fields, which will help study a particular case of these codes.

Chapter 2

LINEAR CODES OVER FINITE RINGS

On finite fields, the first research on error-correcting codes occurred in [76, 79, 81]. The code over finite rings has generated a great deal of interest since its disclosure in 1994, according to [56]. Many methods and many approaches are used to generate specific types of code with appropriate parameters and properties [72] and [37].

2.1 Linear codes over finite rings

Definition 2.1.1 *If the only maximal ideal in the $\mathcal{R}$ commutative local ring is $\{0\}$, then R is a field.*
Let $\mathcal{A}$ be the maximal ideal of a commutative local ring $\mathcal{R}$, then $\mathcal{R}/\mathcal{A}$ is the group of units of $\mathcal{R}$ and the quotient ring $\mathcal{R}/\mathcal{A}$ is a field that is known as the residue field of $\mathcal{R}$.
A commutative local ring $\mathcal{R}$ is also accoutred with the natural map $\Xi : \mathcal{R} \to \mathcal{R}/\mathcal{A}$, designated by $\Xi(x) = x + \mathcal{A}$ for all $x \in \mathcal{R}$.
Therefore, if $T = [x_{ij}]$ is a matrix over $\mathcal{R}$, then $\Xi(T) = [\Xi(x_{ij})]$ is a matrix over its residue field $\mathcal{R}/\mathcal{A}$, see [18], [36] and [74], [34], [11–13] [34].

The following lemma can be used to determine the rank of matrices over commutative

finite local rings.

Lemma 2.1.2 *[18] Let $\mathcal{A}$ is the maximal ideal of a commutative finite local ring $\mathcal{R}$ and let the natural map $\Xi : \mathcal{R} \to \mathcal{R}/\mathcal{A}$. If T is the matrix over $\mathcal{R}$, then*

$$rank(T) = rank\ \Xi(T).$$

Definition 2.1.3 *If we consider $\mathcal{R}$ a local finite ring, then a linear code C of length n over $\mathcal{R}$ is a submodule of $\mathcal{R}$-module of $\mathcal{R}^n$, which can be free or not. The C codewords are what are known as the C vectors.*

Example 2.1.4 *Let $R = \mathbb{Z}_4 + \vartheta\mathbb{Z}_4$ a ring, where $\vartheta^2 = \vartheta$. The linear codes over R are*

$$C = \left\{ \begin{array}{cccccccccccc}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0, \\
1 & \vartheta & 0 & 0 & 0 & \vartheta & \vartheta & \vartheta & 1 & 1 & 1, \\
0 & 1+3\vartheta & 3+\vartheta & 3+\vartheta & 3+\vartheta & \vartheta & 0 & 0 & 3\vartheta & 3\vartheta & \vartheta, \\
0 & 1+3\vartheta & 3+\vartheta & 3+\vartheta & 3+\vartheta & 0 & \vartheta & 0 & \vartheta & 3\vartheta & 3\vartheta, \\
0 & 1+3\vartheta & 3+\vartheta & 3+\vartheta & 3+\vartheta & 0 & 0 & \vartheta & 3\vartheta & \vartheta & 3\vartheta, \\
2 & 2\vartheta & 0 & 0 & 0 & 2\vartheta & 2\vartheta & 2\vartheta & 2 & 2 & 2, \\
0 & 2+2\vartheta & 2+2\vartheta & 2+2\vartheta & 2+2\vartheta & 2\vartheta & 0 & 0 & 2\vartheta & 2\vartheta & 2\vartheta, \\
0 & 2+2\vartheta & 2+2\vartheta & 2+2\vartheta & 2+2\vartheta & 0 & 2\vartheta & 0 & 2\vartheta & 2\vartheta & 2\vartheta, \\
0 & 2+2\vartheta & 2+2\vartheta & 2+2\vartheta & 2+2\vartheta & 0 & 0 & 2\vartheta & 2\vartheta & 2\vartheta & 2\vartheta, \\
3 & 3\vartheta & 0 & 0 & 0 & 3\vartheta & 3\vartheta & 3\vartheta & 3 & 3 & 3, \\
0 & 3+\vartheta & 1+3\vartheta & 1+3\vartheta & 1+3\vartheta & 3\vartheta & 0 & 0 & \vartheta & \vartheta & 3v\vartheta, \\
0 & 3+\vartheta & 1+3\vartheta & 1+3\vartheta & 1+3\vartheta & 0 & 3\vartheta & 0 & 3\vartheta & \vartheta & \vartheta, \\
0 & 3+\vartheta & 1+3\vartheta & 1+3\vartheta & 1+3\vartheta & 0 & 0 & 3\vartheta & \vartheta & 3\vartheta & \vartheta
\end{array} \right\}.$$

We can also show that free codes over finite local commutative rings are equivalent, which is another similar result that we can prove.

Definition 2.1.5 *If the codewords of a code $\overline{C}$ can be obtained by permuting the coordinate positions and multiplying a unit in each coordinate position of all the codewords of C, the code $\overline{C}$ is said to be equivalent to C over finite commutative rings.*

Definition 2.1.6 *Let C be a lineare code of length n over $\mathcal{R}$, a matrix G of size $k \times n$ is called a generator matrix of the code C, if the application defined as*

$$\begin{array}{rccc} \Theta & : & \mathcal{R}^k & \rightarrow & \mathcal{R}^n \\ & & \vartheta & \mapsto & \Theta(\vartheta) = \vartheta.G, \end{array} \tag{2.1}$$

where $\Theta(\mathcal{R}^k) = C$.

Example 2.1.7 *The matrix $G =$*

$$\left[\begin{array}{cccccccccccccccc} 1 & 0 & 0 & 0 & 3\vartheta & 3\vartheta & 3\vartheta & 3\vartheta & 0 & 1+2\vartheta & 3+2\vartheta & 0 & 3\vartheta & 3\vartheta & 3\vartheta & 3\vartheta \\ 0 & 1 & 0 & 0 & 3\vartheta & 3\vartheta & 3\vartheta & 3\vartheta & 1 & 1 & 1 & 0 & 3\vartheta & 3\vartheta & 3\vartheta & 3\vartheta \\ 0 & 0 & 1 & 0 & 3v\vartheta & 3\vartheta & 3\vartheta & 3\vartheta & 3+2\vartheta & 0 & 1+2\vartheta & 3 & 3\vartheta & 3\vartheta & 3\vartheta & 3\vartheta \\ 0 & 0 & 0 & 1 & 3\vartheta & 3\vartheta & 3\vartheta & 3\vartheta & 1+2\vartheta & 3+2\vartheta & 0 & 3 & 3\vartheta & 3\vartheta & 3\vartheta & 3\vartheta \\ 3\vartheta & 3\vartheta & 3\vartheta & 3\vartheta & 1 & 0 & 0 & 0 & 3\vartheta & 3\vartheta & 3\vartheta & 3\vartheta & 0 & 1+2\vartheta & 3+2\vartheta & 0 \\ 3\vartheta & 3\vartheta & 3\vartheta & 3\vartheta & 0 & 1 & 0 & 0 & 3\vartheta & 3\vartheta & 3\vartheta & 3\vartheta & 1 & 1 & 1 & 0 \\ 3\vartheta & 3\vartheta & 3\vartheta & 3\vartheta & 0 & 0 & 1 & 0 & 3\vartheta & 3\vartheta & 3\vartheta & 3\vartheta & 3+2\vartheta & 0 & 1+2\vartheta & 3 \\ 3\vartheta & 3\vartheta & 3\vartheta & 3\vartheta & 0 & 0 & 0 & 1 & 3\vartheta & 3\vartheta & 3\vartheta & 3\vartheta & 1+2\vartheta & 3+2\vartheta & 0 & 3 \end{array}\right],$$

generates a linear code of length 16 over $R = \mathbb{Z}_4 + \vartheta\mathbb{Z}_4$, where $\vartheta^2 = \vartheta$.

2.1.1 Covering radius of linear codes over finite ring

Another important quantity of a code is the Covering radius [9, 30, 43, 46], to introduce it, we first define the distance from a point to a set.

Definition 2.1.8 ***(minimal distance)**. Let E be a set in $\mathcal{R}_q^n$ and $\upsilon \in \mathcal{R}_q^n$, we define the distance from υ to E by,*

$$d(\upsilon, E) = \min_{e \in E} d(\upsilon, e) \tag{2.2}$$

Definition 2.1.9 *The covering radius $r(C)$ of binary linear code C is given by*

$$\begin{aligned} r(C) &= \max_{u \in \mathbb{F}_2^n} \{d_{Ham}(u, C)\} \\ &= \max_{u \in \mathbb{F}_2^n} \left\{ \min_{c \in C} d(u, c) \right\}. \end{aligned} \tag{2.3}$$

In other words $r(C)$ is defined as the greatest distance between the points of the ambient space of the code to the code.

Remark 2.1.10 *This definition means the spheres of radius r around the codewords cover $\mathbb{F}_2^n$, and the covering radius is the smallest of those.*

This definition's extension to codes over the finite ring $\mathcal{R}$ is identical.

Definition 2.1.11 *The smallest radius r of the spheres surrounding the code words that cover $\mathcal{R}$ is the covering radius of a code C,*

$$r(C) = \max_{u \in \mathcal{R}^n} \left\{ \min_{c \in C} d(u, c) \right\}. \tag{2.4}$$

It is clear that $r(C)$ is the smallest radius r such that,

$$\mathcal{R}^n = \cup_{c \in C} S_r(c),$$

where

$$S_r(u) = \{ \upsilon \in \mathcal{R}^n; d(u, \upsilon) \leq r \},$$

for $u \in \mathcal{R}^n$.

Following results allow over the finite rings to determine the covering radius of the codes. It is a generalization of the consequence in [30], for codes over a finite field [71].

Proposition 2.1.12 *If $\mathsf{G_0}$, $\mathsf{G_1}$ are generator matrices of C_0, C_1 codes over $\mathcal{R}$ respectively of minimal distance d_0 and d_1, with length n_0 and n_1. And the generator matrix of C is given*

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

then

$$r_d(C) \leq r_{d_0}(C_0) + r_{d_1}(C_1),$$

in addition, the following inequality is satisfied by the covering radius of the concatenation of C_0 and C_1, indicated by C_c.

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

for all distances d over $\mathcal{R}$.

Proof 2.1.13 *Let* G *the generator matrix of the code* C_c *is defined as*

$$\mathsf{G} = \left[\begin{array}{cc} \mathsf{G_0}' & \mathsf{G_1}' \end{array} \right],$$

then C_c *is a code of length* $n_0 + n_1$*. The minimum distance* d*, where*

$$d \geq \min\{d_0, d_1\}.$$

Hence the covering radius satisfies,

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

Proposition 2.1.14 *Let* C *be a code over* $\mathcal{R}$*, and* $\Phi(C)$ *be the image of* C *by the Gray map, then*

$$r\left(C\right) = r\left(\Phi(C)\right).$$

Definition 2.1.15 ***(Perfect code).*** *Let* C *be a code, the number* t *is the correction capacity and* $r(C)$ *the covering radius of* C*. The code* C *is a perfect code if*

$$t = r(C).$$

Example 2.1.16 *Let* C_0 *and* C_1 *be linears codes of lenght 5 and 4 repectivly over* $\mathbb{F}_3$*. So,*

$$C_0 = \{00000, 02111, 01222\},$$

$$C_1 = \{0000, 2111, 1222\}.$$

Hence, $r_{d_0}(C_0) = 4$ *and* $r_{d_1}(C_1) = 4$ *then* $r_d(C_c) = 8 \geqslant 4 + 4$*.*

2.1.2 Linear codes over finite ring $\mathcal{R}_{p^s,\theta}$

We review certain fundamental concepts for later usage in this part. A linear code C of length n over $\mathcal{R}_{p^s,\theta}$ is an $\mathcal{R}_{p^s,\theta}$-module of $\mathcal{R}^n_{p^s,\theta}$, where

$$\mathcal{R}_{p^s,\theta} = \{\sum_{l=0}^{\theta} u_l \xi_l^i \mid u_0 = 1,\ \xi_l^i \in \mathbb{F}_{p^s},\ \text{for all } 0 \leq i \leq p^s - 1\}$$

is a commutative Frobenious ring with characteristic p, where $|\mathcal{R}_{p^s,\theta}| = p^{(\theta+1)s}$. The set

$$C^{\perp} = \{x \in \mathcal{R}^n_{p^s,\theta} | \langle x, y\rangle_{\mathcal{R}_{p^s,\theta}} = 0 \text{ for all } y \in C\},$$

is called the dual code of C. According to [34], [35] and [47], we write x in $\mathcal{R}_{p^s,\theta}$ of the form

$$x = (1 - u_1 - \ldots - u_\theta)a_0 + u_1(a_1 + a_0) + \ldots + u_\theta(a_\theta + a_0). \tag{2.5}$$

We can also present C and $C^{\perp}$ as follows,

$$C = (1 - u_1 - \ldots - u_\theta)C_0 \oplus (u_1)C_1 \oplus \ldots \oplus (u_\theta)C_\theta, \tag{2.6}$$

$$C^{\perp} = (1 - u_1 - \ldots - u_\theta)C_0^{\perp} \oplus (u_1)C_1^{\perp} \oplus \ldots \oplus (u_\theta)C_\theta^{\perp}, \tag{2.7}$$

where, $C_i, C_j^{\perp}, 0 \leq i, j \leq \theta$ is a linear code of length n over $\mathbb{F}_{p^s}$. The Gray map is given by

$$\begin{array}{rcccc} \Psi & : & \mathcal{R}_{p^s,\theta} & \to & \mathbb{F}_{p^s}^{\theta+1} \\ & & x & \mapsto & \Psi(x), \end{array} \tag{2.8}$$

with

$$\Psi(x = a_0 + u_1a_1 + \ldots + u_\theta a_\theta) = (a_0, a_1 + a_0, \ldots, a_\theta + a_0).$$

This map can be extended to $\mathcal{R}^n_{p^s,\theta}$ as

$$\begin{array}{rcccc} \Phi & : & \mathcal{R}^n_{p^s,\theta} & \to & \mathbb{F}_{p^s}^{(\theta+1)n} \\ & & (x_1, x_2, \ldots, x_n) & \mapsto & \Phi_{Lee}((x_1, x_2, \ldots, x_n)) \end{array},$$

defined by

$$\Phi(x_1, x_2, \ldots, x_n) = ((a_0^0, a_1^0 + a_0^0, \ldots, a_\theta^0 + a_0^0), \ldots, (a_0^n, a_1^n + a_0^n, \ldots, a_\theta^n + a_0^n)).$$

The next Corollary is a generalization of a results in reference [47].

Corollary 2.1.17 *The Gray map is an isometry from*

$$(\mathcal{R}^n_{p^s,\theta}, \textit{Minimal distance}) \to (\mathbb{F}_{p^s}^{(\theta+1)n}, \textit{Hamming distance}).$$

Corollary 2.1.18 *Let $C = (1-u_1-\ldots-u_\theta)C_0 \oplus (u_1)C_1 \oplus \ldots \oplus (u_\theta)C_\theta$ be a linear code of length n over $\mathcal{R}_{p^s,\theta}$, where C_i is $[n; k_i; d_i]$-linear codes over $\mathbb{F}_{p^s}$, for $0 \leq i \leq \theta$. Then $\Phi(C)$ is $[(\theta+1)n; \sum_{i=0}^{i=\theta} k_i; d = min\{d_0, d_1, \ldots, d_\theta\}]$-linear codes over $\mathbb{F}_{p^s}$.*

Theorem 2.1.19 *Let C be a linear code of length n over $\mathcal{R}_{p^s,\theta}$. Then*

$$\Phi_{Lee}(C) = C_0 \otimes C_1 \otimes \ldots \otimes C_\theta$$

and

$$|C| = |C_0||C_1|\ldots|C_\theta|.$$

2.2 Homogeneous weight on the ring $\mathcal{R}_{p^s,\theta}$

Now, we point out some information from the articles [55] and [77], to treat homogeneous weight on Now, we draw attention to relevant information from the articles [55] and [77] to address the treatment of homogeneous weight on. $\mathcal{R}_{p^s,\theta}$.

Definition 2.2.1 *The weight w is homogeneous over a finite ring $\mathcal{R}_{p^s,\theta}$ if it meets the criteria that follow.*

1. *$\forall\ \tau, \upsilon \in \mathcal{R}_{p^s,\theta}$, $\mathcal{R}_{p^s,\theta}\tau = \mathcal{R}_{p^s,\theta}\upsilon \Rightarrow w(\tau) = w(\upsilon)$ holds.*

2. *The average weight of any non-zero ideal $\mathcal{R}_{p^s,\theta}\tau$ of $\mathcal{R}_{p^s,\theta}$ is the same, there is a real integer η that is nonzero and such that*

$$\sum_{\upsilon \in \mathcal{R}_{p^s,\theta}\tau} w(\upsilon) = \eta \cdot |\mathcal{R}_{p^s,\theta}\tau|,\ \forall\ \upsilon \in \mathcal{R}_{p^s,\theta}. \tag{2.9}$$

The average value of w on $\mathcal{R}_{p^s,\theta}$ is the value η.

Remark 2.2.2 *On $\mathbb{F}_{p^s}$ the Hamming weight is a homogeneous weight with $\eta = \dfrac{p^s-1}{p^s}$, see [58].*

On the Frobenius ring $\mathcal{R}_{p^s,\theta}$ the homogeneous weight w is given by generating character χ

$$\begin{array}{rcccl} w & : & \mathcal{R}_{p^s,\theta} & \to & \mathbb{R} \\ & & \tau & \mapsto & w(\tau) = \eta \cdot \left(1 - \dfrac{1}{|\mathcal{R}^{\times}_{p^s,\theta}|} \displaystyle\sum_{u \in \mathcal{R}^{\times}_{p^s,\theta}} \chi(\tau u)\right), \end{array} \tag{2.10}$$

where $\mathcal{R}^{\times}_{p^s,\theta}$ is the group of units of $\mathcal{R}_{p^s,\theta}$. Hence, we can state the followings.

Definition 2.2.3 *Let $R_1, R_2, \ldots, R_n$ be a Frobenius rings, we have*

1. *The finite direct sum of Frbenius rings is a Frobenius ring.*

2. *If the Frbenius rings $R_1, \ldots, R_n$ each have right generating characters $\chi_1, \ldots, \chi_n$, then $\mathcal{R}^{\times}_{p^s,\theta} = R_1 \oplus \ldots \oplus R_n$, has generating character $\chi = \prod_{i=1}^{n} \chi_i$. Hence, the generating character of $\overbrace{\mathbb{F}_{p^s} \times \mathbb{F}_{p^s} \times \ldots \times \mathbb{F}_{p^s}}^{n}$ is given by*

$$\begin{array}{rcccl} \chi & : & \overbrace{\mathbb{F}_{p^s} \times \mathbb{F}_{p^s} \times \ldots \times \mathbb{F}_{p^s}}^{n} & \to & \mathbb{T} \\ & & \varpi = (\varpi_1, \varpi_2, \ldots, \varpi_n) & \mapsto & \chi(X) = e^{\frac{2\pi i}{p} tr(\varpi_1 + \varpi_2 + \ldots + \varpi_n)}, \end{array} \tag{2.11}$$

where the trace function tr is defined by

$$\begin{array}{rcccl} tr & : & \mathbb{F}_{p^s} & \to & \mathbb{F}_p \\ & & \beta & \mapsto & tr(\beta) = \beta + \beta^p + \ldots + \beta^{p^{s-1}}, \end{array} \tag{2.12}$$

Additionally, the multiplicative group of unit complex numbers that makes up the set $\mathbb{T}$ is a one-dimensional torus.

Theorem 2.2.4 *[57] If the rings $R_1, \ldots, R_n$ with identity and $\mathcal{I}$ an ideal in $\prod_{j=1}^{n} R_j$, then, $\mathcal{I} = \prod_{j=1}^{n} A_j$ where A_j is an ideal in R_j, with*

$$\prod_{j=1}^{n} R_j = \{(\varpi_1, \varpi_2, \ldots, \varpi_n) | \varpi_j \in R_j\}. \tag{2.13}$$

2.2.1 Covering radius of linear codes over $\mathcal{R}_{p^s,\theta}$

According to [5, 30], the set of $x \in \mathbb{F}_{p^s}^n$, *such that* $d(x, y) \leq t$ corresponds to the ball of radius t around a word $y \in \mathbb{F}_{p^s}^n$, then the covring radius $r(C)$ of a code C, is defined as

$$r(C) = \max_{x \in \mathbb{F}_{p^s}^n} \min_{c \in C} d(x, c). \tag{2.14}$$

In the general case, using Equation 2.14, we define different covering radius of code C, by the followings

1 .The covering radius of $C = \bigotimes_{i=0}^{m} C_i$ is

$$r(C) = \sum_{i=0}^{m} (r(C_i)) . \tag{2.15}$$

2 . The covering radius of the concatenation $\sum_{i=0}^{m} C_i$ of C_i, for $0 \leq i \leq m$, is

$$r\left(\sum_{i=0}^{m} C_i\right) \geq \sum_{i=0}^{m} (r(C_i)) . \tag{2.16}$$

3 . The covring radius of an $[n; 1; n]$-repetition code over $\mathbb{F}_{p^s}$, is

$$r([n; 1; n]) = \lceil \frac{n(p^s - 1)}{p^s} \rceil. \tag{2.17}$$

2.2.2 Conclusion

We have introduced a new class of rings $\mathcal{R}_{p^s,\theta}$ forming the basis for this entire work. The initial step involved defining the ring $\mathcal{R}_{p^s,\theta}$. Subsequently, we presented the generator matrices of these codes in a novel manner, along with exploring Gray maps within the ring $\mathcal{R}_{p^s,\theta}$ to the fields $\mathbb{F}_{p^s}$, their resulting Gray images, and the homogeneous weight. Additionally, we discussed the covering radius of linear codes over $\mathcal{R}_{p^s,\theta}$.

Chapter 3

LINEAR CODES AND HOMOGENEOUS WEIGHTS OVER THE RING $\mathfrak{R}_{5,3}$

3.1 Introduction

In 1990, researchers placed significant importance on "algebraic coding theory" for linear codes defined over finite rings, establishing numerous mathematical methods. One notable example is the introduction of homogeneous weight as an alternative to the standard Hamming metric, serving as the distance function in the alphabet. Constantinescu and Heise initially introduced homogeneous weights in the context of encoding integer residual rings and finite rings [31]. Greferath and Schmidt later generalized this concept to arbitrary finite rings [41]. However, as the application of homogeneous weight is limited to local rings, such as finite Frobenius rings, other rings like chainless rings have also been studied, particularly in works such as [23, 27, 34, 35, 81].

This chapter aims to introduce the principles of linear codes on finite rings, represented as $\mathfrak{R}_{5,3} = \mathbb{F}_5 + u_1\mathbb{F}_5 + u_2\mathbb{F}_5 + u_3\mathbb{F}_5$, with $u_iu_j = u_ju_i = 0$ and $u_i^2 = u_i$, for $1 \leq j \neq i \leq 3$. The homogeneous weights are considered a generalization of the Hamming weights for finite

rings. Our current work primarily focuses on the study of this weight on $\mathfrak{R}_{5,3}$, employing the definition of homogeneous weight on $\mathbb{F}_5$ [49, 50, 53].

3.2 Linear codes over the ring $\mathfrak{R}_{5,3}$

Linear codes over $\mathfrak{R}_{5,3}$, is an $\mathfrak{R}_{5,3}$-module of $\mathfrak{R}_{5,3}^n$, wich is of length n, where

$$\mathfrak{R}_{5,3} = \{\bar{\omega}_i = \xi_0^i + u_1\xi_1^i + u_2\xi_2^i + u_3\xi_3^i \mid \xi_0^i, \xi_1^i, \xi_2^i, \xi_3^i \in \mathbb{F}_5, 1 \leq i \leq 625\} \tag{3.1}$$

is a "Frobenius ring" that is commutative and has characteristic 5, where $|\mathfrak{R}_{5,3}| = 5^4 = 625$. We define the inner product between any two elements $\vartheta = (\vartheta_1, \vartheta_2, \ldots, \vartheta_n)$ and $\vartheta' = (\vartheta'_1, \vartheta'_2, \ldots, \vartheta'_n)$ of $\mathfrak{R}_{5,3}^n$ by

$$\langle \vartheta, \vartheta' \rangle_{\mathfrak{R}_{5,3}} = \sum_{i=0}^{n} \vartheta_i \vartheta'_i.$$

We define the dual code $C^\perp$ of C by

$$C^\perp = \{\vartheta \in \mathfrak{R}_{5,3}^n | \langle \vartheta, \vartheta' \rangle_{\mathcal{R}_p} = 0 \text{ for all } \vartheta' \in C\}.$$

Following [34], the element ϑ in $\mathfrak{R}_{5,3}$ written by,

$$\vartheta = (1 + 4u_1 + 4u_2 + 4u_3)\kappa_0 + u_1(\kappa_1 + \kappa_0) + u_2(\kappa_2 + \kappa_0) + u_3(\kappa_3 + \kappa_0). \tag{3.2}$$

Let C be a linear code of length n over $\mathfrak{R}_{5,3}$, there are linear codes $\mathcal{C}_0, \mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$ of length n over $\mathbb{F}_5$ that exist, and the code C can be expressed uniquely as,

$$C = (1 + 4u_1 + 4u_2 + 4u_3)\mathcal{C}_0 \oplus (u_1)\mathcal{C}_1 \oplus (u_2)\mathcal{C}_2 \oplus (u_3)\mathcal{C}_3, \tag{3.3}$$

where

$$\begin{aligned}
\mathcal{C}_0 &= \{\kappa_0 \in \mathbb{F}_5^n, \exists \kappa_1, \kappa_2, \kappa_3 \in \mathbb{F}_5^n, \kappa_0 + u_1\kappa_1 + u_2\kappa_2 + u_1\kappa_3 \in C\}, \\
\mathcal{C}_1 &= \{\kappa_0 + \kappa_1 \in \mathbb{F}_5^n, \exists \kappa_2, \kappa_3 \in \mathbb{F}_5^n, \kappa_0 + u_1\kappa_1 + u_2\kappa_2 + u_1\kappa_3 \in C\}, \\
\mathcal{C}_2 &= \{\kappa_0 + \kappa_2 \in \mathbb{F}_5^n, \exists \kappa_1, \kappa_3 \in \mathbb{F}_5^n, \kappa_0 + u_1\kappa_1 + u_2\kappa_2 + u_1\kappa_3 \in C\}, \\
\mathcal{C}_3 &= \{\kappa_0 + \kappa_3 \in \mathbb{F}_5^n, \exists \kappa_1, \kappa_2 \in \mathbb{F}_5^n, \kappa_0 + u_1\kappa_1 + u_2\kappa_2 + u_1\kappa_3 \in C\}.
\end{aligned}$$

Theorem 3.2.1 *Let* $C = (1 + 4u_1 + 4u_2 + 4u_3)\mathcal{C}_0 \oplus (u_1)\mathcal{C}_1 \oplus (u_2)\mathcal{C}_2 \oplus (u_3)\mathcal{C}_3$ *be a linear code of length* n *over* $\mathfrak{R}_{5,3}$*, then*

$$C^{\perp} = (1 + 4u_1 + 4u_2 + 4u_3)\mathcal{C}_0^{\perp} \oplus (u_1)\mathcal{C}_1^{\perp} \oplus (u_2)\mathcal{C}_2^{\perp} \oplus (u_3)\mathcal{C}_3^{\perp}.$$

Corollary 3.2.2 *If* G_0, G_1, G_2 *and* G_3*, respectively, the generator matrices of linear codes* $\mathcal{C}_0, \mathcal{C}_1, \mathcal{C}_2$ *and* $\mathcal{C}_3$ *then the genertor matrix of* C *is*

$$G = \begin{bmatrix} (1 + 4u_1 + 4u_2 + 4u_3)G_0 \\ u_1G_1 \\ u_2G_2 \\ u_3G_3 \end{bmatrix}. \tag{3.4}$$

Example 3.2.3 *Consider the genertor matrices of linear codes* $\mathcal{C}_0, \mathcal{C}_1, \mathcal{C}_2$ *and* $\mathcal{C}_3$*,*

$$G_0 = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 0 & 2 \end{bmatrix}, G_2 = \begin{bmatrix} 1 & 4 & 0 \\ 0 & 1 & 2 \end{bmatrix}$$

,

$$G_1 = \begin{bmatrix} 0 & 2 & 0 \\ 2 & 0 & 2 \end{bmatrix}, G_3 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix},$$

then the generator matrix of C *can be expressed as*

$$G = \begin{bmatrix} 1 + 4u_1 + 4u_2 + 4u_3 & 2 + 3u_1 + 3u_2 + 3u_3 & 3 + 4u_1 + 4u_2 + 4u_3 \\ 0 & 0 & 2 + 3u_1 + 3u_2 + 3u_3 \\ 0 & 2 + 3u_1 + 3u_2 + 3u_3 & 0 \\ 2 + 3u_1 + 3u_2 + 3u_3 & 0 & 2 + 3u_1 + 3u_2 + 3u_3 \\ 1 + 4u_1 + 4u_2 + 4u_3 & 4 + u_1 + u_2 + u_3 & 0 \\ 0 & 1 + 4u_1 + 4u_2 + 4u_3 & 2 + 3u_1 + 3u_2 + 3u_3 \\ 1 + 4u_1 + 4u_2 + 4u_3 & 1 + 4u_1 + 4u_2 + 4u_3 & 0 \\ 0 & 1 + 4u_1 + 4u_2 + 4u_3 & 1 + 4u_1 + 4u_2 + 4u_3 \end{bmatrix}.$$

Next, we formulate the definition of the Gray map

$$\begin{array}{rccc} \Psi & : & \mathcal{R}_{5,3} & \to & \mathbb{F}_5^4 \\ & & \vartheta & \mapsto & \Psi(\vartheta), \end{array} \tag{3.5}$$

with

$$\Psi(\vartheta = \kappa_0 + u_1\kappa_1 + u_2\kappa_2 + u_3\kappa_3) = (\kappa_0, \kappa_0 + \kappa_1, \kappa_0 + \kappa_2, \kappa_0 + \kappa_3).$$

This map can be extended to $\left(\mathcal{R}_{5,3}^n, d\right)$

We can establish the following theorems, from the above results.

Theorem 3.2.4 *If the linear codes $\mathcal{C}_0, \mathcal{C}_1, \mathcal{C}_2$ and $\mathcal{C}_3$ are represented by the generator matrices G_0, G_1, G_2 and G_3, respectively, then $\Psi(G)$ is the genertor matrix of $\Psi(C)$.*

$$\Psi(G) = \begin{bmatrix} G_0 & 0 & 0 & 0 \\ G_0 & G_1 & 0 & 0 \\ G_0 & 0 & G_2 & 0 \\ G_0 & 0 & 0 & G_3 \end{bmatrix}. \tag{3.6}$$

Example 3.2.5 *In $\mathfrak{R}_{5,3}$, if $G_i = \begin{bmatrix} 1 & 3 \\ 3 & 1 \end{bmatrix}$, are genertor matrices of $\mathcal{C}_i$, for $i = \overline{0,3}$ then th code $\Phi(C)$ generated by*

$$\Phi(G) = \begin{bmatrix} 1 & 3 & 0 & 0 & 0 & 0 & 0 & 0 \\ 3 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 3 & 1 & 3 & 0 & 0 & 0 & 0 \\ 3 & 1 & 3 & 1 & 0 & 0 & 0 & 0 \\ 1 & 3 & 0 & 0 & 1 & 3 & 0 & 0 \\ 3 & 1 & 0 & 0 & 3 & 1 & 0 & 0 \\ 1 & 3 & 0 & 0 & 0 & 0 & 1 & 3 \\ 3 & 1 & 0 & 0 & 0 & 0 & 3 & 1 \end{bmatrix}.$$

Theorem 3.2.6 *Let $C = (1 + 4u_1 + 4u_2 + 4u_3)\mathcal{C}_0 \oplus (u_1)\mathcal{C}_1 \oplus (u_2)\mathcal{C}_2 \oplus (u_3)\mathcal{C}_3$ be a linear code of length n over $\mathfrak{R}_{5,3}$. Then,*

$$\Psi(C) = \mathcal{C}_0 \otimes \mathcal{C}_1 \otimes \mathcal{C}_2 \otimes \mathcal{C}_3 \tag{3.7}$$

and

$$C = |\mathcal{C}_0||\mathcal{C}_1||\mathcal{C}_2||\mathcal{C}_3|. \tag{3.8}$$

Corollary 3.2.7 *Assume that C is a linear code with length n over $\mathfrak{R}_{5,3}$, then $\Phi(C^{\perp}) = [\Phi(C)]^{\perp}$. Further, C is a self-dual code if and only if $\Phi(C)$ is a self-dual code.*

Corollary 3.2.8 *Let $C = (1 + 4u_1 + 4u_2 + 4u_3)\mathcal{C}_0 \oplus (u_1)\mathcal{C}_1 \oplus (u_2)\mathcal{C}_2 \oplus (u_3)\mathcal{C}_3$ be a linear code of length n over $\mathfrak{R}_{5,3}$, where $\mathcal{C}_i$ are $[n, k_i, d_i]$-linear codes over $\mathbb{F}_5$, for $0 \leq i \leq 3$. Then $\Psi(C)$ is $[4n, \sum_{i=0}^{3} k_i, d = \min(d_0, d_1, d_2, d_3)]$-linear code over $\mathbb{F}_5$.*

3.3 Homogeneous weight on the ring $\mathfrak{R}_{5,3}$

We shall determine the homogeneous weight on the ring $\mathfrak{R}_{5,3}$ based on the simplistic representation of [58]. Later, several applications will be defined and examined using these results.

The homogneous weight ω on $\mathfrak{R}_{5,3}$, with generating character χ is given by

$$\begin{array}{rcl} \omega : \mathfrak{R}_{5,3} \longrightarrow & & \mathbb{R} \\ \tau \longrightarrow & \omega(\tau) = \eta.(1 - \frac{1}{|\mathfrak{R}_{5,3}^{\times}|}. \sum_{u \in \mathfrak{R}_{5,3}^{\times}} \chi(\tau u)), \end{array} \tag{3.9}$$

where $\mathfrak{R}_{5,3}^{\times}$ is the grop of units of $\mathfrak{R}_{5,3}$.

The techniques in [57], leads to

1. The Frobenius ring is the finite direct sum of Frobenius rings.

2. If the Frobenius rings R_1, R_2, R_3, R_4 each have right generating characters $\chi_1, \chi_2, \chi_3, \chi_4$, then $R = R_1 \oplus R_2 \oplus R_3 \oplus R_4$ has generating character $\chi = \prod_{i=1}^{4} \chi_i$.

3. The generating character of $\overbrace{\mathbb{F}_5 \times \mathbb{F}_5 \times \mathbb{F}_5 \times \mathbb{F}_5}^{4}$ is defined as

$$\begin{array}{rcl} \chi : \overbrace{\mathbb{F}_5 \times \mathbb{F}_5 \times \mathbb{F}_5 \times \mathbb{F}_5}^{4} \longrightarrow & & \mathbb{T} \\ \varpi = (\varpi_1, \varpi_2, \varpi_3, \varpi_4) \longrightarrow & \chi(\varpi) = e^{\frac{2i\pi}{5} tr(\varpi_1 + \varpi_2 + \varpi_3 + \varpi_4)}, \end{array} \tag{3.10}$$

   where tr is the function trace and the multiplicative group of unit complex numbers that makes up the set $\mathbb{T}$ is a one-dimensional torus.

Theorem 3.3.1 *If the rings $R_1, R_2, \ldots, R_n$ with identity and $\mathcal{I}$ an ideal in $\prod_{j=1}^{n} R_j$, then $\mathcal{I} = \prod_{j=1}^{n} A_j$ with A_j is an ideal in R_j, where*

$$\prod_{j=1}^{n} R_j = \{(\varpi_1, \varpi_2, \ldots, \varpi_n) |\ \varpi_j \in R_j\}. \tag{3.11}$$

The ideals of $\mathbb{F}_5^4$ are established to be represented by the following sets in this instance by means of arguments similar to those used in Theorem 3.3.1.

1. $\mathbb{F}_5 \times \{0\} \times \{0\} \times \{0\} = \langle(\varpi_1, 0, 0, 0)\rangle, \varpi_1 \neq 0$
2. $\{0\} \times \mathbb{F}_5 \times \{0\} \times \{0\} = \langle(0, \varpi_2, 0, 0)\rangle, \varpi_2 \neq 0$
3. $\{0\} \times \{0\} \times \mathbb{F}_5 \times \{0\} = \langle(0, 0, \varpi_3, 0)\rangle, \varpi_3 \neq 0$
4. $\{0\} \times \{0\} \times \{0\} \times \mathbb{F}_5 = \langle(0, 0, 0, \varpi_4)\rangle, \varpi_4 \neq 0$
5. $\overbrace{\mathbb{F}_5 \times \mathbb{F}_5 \times \mathbb{F}_5 \times \mathbb{F}_5}^{4} = \langle(\varpi_1, \varpi_2, \varpi_3, \varpi_4)\rangle, \varpi_1, \varpi_2, \varpi_3, \varpi_4 \neq 0$
6. $\{(0, 0, 0, 0)\} = \langle(0, 0, 0, 0)\rangle$

Remark 3.3.2 *The number of zero divisors of $\mathbb{F}_5 \times \mathbb{F}_5 \times \mathbb{F}_5 \times \mathbb{F}_5$ are 16, and the number of unites of this product are $|\{\mathbb{F}_5 \times \mathbb{F}_5 \times \mathbb{F}_5 \times \mathbb{F}_5\}^{\times}| = 4^4$. Moreover the ideals $\mathcal{I}_1 = \langle(\varpi_1, 0, 0, 0)\rangle$, $\mathcal{I}_2 = \langle(0, \varpi_2, 0, 0)\rangle$, $\mathcal{I}_3 = \langle(0, 0, \varpi_3, 0)\rangle$, $\mathcal{I}_4 = \langle(0, 0, 0, \varpi_4)\rangle$ in $\mathbb{F}_5 \times \mathbb{F}_5 \times \mathbb{F}_5 \times \mathbb{F}_5$ are maximals.*

After putting all this information, we formulate the following theorem for computing homogeneous weight on $\mathfrak{R}_{5,3}$.

Theorem 3.3.3 *The homogeneous weight on $\mathfrak{R}_{5,3}$ is obtained as*

$$\omega_{hom}(\varpi) = \begin{cases} 0 & \text{if } \varpi = 0 \\ \dfrac{65}{64}\eta_1 & \text{if } \varpi \text{ is divisor of zero} \\ \dfrac{255}{256}\eta_2 & \text{if } \varpi \text{ is unit.} \end{cases}$$

Proof 3.3.4 *Let $\mathcal{H}\in \mathbb{F}_5^4$. According to Equation 3.10, the homogeneous weght of*

$$\varpi = (\varpi_1, \varpi_2, \varpi_3, \varpi_4) \in \mathcal{H}$$

is

$$\omega_{hom}(\varpi) = \eta_j.(1 - \frac{1}{4^4} \sum_{a\in(\mathcal{H})^\times} e^{\frac{2i\pi}{5} tr(a_1\varpi_1 + a_2\varpi_2 + a_3\varpi_3 + a_4\varpi_4)}),\ for\ j = \overline{1,2}. \tag{3.12}$$

The homogenous weight for three situations will be calculated in the following. ***In case 1****: If $(\varpi_1, \varpi_2, \varpi_3, \varpi_4) = (0,0,0,0)$, we have $tr((0,0,0,0)) = 0$, and*

$$\omega_{hom}((0,0,0,0)) = \eta_1.(1 - \frac{1}{4^4} \sum_{a\in(\mathcal{H})^\times} e^0), \tag{3.13}$$

then

$$\omega_{hom}((0,0,0,0)) = \eta_1.(1 - \frac{4^4}{4^4}),$$

so that

$$\omega_{hom}((0,0,0,0)) = 0. \tag{3.14}$$

In case 2*: If $\varpi = (\varpi_1, \varpi_2, \varpi_3, \varpi_4)$ is a zero divisor in $\mathcal{H}$. Assume that $\varpi_2, \varpi_3, \varpi_4 = 0$ and $\varpi_1 \neq 0$ (that means $\varpi_1 \in \mathbb{F}_5^*$) and $|\mathbb{F}_5^*| = 4$, we have*

$$tr(\langle a, \varpi\rangle_{\mathfrak{R}_{5,3}}) = tr(a_1\varpi_1), a = (a_1, a_2, a_3, a_4) \in (\mathcal{H})^\times.$$

For $j = 1,2,3,4$, the number of elements $\rho \in \mathbb{F}_5^*$, such that $tr(\rho) = 0$ is 0.
If $tr(\varrho) = j$ such that $\varrho \in \mathbb{F}_5^*$, then the number of elements in this case is 1. Using Equation 3.10, we obtain

$$\sum_{a\in(\mathcal{H})^\times} e^{\frac{2i\pi}{5} tr(ax)} = 0 + 4\sum_{j=1}^{4} e^{\frac{2i\pi}{5} j}$$

$$= -1,$$

as well as

$$\omega_{hom}(\varpi_1, \varpi_2, \varpi_3, \varpi_4) = \frac{65}{64}\eta_1. \tag{3.15}$$

In case 3*: If $\varpi = (\varpi_1, \varpi_2, \varpi_3, \varpi_4)$ is a unit in $\mathcal{H}$. We consider the following disjoint subsets of group under the multiplication $(\mathcal{H})^\times$, for $0 \leq j_i \leq 4$ and $1 \leq i \leq 4$*

$\mathcal{B}_{0000} = \langle(\varpi_1, \varpi_2, \varpi_3, \varpi_4)\rangle, tr(\varpi_i) = 0,\ i \in \{1,2,3,4\},$

$\mathcal{B}_{j_1000} = \langle(\varpi_1, \varpi_2, \varpi_3, \varpi_4)\rangle,\ tr(\varpi_1) = j_1,\ tr(\varpi_i) = 0,\ i \in \{2,3,4\},$

$\mathcal{B}_{0j_200} = \langle(\varpi_1, \varpi_2, \varpi_3, \varpi_4)\rangle,\ tr(\varpi_2) = j_2,\ tr(\varpi_i) = 0,\ i \in \{1,3,4\},$

$\mathcal{B}_{00j_30} = \langle(\varpi_1, \varpi_2, \varpi_3, \varpi_4)\rangle,\ tr(\varpi_3) = j_3,\ tr(\varpi_i) = 0,\ i \in \{1,2,4\},$

$\mathcal{B}_{000j_4} = \langle(\varpi_1, \varpi_2, \varpi_3, \varpi_4)\rangle,\ tr(\varpi_4) = j_4,\ tr(\varpi_i) = 0,\ i \in \{1,2,3\},$

$\mathcal{B}_{j_1j_200} = \langle(\varpi_1, \varpi_2, \varpi_3, \varpi_4)\rangle,\ tr(\varpi_1) = j_1,\ tr(\varpi_i) = 0,\ i \in \{3,4\},$

$\mathcal{B}_{j_10j_30} = \langle(\varpi_1, \varpi_2, \varpi_3, \varpi_4)\rangle,\ tr(\varpi_1) = j_1,\ tr(\varpi_i) = 0,\ i \in \{2,4\},$

$\mathcal{B}_{j_100j_4} = \langle(\varpi_1, \varpi_2, \varpi_3, \varpi_4)\rangle,\ tr(\varpi_1) = j_1,\ tr(\varpi_i) = 0,\ i \in \{2,3\},$

$\mathcal{B}_{0j_2j_30} = \langle(\varpi_1, \varpi_2, \varpi_3, \varpi_4)\rangle,\ tr(\varpi_1) = j_1,\ tr(\varpi_i) = 0,\ i \in \{1,4\},$

$\mathcal{B}_{0j_20j_4} = \langle(\varpi_1, \varpi_2, \varpi_3, \varpi_4)\rangle,\ tr(\varpi_1) = j_1,\ tr(\varpi_i) = 0,\ i \in \{1,3\},$

$\mathcal{B}_{00j_3j_4} = \langle(\varpi_1, \varpi_2, \varpi_3, \varpi_4)\rangle,\ tr(\varpi_1) = j_1,\ tr(\varpi_i) = 0,\ i \in \{1,2\},$

$\mathcal{B}_{j_1j_2j_30} = \langle(\varpi_1, \varpi_2, \varpi_3, \varpi_4)\rangle,\ tr(\varpi_1) = j_1,\ tr(\varpi_2) = j_2,\ tr(\varpi_3) = j_3,\ tr(\varpi_4) = 0,$

$\mathcal{B}_{j_1j_20j_4} = \langle(\varpi_1, \varpi_2, \varpi_3, \varpi_4)\rangle,\ tr(\varpi_1) = j_1,\ tr(\varpi_2) = j_2,\ tr(\varpi_3) = 0,\ tr(\varpi_4) = j_4,$

$\mathcal{B}_{j_10j_3j_4} = \langle(\varpi_1, \varpi_2, \varpi_3, \varpi_4)\rangle,\ tr(\varpi_1) = j_1,\ tr(\varpi_2) = 0,\ tr(\varpi_3) = j_3,\ tr(\varpi_4) = j_4,$

$\mathcal{B}_{0j_2j_3j_4} = \langle(\varpi_1, \varpi_2, \varpi_3, \varpi_4)\rangle,\ tr(\varpi_1) = 0,\ tr(\varpi_2) = j_2,\ tr(\varpi_3) = j_3,\ tr(\varpi_4) = j_4,$

$\mathcal{B}_{j_1j_2j_3j_4} = \langle(\varpi_1, \varpi_2, \varpi_3, \varpi_4)\rangle,\ tr(\varpi_1) = j_1,\ tr(\varpi_2) = j_2,\ tr(\varpi_3) = j_3,\ tr(\varpi_4) = j_4,$ *we can obtain the following relationship*

$$|\mathcal{B}_{0000}| = 0, |\mathcal{B}_{j_1000}| = 0, |\mathcal{B}_{j_1j_200}| = 0, |\mathcal{B}_{j_1j_2j_30}| = 0 \text{ and } |\mathcal{B}_{j_1j_2j_3j_4}| = 1. \tag{3.16}$$

We calculate,

$$\begin{aligned}\sum_{a\in(\mathcal{H})^{\times}} e^{\frac{2i\pi}{5}tr(\langle a,\varpi\rangle_{\mathfrak{R}_{5,3}})} &= |\mathcal{B}_{0000}|e^{\frac{2i\pi}{5}0} + \sum_{j_1=1}^{4}|\mathcal{B}_{j_1000}|e^{\frac{2i\pi}{5}j_1} + \cdots + \sum_{j_4=1}^{4}|\mathcal{B}_{000j_4}|e^{\frac{2i\pi}{5}j_4} \\ &+ \sum_{j_1=1}^{4}\sum_{j_2=1}^{4}|\mathcal{B}_{j_1j_200}|e^{\frac{2i\pi}{5}(j_1+j_2)} + \cdots + \sum_{j_3=1}^{4}\sum_{j_4=1}^{4}|\mathcal{B}_{0j_3j_4}|e^{\frac{2i\pi}{5}(j_3+j_4)} \\ &+ \sum_{j_1=1}^{4}\sum_{j_2=1}^{4}\sum_{j_3=1}^{4}|\mathcal{B}_{j_1j_2j_30}|e^{\frac{2i\pi}{5}(j_1+j_2+j_3)} + \sum_{j_1=1}^{4}\sum_{j_3=1}^{4}\sum_{j_4=1}^{4}|\mathcal{B}_{j_1j_2j_30}|e^{\frac{2i\pi}{5}(j_1+j_3+j_4)} \\ &+ \sum_{j_1=1}^{4}\sum_{j_2=1}^{4}\sum_{j_4=1}^{4}|\mathcal{B}_{j_1j_20j_4}|e^{\frac{2i\pi}{5}(j_1+j_2+j_4)} + \sum_{j_2=1}^{4}\sum_{j_3=1}^{4}\sum_{j_4=1}^{4}|\mathcal{B}_{0j_2j_3j_4}|e^{\frac{2i\pi}{5}(j_2+j_3+j_4)} \\ &+ \sum_{j_1=1}^{4}\sum_{j_2=1}^{4}\sum_{j_3=1}^{4}\sum_{j_4=1}^{4}|\mathcal{B}_{j_1j_2j_3j_4}|e^{\frac{2i\pi}{5}(j_1+j_2+j_3+j_4)} \\ &= 0 + 0.. + \sum_{j_1=1}^{4}e^{\frac{2i\pi}{5}j_1}\sum_{j_2=1}^{4}e^{\frac{2i\pi}{5}j_2}\sum_{j_3=1}^{4}e^{\frac{2i\pi}{5}j_3}\sum_{j_4=1}^{4}e^{\frac{2i\pi}{5}j_4} \\ &= (-1)(-1)(-1)(-1) = 1\end{aligned}$$

The following is the final result.

$$\omega_{hom}(\varpi_1,\varpi_2,\varpi_3,\varpi_4) = \frac{255}{256}\eta_2. \tag{3.17}$$

Example 3.3.5 *Let $\mathcal{C}_0,\mathcal{C}_1,\mathcal{C}_2,\mathcal{C}_3$ are linear codes of lenght 4 and dimension 2 over $\mathfrak{R}_{5,3}$, with generator matrices*

$$G_0 = \begin{bmatrix}2131\\1322\end{bmatrix}, G_1 = \begin{bmatrix}0221\\1120\end{bmatrix},$$

$$G_2 = \begin{bmatrix}1031\\0103\end{bmatrix} \text{ and } G_3 = \begin{bmatrix}1011\\0112\end{bmatrix}.$$

Assume that $\varepsilon = 1 + 4u_1 + 4u_2 + 4u_3$*, the generator matrix* G *is computed as follows*

$$G = \begin{bmatrix} 2\varepsilon & \varepsilon & 3\varepsilon & \varepsilon \\ \varepsilon & 3\varepsilon & 2\varepsilon & 2\varepsilon \\ 0 & 2u_1 & 2u_1 & u_1 \\ u_1 & u_1 & 2u_1 & 0 \\ u_2 & 0 & 3u_2 & u_2 \\ 0 & u_2 & 0 & 3u_2 \\ u_3 & 0 & u_3 & u_3 \\ 0 & u_3 & u_3 & 2u_3 \end{bmatrix}.$$

If $\eta_1 = 0$ *and* $\eta_2 = \dfrac{512}{255}$*, for all* $c \in C$*, then we have*

$$w_{hom}(c) \in \{6, 8, 10, 14, 16\}.$$

Furthermore

$$\Psi(G) = \begin{bmatrix} 2131 & 0000 & 0000 & 0000 \\ 1322 & 0000 & 0000 & 0000 \\ 2131 & 0221 & 0000 & 0000 \\ 1322 & 1120 & 0000 & 0000 \\ 2131 & 0000 & 1031 & 0000 \\ 1322 & 0000 & 0103 & 0000 \\ 2131 & 0000 & 0000 & 1011 \\ 1322 & 0000 & 0000 & 0112 \end{bmatrix}.$$

Example 3.3.6 *Let* $\mathcal{C}_0, \mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$ *are* $[26, 4]$*-linear codes over* $\mathfrak{R}_{5,3}$*, with generator matrices*

$$G_i = \begin{bmatrix} 00142323230023014140231414 \\ 00002233112344122334001144 \\ 10111111222222333333444444 \\ 01111111111111111111111111 \end{bmatrix}, \text{ for } 0 \leq i \leq 3.$$

Assume that $\varepsilon = 1+4u_1+4u_2+4u_3$*, the generator matrix of* C *is therefore given as follows.*

$$G = \begin{bmatrix} \overline{\mathcal{G}} & \overline{\overline{\mathcal{G}}} \end{bmatrix},$$

with

$$\overline{\mathcal{G}} = \begin{bmatrix}
0 & 0 & \varepsilon & 4\varepsilon & 2\varepsilon & 3\varepsilon & 2\varepsilon & 3\varepsilon & 2\varepsilon & 3\varepsilon & 0 & 0 & 2\varepsilon \\
0 & 0 & 0 & 0 & 2\varepsilon & 2\varepsilon & 3\varepsilon & 3\varepsilon & \varepsilon & \varepsilon & 2\varepsilon & 3\varepsilon & 4\varepsilon \\
\varepsilon & 0 & \varepsilon & \varepsilon & \varepsilon & \varepsilon & \varepsilon & \varepsilon & 2\varepsilon & 2\varepsilon & 2\varepsilon & 2\varepsilon & 2\varepsilon \\
0 & \varepsilon & \varepsilon & \varepsilon & \varepsilon & \varepsilon & \varepsilon & \varepsilon & \varepsilon & \varepsilon & \varepsilon & \varepsilon & \varepsilon \\
0 & 0 & u_1 & 4u_1 & 2u_1 & 3u_1 & 2u_1 & 3u_1 & 2u_1 & 3u_1 & 0 & 0 & 2u_1 \\
0 & 0 & 0 & 0 & 2u_1 & 2u_1 & 3u_1 & 3u_1 & u_1 & u_1 & 2u_1 & 3u_1 & 4u_1 \\
u_1 & 0 & u_1 & u_1 & u_1 & u_1 & u_1 & u_1 & 2u_1 & 2u_1 & 2u_1 & 2u_1 & 2u_1 \\
0 & u_1 & u_1 & u_1 & u_1 & u_1 & u_1 & u_1 & u_1 & u_1 & u_1 & u_1 & u_1 \\
0 & 0 & u_2 & 4u_2 & 2u_2 & 3u_2 & 2u_2 & 3u_2 & 2u_2 & 3u_2 & 0 & 0 & 2u_2 \\
0 & 0 & 0 & 0 & 2u_2 & 2u_2 & 3u_2 & 3u_2 & u_2 & u_2 & 2u_2 & 3u_2 & 4u_2 \\
u_2 & 0 & u_2 & u_2 & u_2 & u_2 & u_2 & u_2 & 2u_2 & 2u_2 & 2u_2 & 2u_2 & 2u_2 \\
0 & u_2 & u_2 & u_2 & u_2 & u_2 & u_2 & u_2 & u_2 & u_2 & u_2 & u_2 & u_2 \\
0 & 0 & u_3 & 4u_3 & 2u_3 & 3u_3 & 2u_3 & 3u_3 & 2u_3 & 3u_3 & 0 & 0 & 2u_3 \\
0 & 0 & 0 & 0 & 2u_3 & 2u_3 & 3u_3 & 3u_3 & u_3 & u_3 & 2u_3 & 3u_3 & 4u_3 \\
u_3 & 0 & u_3 & u_3 & u_3 & u_3 & u_3 & u_3 & 2u_3 & 2u_3 & 2u_3 & 2u_3 & 2u_3 \\
0 & u_3 & u_3 & u_3 & u_3 & u_3 & u_3 & u_3 & u_3 & u_3 & u_3 & u_3 & u_3
\end{bmatrix}$$

and

$$\overline{\overline{\mathcal{G}}} = \begin{bmatrix}
3\varepsilon & 0 & \varepsilon & 4\varepsilon & \varepsilon & 4\varepsilon & 0 & 2\varepsilon & 3\varepsilon & \varepsilon & 4\varepsilon & \varepsilon & 4\varepsilon \\
4\varepsilon & \varepsilon & 2\varepsilon & 2\varepsilon & 3\varepsilon & 3\varepsilon & 4\varepsilon & 0 & 0 & \varepsilon & \varepsilon & 4\varepsilon & 4\varepsilon \\
2\varepsilon & 3\varepsilon & 3\varepsilon & 3\varepsilon & 3\varepsilon & 3\varepsilon & 3\varepsilon & 4\varepsilon & 4\varepsilon & 4\varepsilon & 4\varepsilon & 4\varepsilon & 4\varepsilon \\
\varepsilon & \varepsilon & \varepsilon & \varepsilon & \varepsilon & \varepsilon & \varepsilon & \varepsilon & \varepsilon & \varepsilon & \varepsilon & \varepsilon & \varepsilon \\
3u_1 & 0 & u_1 & 4u_1 & u_1 & 4u_1 & 0 & 2u_1 & 3u_1 & u_1 & 4u_1 & u_1 & 4u_1 \\
4u_1 & u_1 & 2u_1 & 2u_1 & 3u_1 & 3u_1 & 4u_1 & 0 & 0 & u_1 & u_1 & 4u_1 & 4u_1 \\
2u_1 & 3u_1 & 3u_1 & 3u_1 & 3u_1 & 3u_1 & 3u_1 & 4u_1 & 4u_1 & 4u_1 & 4u_1 & 4u_1 & 4u_1 \\
u_1 & u_1 & u_1 & u_1 & u_1 & u_1 & u_1 & u_1 & u_1 & u_1 & u_1 & u_1 & u_1 \\
3u_2 & 0 & u_2 & 4u_2 & u_2 & 4u_2 & 0 & 2u_2 & 3u_2 & u_2 & 4u_2 & u_2 & 4u_2 \\
4u_2 & u_2 & 2u_2 & 2u_2 & 3u_2 & 3u_2 & 4u_2 & 0 & 0 & u_2 & u_2 & 4u_2 & 4u_2 \\
2u_2 & 3u_2 & 3u_2 & 3u_2 & 3u_2 & 3u_2 & 3u_2 & 4u_2 & 4u_2 & 4u_2 & 4u_2 & 4u_2 & 4u_2 \\
u_2 & u_2 & u_2 & u_2 & u_2 & u_2 & u_2 & u_2 & u_2 & u_2 & u_2 & u_2 & u_2 \\
3u_3 & 0 & u_3 & 4u_3 & u_3 & 4u_3 & 0 & 2u_3 & 3u_3 & u_3 & 4u_3 & u_3 & 4u_3 \\
4u_3 & u_3 & 2u_3 & 2u_3 & 3u_3 & 3u_3 & 4u_3 & 0 & 0 & u_3 & u_3 & 4u_3 & 4u_3 \\
2u_3 & 3u_3 & 3u_3 & 3u_3 & 3u_3 & 3u_3 & 3u_3 & 4u_3 & 4u_3 & 4u_3 & 4u_3 & 4u_3 & 4u_3 \\
u_3 & u_3 & u_3 & u_3 & u_3 & u_3 & u_3 & u_3 & u_3 & u_3 & u_3 & u_3 & u_3
\end{bmatrix}.$$

If $\eta_1 = \dfrac{64}{65}$ *and* $\eta_2 = \dfrac{768}{255}$, *for all* $c \in C$, *we then have*

$$w_{hom}(c) \in \{75, 150, 183\}.$$

Also, the $\Psi(C)$ *generator matrix is determined by*

$$\Psi(G) = \begin{bmatrix} \mathcal{D}_1 & \mathcal{D}_2 \end{bmatrix},$$

where

$$\mathcal{D}_1 = \begin{bmatrix} 00142323230023014140231414 & 00000000000000000000000000 \\ 00002233112344122334001144 & 00000000000000000000000000 \\ 10111111222222333333444444 & 00000000000000000000000000 \\ 01111111111111111111111111 & 00000000000000000000000000 \\ 00142323230023014140231414 & 00142323230023014140231414 \\ 00002233112344122334001144 & 00002233112344122334001144 \\ 10111111222222333333444444 & 10111111222222333333444444 \\ 01111111111111111111111111 & 01111111111111111111111111 \\ 00142323230023014140231414 & 00000000000000000000000000 \\ 00002233112344122334001144 & 00000000000000000000000000 \\ 10111111222222333333444444 & 00000000000000000000000000 \\ 01111111111111111111111111 & 00000000000000000000000000 \\ 00142323230023014140231414 & 00000000000000000000000000 \\ 00002233112344122334001144 & 00000000000000000000000000 \\ 10111111222222333333444444 & 00000000000000000000000000 \\ 01111111111111111111111111 & 00000000000000000000000000 \end{bmatrix}$$

and

$$\mathcal{D}_2 = \begin{bmatrix} 00000000000000000000000000 & 00000000000000000000000000 \\ 00000000000000000000000000 & 00000000000000000000000000 \\ 00000000000000000000000000 & 00000000000000000000000000 \\ 00000000000000000000000000 & 00000000000000000000000000 \\ 00000000000000000000000000 & 00000000000000000000000000 \\ 00000000000000000000000000 & 00000000000000000000000000 \\ 00000000000000000000000000 & 00000000000000000000000000 \\ 00000000000000000000000000 & 00000000000000000000000000 \\ 00142323230023014140231414 & 00000000000000000000000000 \\ 00002233112344122334001144 & 00000000000000000000000000 \\ 10111111222222333333444444 & 00000000000000000000000000 \\ 01111111111111111111111111 & 00000000000000000000000000 \\ 00000000000000000000000000 & 00142323230023014140231414 \\ 00000000000000000000000000 & 00002233112344122334001144 \\ 00000000000000000000000000 & 10111111222222333333444444 \\ 00000000000000000000000000 & 01111111111111111111111111 \end{bmatrix}$$

3.4 Conclusion

This chapter studied linear codes over the particular Frobenius ring $\mathfrak{R}_{5,3} = \mathbb{F}_5 + u_1\mathbb{F}_5 + u_2\mathbb{F}_5 + u_3\mathbb{F}_5$, with $u_i^2 = u_i$ and $1 \leq i \leq 3$, that endowed duality and a Gray map that preserves distance. Additionally, we principally research the created homogenous weight on this ring's structural characteristics.

Chapter 4

HOMOGENEOUS WEIGHTS AND LINEAR SIMPLEX AND MacDonald CODES OVER THE RING $\mathcal{R}_{p^s,\theta}$

4.1 Introduction

Over the past two decades, simplex and MacDonald codes over finite rings have proven successful in generating new classes of linear codes, particularly in the context of commutative rings such as finite Frobenius rings. This chapter focuses on our efforts to compute homogeneous points on the novel ring $\mathcal{R}_{p^s,\theta}$, providing illustrative examples of applications. Subsequently, we present a fresh definition of simplex and MacDonald codes, along with the introduction of Gray images for these codes. Lastly, we calculate the covering radius. Throughout this developmental exploration, we leverage relevant references, including [21, 23, 27, 49, 50, 53, 80].

4.2 Compute the homogeneous weight on the ring $\mathcal{R}_{p^s,\theta}$

Using the results of [49,50,53,58], the homogeneous weight on $\mathcal{R}_{p^s,\theta}$ can be determined. In the first by Theorem 2.2.4, the ideals of $\mathbb{F}_{p^s}^{(\theta+1)}$ are the followings $\overbrace{\mathbb{F}_{p^s} \times \mathbb{F}_{p^s} \times \ldots \times \mathbb{F}_{p^s}}^{(\theta+1)} = \langle (x_1, x_2, \ldots, x_{\theta+1}) \rangle, x_1, x_2, \ldots, x_{\theta+1} \neq 0,$
$\mathbb{F}_{p^s} \times \{0\} \times \ldots \times \{0\} = \langle (x_1, 0, \ldots, 0) \rangle, x_1 \neq 0,$
$\vdots$
$\{0\} \times \{0\} \times \ldots \times \mathbb{F}_{p^s} = \langle (0, 0, \ldots, x_{\theta+1}) \rangle, x_{\theta+1} \neq 0,$
$\{(0, 0, \ldots, 0)\} = \langle (0, 0, \ldots, 0) \rangle$. In the light of previous results, we can note that

1. The zero divisors of $\mathbb{F}_{p^s} \times \mathbb{F}_{p^s} \times \ldots \times \mathbb{F}_{p^s}$ are $(\theta+1)(p^s-1)$,
2. The unit of $\mathbb{F}_{p^s} \times \mathbb{F}_{p^s} \times \ldots \times \mathbb{F}_{p^s}$ are $|(\mathbb{F}_{p^s} \times \mathbb{F}_{p^s} \times \ldots \times \mathbb{F}_{p^s})^{\times}| = (p^s-1)^{(\theta+1)}$,
3. The ideals $\langle (x_1, 0, \ldots, 0) \rangle, \langle (0, x_2, \ldots, 0) \rangle, \ldots, \langle (0, 0, \ldots, x_{\theta+1}) \rangle$ in $\mathbb{F}_{p^s} \times \mathbb{F}_{p^s} \times \ldots \times \mathbb{F}_{p^s}$ are maximals.

Our aim of now, is to prove the following result.

Theorem 4.2.1 *The homogeneous weight of an element x of $\mathcal{R}_{p^s,\theta}$ in the sense of Definition 2.2.1, is defined as follows*

$$w_{hom}(x) = \begin{cases} 0 & \text{if} \quad x = 0, \\ \eta\left(\dfrac{(p^s-1)^{\theta}+1}{(p^s-1)^{\theta}}\right) & \text{if} \quad x \text{ is divisor of zero}, \\ \eta\left(\dfrac{(p^s-1)^{(\theta+1)}+1}{(p^s-1)^{(\theta+1)}}\right) & \text{if} \quad x \text{ is unit and } \theta \text{ is even}, \\ \eta\left(\dfrac{(p^s-1)^{(\theta+1)}-1}{(p^s-1)^{(\theta+1)}}\right) & \text{if} \quad x \text{ is unit and } \theta \text{ is odd}. \end{cases}$$

Proof 4.2.2 *Let $\mathcal{H} = \mathbb{F}_{p^s}^{\theta+1}$, according to Equation (2.10), the homogeneous weight of $x = (x_1, x_2, \ldots, x_{\theta+1}) \in \mathcal{H}$ is given by*

$$w_{hom}(x) = \eta\left(1 - \frac{1}{(p^s-1)^{\theta+1}} \sum_{a \in (\mathcal{H})^{\times}} e^{\frac{2\pi i}{p} tr(\langle a,x \rangle_{\mathcal{R}_{p^s,\theta}})}\right), \tag{4.1}$$

with $a = (a_1, a_2, \ldots, a_{\theta+1})$ *therefore, we calculate the homogeneous weight on three cases.* ***Case 1, for*** $(x_1, x_2, \ldots, x_{\theta+1}) = (0, 0, \ldots, 0)$*, we have* $tr((0, 0, \ldots, 0)) = 0$*, and*

$$w_{hom}((0, 0, \ldots, 0)) = \eta \left(1 - \frac{1}{(p^s - 1)^{\theta+1}} \sum_{a \in (\mathcal{H})^\times} e^0 \right),$$

then

$$w_{hom}((0, 0, \ldots, 0)) = \eta \left(1 - \frac{1}{(p^s - 1)^{\theta+1}} (p^s - 1)^{\theta+1} \right),$$

so that

$$w_{hom}((0, 0, \ldots, 0)) = 0. \tag{4.2}$$

Case 2, if $(x_1, x_2, \ldots, x_{\theta+1}) \in \mathcal{H}$ ***is a zero divisor****, assume that* $x_2, \ldots, x_{\theta+1} = 0$ *and* $x_1 \neq 0$*(that means* $x_1 \in \mathbb{F}_{p^s}^*$ *and* $|\mathbb{F}_{p^s}^*| = p^s - 1$*), we have* $tr(\langle a, x \rangle_{\mathcal{R}_{p^s,\theta}}) = tr(a_1 x_1), a = (a_1, a_2, \ldots, a_{\theta+1}) \in (\mathcal{H})^\times$*. Then,* • *The number of elements* $\rho \in \mathbb{F}_{p^s}^*$*, such that* $tr(\rho) = 0$ *is* $p^{s-1} - 1$*.* • *For* $j = 1, \ldots, p-1$*, the number of elements* $\varrho \in \mathbb{F}_{p^s}^*$*, such that* $tr(\varrho) = j$ *is* p^{s-1}*. By Equation (2.11), we have*

$$\begin{aligned} \sum_{a \in \mathbb{F}_{p^s}^*} e^{\frac{2\pi i}{p} tr(ax)} &= (p^{s-1} - 1)(p^s - 1) e^{\frac{2\pi i}{p} 0} + p^{s-1}(p^s - 1) \sum_{j=1}^{p-1} e^{\frac{2\pi j}{p} i} \\ &= (p^{s-1} - 1)(p^s - 1) + p^{s-1}(p^s - 1)(-1) \\ &= -(p^s - 1), \end{aligned}$$

consequently

$$\begin{aligned} w_{hom}((x_1, x_2, \ldots, x_{\theta+1})) &= \eta \left(1 - \frac{1}{(p^s - 1)^{\theta+1}} (-(p^s - 1)) \right) \\ &= \eta \left(\frac{(p^s - 1)^\theta + 1}{(p^s - 1)^\theta} \right). \end{aligned}$$

Case 3 assume that $(x_1, x_2, \ldots, x_\theta) \in \mathcal{H}$ ***is a unit.*** *Since the set* $(\mathcal{H})^\times$ *forms a group*

under the multiplication, consider the following disjoint subsets of $(\mathcal{H})^{\times}$.

$$\begin{aligned}
S_{00\ldots0} &= \langle (x_1, x_2, \ldots, x_{\theta+1}) \rangle, tr(x_i) = 0, i = \overline{1, \theta+1} \\
S_{j_1 0\ldots0} &= \langle (x_1, x_2, \ldots, x_{\theta+1}) \rangle, tr(x_1) = j_1, tr(x_i) = 0, i = \overline{2, \theta+1} \\
&\vdots \\
S_{j_1 j_2 \ldots j_{\theta+1}} &= \langle (x_1, x_2, \ldots, x_{\theta+1}) \rangle tr(x_i) = j_i, i = \overline{1, \theta+1}.
\end{aligned}$$

Then,

$$\begin{aligned}
|S_{00\ldots0}| &= (p^{s-1} - 1)^{\theta+1} \\
|S_{j_1 0\ldots0}| &= |S_{0 j_2 \ldots 0}| = \ldots = |S_{00\ldots j_{\theta+1}}| = p^{s-1}(p^{s-1} - 1)^{\theta} \\
|S_{j_1 j_2 0\ldots0}| &= |S_{0 j_2 j_3 \ldots 0}| = \ldots = |S_{00\ldots j_\theta j_{\theta+1}}| = (p^{s-1})^2 (p^{s-1} - 1)^{\theta-1} \\
&\vdots \\
|S_{j_1 j_2 \ldots j_{\theta+1}}| &= (p^{s-1})^{\theta+1}.
\end{aligned}$$

Therefore,

$$\sum_{a \in (\mathcal{H})^{\times}} e^{\frac{2\pi i}{p} tr(\langle a, x \rangle_{\mathcal{R}_{p^s, \theta}})} = \mathcal{B}_0 + \mathcal{B}_1 + \mathcal{B}_2 + \mathcal{B}_3 + \ldots + \mathcal{B}_\theta.$$

Where,

$$
\begin{aligned}
\mathcal{B}_0 &= |S_{00\ldots0}|e^{\frac{2\pi i}{p}(0)}, \\
\mathcal{B}_1 &= \sum_{j_1=1}^{p-1}|S_{j_0 0\ldots0}|e^{\frac{2\pi i}{p}(j_1)} + \sum_{j_2=1}^{p-1}|S_{0 j_2\ldots0}|e^{\frac{2\pi i}{p}(j_2)} + \ldots + \sum_{j_{\theta+1}=1}^{p-1}|S_{00\ldots j_{\theta+1}}|e^{\frac{2\pi i}{p}(j_{\theta+1})}, \\
\mathcal{B}_2 &= \sum_{j_1=1}^{p-1}\sum_{j_2=1}^{p-1}|S_{j_1 j_2\ldots0}|e^{\frac{2\pi i}{p}(j_1+j_2)} + \ldots + \sum_{j_\theta=1}^{p-1}\sum_{j_{\theta+1}=1}^{p-1}|S_{00\ldots j_\theta j_{\theta+1}}|e^{\frac{2\pi i}{p}(j_\theta+j_{\theta+1})}, \\
\mathcal{B}_3 &= \sum_{j_1=1}^{p-1}\sum_{j_2=1}^{p-1}\sum_{j_3=1}^{p-1}|S_{j_1 j_2 j_3\ldots0}|e^{\frac{2\pi i}{p}(j_1+j_2+j_3)} + \ldots \\
&\quad + \sum_{j_{\theta-1}=1}^{p-1}\sum_{j_\theta=1}^{p-1}\sum_{j_{\theta+1}=1}^{p-1}|S_{0\ldots j_{\theta-1} j_\theta j_{\theta+1}}|e^{\frac{2\pi i}{p}(j_{\theta-1}+j_\theta+j_{\theta+1})} \\
&\vdots \\
\mathcal{B}_\theta &= \sum_{j_1=1}^{p-1}\sum_{j_2=1}^{p-1}\cdots\sum_{j_{\theta+1}=1}^{p-1}|S_{j_1 j_2\ldots j_{\theta+1}}|e^{\frac{2\pi i}{p}(j_1+j_2+\ldots+j_{\theta+1})},
\end{aligned}
$$

so

$$
\begin{aligned}
\mathcal{B}_0 &= (p^{s-1}-1)^{\theta+1}, \\
\mathcal{B}_1 &= (\theta+1)p^{s-1}(p^{s-1}-1)^\theta \sum_{j_1=1}^{p-1} e^{\frac{2\pi i}{p}(j_1)}, \\
\mathcal{B}_2 &= (\theta+1)(p^{s-1})^2(p^{s-1}-1)^\theta \sum_{j_1=1}^{p-1} e^{\frac{2\pi i}{p}(j_1)} \sum_{j_2=1}^{p-1} e^{\frac{2\pi i}{p}(j_2)}, \\
\mathcal{B}_3 &= (\theta+1)(p^{s-1})^3(p^{s-1}-1)^{\theta-1} \sum_{j_1=1}^{p-1} e^{\frac{2\pi i}{p}(j_1)} \sum_{j_2=1}^{p-1} e^{\frac{2\pi i}{p}(j_2)} \sum_{j_3=1}^{p-1} e^{\frac{2\pi i}{p}(j_3)} \\
&\vdots \\
\mathcal{B}_\theta &= (p^{s-1})^{\theta+1} \sum_{j_1=1}^{p-1} e^{\frac{2\pi i}{p}(j_1)} \sum_{j_1=1}^{p-1} e^{\frac{2\pi i}{p}(j_2)} \cdots \sum_{j_{\theta+1}=1}^{p-1} e^{\frac{2\pi i}{p}(j_{\theta+1})}.
\end{aligned}
$$

Hence,

$$\begin{aligned}\sum_{a\in(\mathcal{H})^{\times}} e^{\frac{2\pi i}{p}tr(\langle a,x\rangle_{\mathcal{R}_{p^s},\theta})} &= (p^{s-1}-1)^{\theta+1}+(\theta+1)p^{s-1}(p^{s-1}-1)^{\theta}(-1)\\ &\quad+(\theta+1)(p^{s-1})^2(p^{s-1}-1)^{\theta-1}(-1)(-1)+\ldots\\ &\quad+(p^{s-1})^{\theta+1}\overbrace{(-1)(-1)\ldots(-1)}^{\theta+1}.\end{aligned}$$

Now, assume $\mathcal{A} = (p^{s-1}-1)^{\theta+1}+(\theta+1)p^{s-1}(p^{s-1}-1)^{\theta}(-1)+(\theta+1)(p^{s-1})^2(p^{s-1}-1)^{\theta-1}(-1)(-1)+\ldots+(p^{s-1})^{\theta+1}\overbrace{(-1)(-1)\ldots(-1)}^{\theta+1}$, *then*

$$\mathcal{A}=\begin{cases}1 & \text{if } \theta \text{ odd},\\ -1 & \text{if } \theta \text{ even}.\end{cases}$$

As a result,

$$w_{hom}((x_1,x_2,\ldots,x_{\theta+1})) = \eta\left(1-\frac{1}{(p^s-1)^{\theta+1}}\mathcal{A}\right), \tag{4.3}$$

by Equation (4.3), we have

$$w_{hom}((x_1,x_2,\ldots,x_{\theta+1}))=\begin{cases}\eta\left(1-\frac{1}{(p^s-1)^{\theta+1}})\right) & \text{if } \theta \text{ odd},\\ \eta\left(1+\frac{1}{(p^s-1)^{\theta+1}})\right) & \text{if } \theta \text{ even}.\end{cases} \tag{4.4}$$

■

Example 4.2.3 *Let* $C_0=C_1=C_2=C_3$ *with* C_i *is* $[4,2]$*-linear codes, for* $0\le i\le 3$ *over* $\mathfrak{R}_{5,3}=\mathbb{F}_5+u_1\mathbb{F}_5+u_2\mathbb{F}_5+u_3\mathbb{F}_5$, *their generator matrices is* $G_0=G_1=G_2=G_3=\begin{bmatrix}1011\\0112\end{bmatrix}$. *Then the generator matrix of* C, *as follows* $G=$

$$\begin{bmatrix}
1+4u_1+4u_2+4u_3 & 0 & 1+4u_1+4u_2+4u_3 & 1+4u_1+4u_2+4u_3\\
0 & 1+4u_1+4u_2+4u_3 & 1+4u_1+4u_2+4u_3 & 2+3u_1+3u_2+3u_3\\
u_1 & 0 & u_1 & u_1\\
0 & u_1 & u_1 & 2u_1\\
u_2 & 0 & u_2 & u_2\\
0 & u_2 & u_2 & 2u_2\\
u_3 & 0 & u_3 & u_3\\
0 & u_3 & u_3 & 2u_3
\end{bmatrix},$$

if $\eta = \dfrac{512}{255}$, *for all* $c \in C$, *we have* $w_{hom}(c) = 6$, *furthermore*

$$\Psi(G) = \begin{bmatrix} 1011 & 0000 & 0000 & 0000 \\ 0112 & 0000 & 0000 & 0000 \\ 1011 & 1011 & 0000 & 0000 \\ 0112 & 0112 & 0000 & 0000 \\ 1011 & 0000 & 1011 & 0000 \\ 0112 & 0000 & 0112 & 0000 \\ 1011 & 0000 & 0000 & 1011 \\ 0112 & 0000 & 0000 & 0112 \end{bmatrix}.$$

Example 4.2.4 *Let* C_0, C_1, C_2 *and* C_3 *are* $[6,3]$*-linear codes over* $\mathfrak{R}_{5,3} = \mathbb{F}_5 + u_1\mathbb{F}_5 + u_2\mathbb{F}_5 + u_3\mathbb{F}_5$, *with generator matrices* $G_0 = G_1 = \begin{bmatrix} 100224 \\ 010313 \\ 001422 \end{bmatrix}$, $G_2 = \begin{bmatrix} 100111 \\ 010123 \\ 001132 \end{bmatrix}$ *and* $G_3 = \begin{bmatrix} 100111 \\ 010321 \\ 201043 \end{bmatrix}$. *Assume that* $\varepsilon = 1 + 4u_1 + 4u_2 + 4u_3$, *then*

$$G = \begin{bmatrix} \varepsilon & 0 & 0 & 2\varepsilon & 2\varepsilon & 4\varepsilon \\ 0 & \varepsilon & 0 & 3\varepsilon & \varepsilon & 3\varepsilon \\ 0 & 0 & \varepsilon & 4\varepsilon & 2\varepsilon & 2\varepsilon \\ u_1 & 0 & 0 & 2u_1 & 2u_1 & 4u_1 \\ 0 & u_1 & 0 & 3u_1 & u_1 & 3u_1 \\ 0 & 0 & u_1 & 4u_1 & 2u_1 & 2u_1 \\ u_2 & 0 & 0 & u_2 & u_2 & u_2 \\ 0 & u_2 & 0 & u_2 & 2u_2 & 3u_2 \\ 0 & 0 & u_2 & u_2 & 3u_2 & 2u_2 \\ u_3 & 0 & 0 & u_3 & u_3 & u_3 \\ 0 & u_3 & 0 & 3u_3 & 2u_3 & u_3 \\ 2u_3 & 0 & u_3 & 0 & 4u_3 & 3u_3 \end{bmatrix}.$$

If $\eta = \dfrac{768}{255}$, *for all* $c \in C$, *we have* $w_{hom}(c) = 12$, *furthermore*

$$\Psi(G) = \begin{bmatrix} 100224 & 000000 & 000000 & 000000 \\ 010313 & 000000 & 000000 & 000000 \\ 001422 & 000000 & 000000 & 000000 \\ 100224 & 100224 & 000000 & 000000 \\ 010313 & 010313 & 000000 & 000000 \\ 001422 & 001422 & 000000 & 000000 \\ 100224 & 000000 & 100111 & 000000 \\ 010313 & 000000 & 010123 & 000000 \\ 001422 & 000000 & 001132 & 000000 \\ 100224 & 000000 & 000000 & 100111 \\ 010313 & 000000 & 000000 & 010321 \\ 001422 & 000000 & 000000 & 201043 \end{bmatrix}.$$

4.3 A new presentation of some linear codes over $\mathcal{R}_{p^s,\theta}$

In general, the construction of linear simplex and MacDonald codes is given in several articles, see [3, 4, 17, 21, 23]. In the next theorems, we devise a new construction of some linear codes over $\mathcal{R}_{p^s,\theta}$.

Theorem 4.3.1 *The generator matrix* $\mathcal{G}_k^{\alpha,\theta}$ *of* $\mathcal{S}_k^{\alpha,\theta}$, *a linear simplex code of type* α *over* $\mathcal{R}_{p^s,\theta}$, *is*

$$\mathcal{G}_k^{\alpha,\theta} = \ (1 - u_1 - \ldots - u_\theta)\mathcal{G}_k^{\alpha} + (u_1)\sigma_1(\mathcal{G}_k^{\alpha}) + \ldots + (u_\theta)\sigma_\theta(\mathcal{G}_k^{\alpha}) \ , \tag{4.5}$$

with $\sigma_i(\mathcal{G}_k^{\alpha})$ *and* $\mathcal{G}_k^{\alpha}$, *for* $1 \leq i \leq \theta$ *are equivalent matrices. where,* $\mathcal{G}_k^{\alpha} = \begin{bmatrix} \overbrace{G_k^{\alpha} \quad G_k^{\alpha} \quad \ldots \quad G_k^{\alpha}}^{p^{s\theta k}} \end{bmatrix}$

and G_k^{α} *is the generator matrix of a linear simplex code of type* α *over* $\mathbb{F}_{p^s}$.

Proof 4.3.2 *If* $\mathcal{R}_{p^s,\theta} = \{0, \eta_1, \eta_2, \ldots, \eta_{p^{(\theta+1)s}-1}\}$, *let* $\mathcal{G}_k^{\alpha,\theta}$ *is a generator matrix of simplex*

codes of type α over $\mathcal{R}_{p^s,\theta}$. According to [21], we have

$$\mathcal{G}_k^{\alpha,\theta} = \begin{bmatrix} 00\ldots0 & \eta_1\eta_1\ldots\eta_1 & \ldots & \eta_{p^{(\theta+1)s}-1}\eta_{p^{(\theta+1)s}-1}\ldots\eta_{p^{(\theta+1)s}-1} \\ \mathcal{G}_{k-1}^{\alpha,\theta} & \mathcal{G}_{k-1}^{\alpha,\theta} & \ldots & \mathcal{G}_{k-1}^{\alpha,\theta} \end{bmatrix}. \tag{4.6}$$

By Equation (2.5), the elements η_i, for $1 \leq i \leq p^{(\theta+1)s}-1$ are expressed in the form

$$\begin{aligned} 0 &= (1-u_1-\ldots-u_\theta)0 + u_1 0 + \ldots + u_\theta 0 \\ \eta_1 &= (1-u_1-\ldots-u_\theta)a_0^1 + u_1(a_1^1+a_0^1) + \ldots + u_\theta(a_\theta^1+a_0^1) \\ &\vdots \\ \eta_{p^{(\theta+1)s}-1} &= (1-u_1-\ldots-u_\theta)a_0^{p^{(\theta+1)s}-1} + \ldots + u_\theta(a_\theta^{p^{(\theta+1)s}-1}+a_0^{p^{(\theta+1)s}-1}), \end{aligned}$$

where $a_i^j \in \mathbb{F}_{p^s} = \{\xi^0, \xi^1, \ldots, \xi^{p^s-1}\}$, with $1 \leq j \leq p^{(\theta+1)s}-1$ and $0 \leq i \leq \theta$. The elements η_i, $1 \leq i \leq p^{(\theta+1)s}-1$ allow us to see that the generator matrix take the form

$$\mathcal{G}_k^{\alpha,\theta} = (1-u_1-\ldots-u_\theta)\mathcal{G}_k^\alpha + (u_1)\sigma_1(\mathcal{G}_k^\alpha) + \ldots + (u_\theta)\sigma_\theta(\mathcal{G}_k^\alpha), \tag{4.7}$$

where

$$\mathcal{G}_k^\alpha = \begin{bmatrix} \overbrace{\begin{matrix} \xi^0\ldots\xi^0 & \xi^1\ldots\xi^1 & \ldots & \xi^{p^s-1}\ldots\xi^{p^s-1} \end{matrix}}^{p^\theta sk} \\ \begin{matrix} \mathcal{G}_{k-1}^\alpha & \mathcal{G}_{k-1}^\alpha & \ldots & \mathcal{G}_{k-1}^\alpha \end{matrix} \end{bmatrix}.$$

■

Remark 4.3.3 *The code generated by this matrix, is called a simplex linear code of type α over $\mathcal{R}_{p^s,\theta}$, of length $p^{(\theta+1)sk}$ and the number of codewords is $p^{(\theta+1)s}$.*

Example 4.3.4 *For $\mathcal{R}_{2^2,1} = \mathbb{F}_4 + u_1\mathbb{F}_4$ where, $\mathbb{F}_4 = \{0, 1, \xi, \xi^2 = \xi+1\}$. A genrator matrix of a linear simplex code over $\mathcal{R}_{2^2,1} = \mathbb{F}_4 + u_1\mathbb{F}_4$ is*

$$\mathcal{G}_k^{\alpha,1} = (1-u_1)\mathcal{G}_k^\alpha + (u_1)\sigma_1(\mathcal{G}_k^\alpha),$$

for $k = 1$, we have

$$\mathcal{G}_1^{\alpha,1} = (1-u_1)\left[\ 01\xi\xi^2 01\xi\xi^2 01\xi\xi^2 01\xi\xi^2\ \right] + (u_1)\sigma_1\left(\left[\ 01\xi\xi^2 01\xi\xi^2 01\xi\xi^2 01\xi\xi^2\ \right]\right)$$

for $k = 2$, we have

$$\mathcal{G}_2^{\alpha,1} = (1-u_1)\begin{bmatrix} \overbrace{00001111\xi\xi\xi\xi\xi^2\xi^2\xi^2\xi^2}^{16} \\ 01\xi\xi^2 01\xi\xi^2 01\xi\xi^2 01\xi\xi^2 \end{bmatrix} + (u_1)\sigma_1\left(\begin{bmatrix} \overbrace{00001111\xi\xi\xi\xi\xi^2\xi^2\xi^2\xi^2}^{16} \\ 01\xi\xi^2 01\xi\xi^2 01\xi\xi^2 01\xi\xi^2 \end{bmatrix}\right).$$

As an immediate consequence of Theorem 4.3.1, we obtain the following.

Corollary 4.3.5 *The generator matrix $\mathcal{G}_{k,t}^{\alpha,\theta}$ of $\mathcal{M}_{k,t}^{\alpha,\theta}$, the linear MacDonald codes of type α over $\mathcal{R}_{p^s,\theta}$, is given by*

$$\mathcal{G}_{k,t}^{\alpha,\theta} = (1-u_1-\ldots-u_\theta)\mathcal{G}_{k,t}^{\alpha} + (u_1)\eta_1(\mathcal{G}_{k,t}^{\alpha}) + \ldots + (u_\theta)\eta_\theta(\mathcal{G}_{k,t}^{\alpha}) \ , \tag{4.8}$$

with, $\eta_i(\mathcal{G}_{k,t}^{\alpha})$ and $\mathcal{G}_{k,t}^{\alpha}$, for $1 \le i \le \theta$ and $1 \le t \le k-1$ are equivalent matrices. Where, $\mathcal{G}_{k,t}^{\alpha} = \begin{bmatrix} \overbrace{G_{k,t}^{\alpha} \quad G_{k,t}^{\alpha} \quad \ldots \quad G_{k,t}^{\alpha}}^{p^{s\theta k}} \end{bmatrix}$ and $G_{k,t}^{\alpha}$ is the generator matrix of linear MacDonald codes of type α over $\mathbb{F}_{p^s}$.

Proof 4.3.6 *Using similar method as in Theorem 4.3.1.*

Remark 4.3.7 *The code generated by the matrix $\mathcal{G}_{k,t}^{\alpha,\theta}$, is called linear MacDonald codes of type α over $\mathcal{R}_{p^s,\theta}$, of length $p^{(\theta+1)sk} - p^{(\theta+1)st}$ and the number of code words is $p^{(\theta+1)s}$.*

Example 4.3.8 *For $\mathcal{R}_{3,3} = \mathbb{F}_3 + u_1\mathbb{F}_3 + u_2\mathbb{F}_3 + u_3\mathbb{F}_3$, the genrator matrix of linear MacDonald codes over $\mathcal{R}_{3,3}$ is*

$$\mathcal{G}_{k,t}^{\alpha,3} = (1-u_1-u_2-u_3)\mathcal{G}_{k,t}^{\alpha} + (u_1)\eta_1(\mathcal{G}_{k,t}^{\alpha}) + (u_2)\eta_2(\mathcal{G}_{k,t}^{\alpha}) + (u_3)\eta_3(\mathcal{G}_{k,t}^{\alpha}) \ ,$$

for $k = 3$ and $1 \le t \le 2$, we have

$$\mathcal{G}_{3,t}^{\alpha,3} = (1-u_1-u_2-u_3)\mathcal{G}_{3,t}^{\alpha} + (u_1)\eta_1(\mathcal{G}_{3,t}^{\alpha}) + (u_2)\eta_2(\mathcal{G}_{3,t}^{\alpha}) + (u_3)\eta_3(\mathcal{G}_{3,t}^{\alpha}) \ ,$$

with $\mathcal{G}_{3,1}^{\alpha} = \begin{bmatrix} 111111111 & 222222222 \\ 000111222 & 000111222 \\ 012012012 & 012012012 \end{bmatrix}$ *and* $\mathcal{G}_{3,2}^{\alpha} = \begin{bmatrix} 000000 & 111111111 & 222222222 \\ 111222 & 000111222 & 000111222 \\ 012012 & 012012012 & 012012012 \end{bmatrix}$.

4.4 The Gray images of linear simplex and MacDonald codes

From the relations given in Theorem 2.1.19 and Corollary 2.1.18, It is simple to achieve the following consequences.

Theorem 4.4.1 *Let* $\mathcal{S}_k^{\alpha,\theta} = (1-u_1-\ldots-u_\theta)\mathcal{S}_k^\alpha \oplus (u_1)\sigma_1(\mathcal{S}_k^\alpha) \oplus \ldots \oplus (u_\theta)\sigma_\theta(\mathcal{S}_k^\alpha)$ *be a linear simplex code of length* n *over* $\mathcal{R}_{p^s,\theta}$*, where* $\mathcal{S}_k^\alpha$ *and* $\sigma_i(\mathcal{S}_k^\alpha)$*, for* $1 \leq i \leq \theta$ *are* $[n;k;d_i]$*-linear codes of type* α *over* $\mathbb{F}_{p^s}$*. Then* $\Phi(\mathcal{S}_k^{\alpha,\theta}) = \mathcal{S}_k^\alpha \otimes \sigma_1(\mathcal{S}_k^\alpha) \otimes \ldots \otimes \sigma_\theta(\mathcal{S}_k^\alpha)$ *is* $\left[(\theta+1)n; k; d = \sum_{i=0}^{\theta} d_i\right]$*-linear simplex code of type* α *over* $\mathbb{F}_{p^s}$*.*

Proof 4.4.2 *If,* $\mathcal{S}_k^{\alpha,\theta} = (1-u_1-\ldots-u_\theta)\mathcal{S}_k^\alpha \oplus (u_1)\sigma_1(\mathcal{S}_k^\alpha) \oplus \ldots \oplus (u_\theta)\sigma_\theta(\mathcal{S}_k^\alpha)$*, then*

$$\Phi(\mathcal{S}_k^{\alpha,\theta}) = \Phi((1-u_1-\ldots-u_\theta)\mathcal{S}_k^\alpha \oplus (u_1)\sigma_1(\mathcal{S}_k^\alpha) \oplus \ldots \oplus (u_\theta)\sigma_\theta(\mathcal{S}_k^\alpha)).$$

Since the Gray map Φ *is linear, we have,*

$$\Phi(\mathcal{S}_k^{\alpha,\theta}) = \Phi((1-u_1-\ldots-u_\theta)\mathcal{S}_k^\alpha) \oplus \Phi((u_1)\sigma_1(\mathcal{S}_k^\alpha)) \oplus \ldots \oplus \Phi((u_\theta)\sigma_\theta(\mathcal{S}_k^\alpha)).$$

So that,

$$\Phi(\mathcal{S}_k^{\alpha,\theta}) = \mathcal{S}_k^\alpha \otimes \sigma_1(\mathcal{S}_k^\alpha) \otimes \ldots \otimes \sigma_\theta(\mathcal{S}_k^\alpha).$$

■

Corollary 4.4.3 *If* $G_0, G_1, \ldots, G_\theta$ *are generator matrices of* $\Phi(\mathcal{S}_k^\alpha)$*,* $\Phi(\sigma_1(\mathcal{S}_k^\alpha))$*, ...,* $\Phi(\sigma_\theta(\mathcal{S}_k^\alpha))$ *respectively, then the generator matrix of* $\Phi(\mathcal{S}_k^{\alpha,\theta})$ *is a permutation equivalent of the matrix*

$$\Phi(\mathcal{G}_k^{\alpha,\theta}) = \begin{bmatrix} G_0 & G_1 & \ldots & G_\theta \end{bmatrix}.$$

Proof 4.4.4 *The matrices* $\Phi(\mathcal{S}_k^\alpha)$*,* $\Phi(\sigma_1(\mathcal{S}_k^\alpha))$*, ...,* $\Phi(\sigma_\theta(\mathcal{S}_k^\alpha))$ *have the same dimension. Then, the matrix* $\Phi(\mathcal{G}_k^{\alpha,\theta})$ *is a direct result of Theorem 4.4.1.*

Corollary 4.4.5 *Let* $\mathcal{M}_{k,t}^{\alpha,\theta} = (1-u_1-\ldots-u_\theta)\mathcal{M}_k^\alpha \oplus (u_1)\eta_1(\mathcal{M}_k^\alpha) \oplus \ldots \oplus (u_\theta)\eta_\theta(\mathcal{M}_k^\alpha)$ *be a linear MacDonald code of type* α *of length* n *over* $\mathcal{R}_{p^s,\theta}$*, where* $\mathcal{M}_k^\alpha$ *and* $\eta_i(\mathcal{M}_k^\alpha)$*, for* $1 \leq i \leq \theta$ *are* $[n;k;d_i]$*-linear code over* $\mathbb{F}_{p^s}$*. Then* $\Phi(\mathcal{M}_{k,t}^{\alpha,\theta}) = \mathcal{M}_k^\alpha \otimes \eta_1(\mathcal{M}_k^\alpha) \otimes \ldots \otimes \eta_\theta(\mathcal{M}_k^\alpha)$ *is* $\left[(\theta+1)n; k; d = \sum_{i=0}^{\theta} d_i\right]$*-linear MacDonald code of type* α *over* $\mathbb{F}_{p^s}$*.*

Proof 4.4.6 *The same proof as in Theorem 4.4.1.*

Corollary 4.4.7 *If $\mathcal{G}_0, \mathcal{G}_1, \ldots, \mathcal{G}_\theta$ are generator matrices of $\Phi(\mathcal{M}_{k,t}^{\alpha})$, $\Phi(\eta_1(\mathcal{M}_{k,t}^{\alpha}))$, ..., $\Phi(\eta_\theta(\mathcal{M}_{k,t}^{\alpha}))$ respectively, then the generator matrix of $\Phi(\mathcal{S}_k^{\alpha,\theta})$ is a permutation equivalent of the matrix*

$$\mathcal{G}_{k,t}^{\alpha,\theta} = \left[\begin{array}{cccc} \mathcal{G}_0 & \mathcal{G}_1 & \ldots & \mathcal{G}_\theta \end{array} \right].$$

Proof 4.4.8 *The same proof as in Corollary 4.4.3.*

■

4.5 Covering Radius of linear simplex and MacDonald codes

We can also calculate the covering radius of simplex and MacDonald linear codes of type α over $\mathcal{R}_{p^s,\theta}$, [67], [71], [40].

Theorem 4.5.1 *The covering radii of linear simplex and MacDonal codes $\mathcal{S}_k^{\alpha,\theta}$ and $\mathcal{M}_{k,t}^{\alpha,\theta}$ are given*

1. $r_{hom}(\mathcal{S}_k^{\alpha,\theta}) \geq (\theta+1)p^{sk}$
2. $r_{hom}(\mathcal{M}_{k,t}^{\alpha,\theta}) \geq (\theta+1)\left[p^{(\theta+1)sk} - p^{(\theta+1)st}\right], \quad for \;\; t < r \leq k.$

Proof 4.5.2 *Let, $\mathcal{S}_k^{\alpha,\theta} = (1-u_1-\ldots-u_\theta)\mathcal{S}_k^{\alpha} \oplus (u_1)\sigma_1(\mathcal{S}_k^{\alpha}) \oplus \ldots \oplus (u_\theta)\sigma_\theta(\mathcal{S}_k^{\alpha})$. By Equation (2.16), we have*

$$r_{hom}(\mathcal{S}_k^{\alpha,\theta}) \geq r_{hom}((1-u_1-\ldots-u_\theta)\mathcal{S}_k^{\alpha}) + r_{hom}((u_1)\sigma_1(\mathcal{S}_k^{\alpha})) + \ldots + r_{hom}((u_\theta)\sigma_\theta(\mathcal{S}_k^{\alpha})),$$

then

$$r_{hom}(\mathcal{S}_k^{\alpha,\theta}) \geq r_{hom}(\mathcal{S}_k^{\alpha}) + r_{hom}(\sigma_1(\mathcal{S}_k^{\alpha})) + \ldots + r_{hom}(\sigma_\theta(\mathcal{S}_k^{\alpha})). \tag{4.9}$$

According to Equation (4.9), we get

$$r_{hom}(\mathcal{S}_k^{\alpha,\theta}) \geq (\theta+1) r_{hom}(\mathcal{S}_k^{\alpha}).$$

Combining Equations (2.14) and (2.17), we have

$$r_{hom}(\mathcal{S}_k^{\alpha}) = (p^s - 1)\left[p^{s(k-1)} + p^{s(k-2)} + \ldots + p^{s.1}\right] + p^s,$$

so

$$r_{hom}(\mathcal{S}_k^{\alpha}) = p^s\left[p^{s(k-1)} - 1\right] + p^s. \tag{4.10}$$

Equation (4.10), leads us towards the following important result

$$r_{hom}(\mathcal{S}_k^{\alpha,\theta}) \geq (\theta+1)p^{sk}.$$

The proof for second part are obtained using a similar approach.

■

Theorem 4.5.3 *The covering radii of linear Gray images of simplex and MacDonald codes* $\Phi(\mathcal{S}_k^{\alpha,\theta})$ *and* $\Phi(\mathcal{M}_{k,t}^{\alpha,\theta})$ *are*

[1] $r_{hom}(\Phi(\mathcal{S}_k^{\alpha,\theta})) = (\theta+1)p^{sk}$

[2] $r_{hom}(\Phi(\mathcal{M}_{k,t}^{\alpha,\theta})) \geq (\theta+1)\left[p^{(\theta+1)sk-1} - p^{(\theta+1)st-1}\right], \quad for \;\; t < r \leq k.$

Proof 4.5.4 *Let* $\Phi(\mathcal{S}_k^{\alpha,\theta}) = \mathcal{S}_k^{\alpha}\sigma_1(\mathcal{S}_k^{\alpha})\ldots\sigma_\theta(\mathcal{S}_k^{\alpha})$ *by Equation (2.15), we have*

$$r_{hom}(\Phi(\mathcal{S}_k^{\alpha,\theta})) = r_{hom}(\mathcal{S}_k^{\alpha}) + r_{hom}(\sigma_1(\mathcal{S}_k^{\alpha})) + \ldots + r_{hom}(\sigma_\theta(\mathcal{S}_k^{\alpha})),$$

Similar arguments using proof of Theorem 4.5.1, give that

$$r_{hom}(\Phi(\mathcal{S}_k^{\alpha,\theta})) = (\theta+1)p^{sk}$$

For the second part, By Equations (2.15) and (2.17), we obtain that

$$r_{hom}(\Phi(\mathcal{M}_{k,t}^{\alpha,\theta})) \geq (\theta+1)\left[p^{(\theta+1)sk-1} - p^{(\theta+1)st-1}\right], \quad for \;\; t < r \leq k.$$

■

4.6 Examples

Based on [21] and [23], we will exhibit example of linear simplex and MacDonald codes of type α over the rings $\mathcal{R}_{7,2} = \mathbb{F}_7 + u_1\mathbb{F}_7 + u_2\mathbb{F}_7$ and $\mathcal{R}_{3,2} = \mathbb{F}_3 + u_1\mathbb{F}_3 + u_2\mathbb{F}_3$, and their Gray images.

$\mathcal{S}_k^{\alpha,\theta}(n)$	k	d_{hom}	$r_{hom}(\mathcal{S}_k^{\alpha,\theta})$
343	1	2052	≥ 21
117649	2	$7^3 \times 2052$	≥ 147
40353607	3	$7^6 \times 2052$	≥ 1029
13841287201	4	$7^9 \times 2052$	≥ 7203

Table 4.1: Simplex codes of type α over $\mathcal{R}_{7,2}$, with $\eta = \frac{1296}{217}$.

$\Phi(\mathcal{S}_k^{\alpha,\theta}) = [n,k]$	d_{Ham}	$r_{Ham}(\Phi(\mathcal{S}_k^{\alpha,\theta}))$
$[1029, 1]$	882	21
$[352947, 2]$	$7^3 \times 882$	147
$[121060821, 3]$	$7^6 \times 882$	1029
$[41523861603, 4]$	$7^9 \times 882$	7203

Table 4.2: Gray images of Simplex codes of type α over $\mathcal{R}_{7,2}$.

$\mathcal{M}_{k,t}^{\alpha,\theta}(n)$	k	d_{hom}	$r_{hom}(\mathcal{M}_{k,t}^{\alpha,\theta})$
18954	3	26×3^5	26×3^6
530712	4	728×3^5	728×3^6
14348178	5	19682×3^5	19682×3^6
387419760	6	531440×3^5	531440×3^6

Table 4.3: MacDonald codes of type α over $\mathcal{R}_{3,2}$, with $\eta = \frac{1296}{217}$ and $t = 2$.

$\Phi(\mathcal{M}_{k,t}^{\alpha,\theta}) = [n,k]$	d_{ham}	$r_{hom}(\Phi(\mathcal{M}_{k,t}^{\alpha,\theta}))$
$[56862, 3]$	54	162
$[1592136, 4]$	216	648
$[430443534, 5]$	702	2106
$[1162259280, 6]$	2160	6480

Table 4.4: Gray images of MacDonald codes of type α over $\mathcal{R}_{3,2}$.

4.7 Simplex and MacDonald LCD Codes over $\mathcal{R}_{p^s,\theta}$

A linear code C is an LCD code over $\mathcal{R}_{p^s,\theta} = \mathbb{F}_{p^s} + u_1\mathbb{F}_{p^s} + \ldots + u_\theta\mathbb{F}_{p^s}$ if satisfy $C \cap C^\perp = \{0\}$. According to [3,4,6,17,29,30,44], in the following theorem, we determine the characteristics for a linear code to be an LCD code over $\mathcal{R}_{p^s,\theta}$.

Theorem 4.7.1 *Simplex and MacDonald LCD codes $\mathcal{S}_k^{\alpha,\theta}$ and $\mathcal{M}_{k,t}^{\alpha,\theta}$ satisfies*

1. *$\mathcal{S}_k^{\alpha,\theta} = (1 - u_1 - \ldots - u_\theta)\mathcal{S}_k^\alpha \oplus (u_1)\sigma_1(\mathcal{S}_k^\alpha) \oplus \ldots \oplus (u_\theta)\sigma_\theta(\mathcal{S}_k^\alpha)$ is an LCD code over $\mathcal{R}_{p^s,\theta}$ if and only if $\mathcal{S}_k^\alpha, \sigma_1(\mathcal{S}_k^\alpha), \ldots, \sigma_\theta(\mathcal{S}_k^\alpha)$ are LCD codes over $\mathbb{F}_{p^s}$.*

2. *$\mathcal{M}_{k,t}^{\alpha,\theta} = (1 - u_1 - \ldots - u_\theta)\mathcal{M}_k^\alpha \oplus (u_1)\eta_1(\mathcal{M}_k^\alpha) \oplus \ldots \oplus (u_\theta)\eta_\theta(\mathcal{M}_k^\alpha)$ is an LCD code over $\mathcal{R}_{p^s,\theta}$ if and only if $\mathcal{M}_k^\alpha, \eta_1(\mathcal{M}_k^\alpha), \ldots, \eta_\theta(\mathcal{M}_k^\alpha)$ are LCD codes over $\mathbb{F}_{p^s}$.*

Proof 4.7.2 *By [Theorem 3.3, [47], Let $C = (1 - u - v)C_1 \oplus uC_2 \oplus vC_3$ be a linear code of length n over R. Then $C^\perp = (1 - u - v)C_1^\perp \oplus uC_2^\perp \oplus vC_3^\perp$].*

So

if

$$\mathcal{S}_k^{\alpha,\theta} = (1 - u_1 - \ldots - u_\theta)\mathcal{S}_k^\alpha \oplus (u_1)\sigma_1(\mathcal{S}_k^\alpha) \oplus \ldots \oplus (u_\theta)\sigma_\theta(\mathcal{S}_k^\alpha),$$

then

$$(\mathcal{S}_k^{\alpha,\theta})^\perp = (1 - u_1 - \ldots - u_\theta)(\mathcal{S}_k^\alpha)^\perp \oplus (u_1)(\sigma_1(\mathcal{S}_k^\alpha))^\perp \oplus \ldots \oplus (u_\theta)(\sigma_\theta(\mathcal{S}_k^\alpha))^\perp.$$

Let $\mathcal{S}_k^{\alpha,\theta}$ is an LCD code over $\mathcal{R}_{p^s,\theta}$ then the intersection of

$$\begin{aligned}\mathcal{S}_k^{\alpha,\theta} \cap (\mathcal{S}_k^{\alpha,\theta})^{\perp} = \{0\} \quad &\Leftrightarrow \quad (1-u_1-\ldots-u_\theta)(\mathcal{S}_k^{\alpha} \cap (\mathcal{S}_k^{\alpha})^{\perp}) \\ &\oplus(u_1)(\sigma_1(\mathcal{S}_k^{\alpha}) \cap (\sigma_1(\mathcal{S}_k^{\alpha}))^{\perp}) \oplus \ldots \oplus \\ &(u_\theta)(\sigma_\theta(\mathcal{S}_k^{\alpha}) \cap (\sigma_\theta(\mathcal{S}_k^{\alpha}))^{\perp}) = \{0\} \\ \Leftrightarrow \quad &(\mathcal{S}_k^{\alpha} \cap (\mathcal{S}_k^{\alpha})^{\perp}) = \{0\}, (\sigma_1(\mathcal{S}_k^{\alpha}) \cap (\sigma_1(\mathcal{S}_k^{\alpha}))^{\perp}) = \{0\}, \ldots, \\ &(\sigma_\theta(\mathcal{S}_k^{\alpha}) \cap (\sigma_\theta(\mathcal{S}_k^{\alpha}))^{\perp}) = \{0\}.\end{aligned}$$

So that $\mathcal{S}_k^{\alpha}, \sigma_1(\mathcal{S}_k^{\alpha}), \ldots, \sigma_\theta(\mathcal{S}_k^{\alpha})$ are LCD codes over $\mathbb{F}_{p^s}$. The same for the second part.

■

Theorem 4.7.3 *If $\mathcal{S}_k^{\alpha,\theta}$ and $\mathcal{M}_{k,t}^{\alpha,\theta}$ are LCD codes over $\mathcal{R}_{p^s,\theta}$ then $\Phi(\mathcal{S}_k^{\alpha,\theta})$ and $\Phi(\mathcal{M}_{k,t}^{\alpha,\theta})$ are LCD codes over $\mathbb{F}_{p^s}$.*

Proof 4.7.4 *According to the definition of $\Phi(\mathcal{S}_k^{\alpha,\theta})$, we have*

$$\Phi(\mathcal{S}_k^{\alpha,\theta}) \cap \Phi(\mathcal{S}_k^{\alpha,\theta})^{\perp} = \Phi(\mathcal{S}_k^{\alpha,\theta} \cap (\mathcal{S}_k^{\alpha,\theta})^{\perp}) \tag{4.11}$$

but

$$\begin{aligned}\Phi(\mathcal{S}_k^{\alpha,\theta} \cap (\mathcal{S}_k^{\alpha,\theta})^{\perp}) &= \Phi(((1-u_1-\ldots-u_\theta)\mathcal{S}_k^{\alpha} \oplus (u_1)\sigma_1(\mathcal{S}_k^{\alpha}) \oplus \ldots \\ &\quad \oplus(u_\theta)\sigma_\theta(\mathcal{S}_k^{\alpha})) \cap ((1-u_1-\ldots-u_\theta)(\mathcal{S}_k^{\alpha})^{\perp} \\ &\quad \oplus(u_1)(\sigma_1(\mathcal{S}_k^{\alpha}))^{\perp} \oplus \ldots \oplus (u_\theta)(\sigma_\theta(\mathcal{S}_k^{\alpha})))^{\perp}) \\ &= \Phi((1-u_1-\ldots-u_\theta)(\mathcal{S}_k^{\alpha} \cap (\mathcal{S}_k^{\alpha})^{\perp}) \\ &\quad \oplus(u_1)(\sigma_1(\mathcal{S}_k^{\alpha}) \cap (\sigma_1(\mathcal{S}_k^{\alpha}))^{\perp}) \oplus \ldots \\ &\quad \oplus(u_\theta)(\sigma_\theta(\mathcal{S}_k^{\alpha}) \cap (\sigma_\theta(\mathcal{S}_k^{\alpha}))^{\perp}) \\ &= (\mathcal{S}_k^{\alpha} \cap (\mathcal{S}_k^{\alpha})^{\perp})(\sigma_1(\mathcal{S}_k^{\alpha}) \cap (\sigma_1(\mathcal{S}_k^{\alpha}))^{\perp}) \\ &\quad \ldots(\sigma_\theta(\mathcal{S}_k^{\alpha}) \cap (\sigma_\theta(\mathcal{S}_k^{\alpha}))^{\perp})\end{aligned}$$

According to Theorem 4.7.1 and Equation (4.11), we have $\Phi(\mathcal{S}_k^{\alpha,\theta}) \cap \Phi(\mathcal{S}_k^{\alpha,\theta})^{\perp} = 0$. The same for the code $\Phi(\mathcal{M}_{k,t}^{\alpha,\theta})$.

■

4.8 Conclusion

This chapter presents a new method for constructing simplex and MacDonald codes over $\mathcal{R}_{p^s,\theta} = \mathbb{F}_{p^s} + u_1\mathbb{F}_{p^s} + \ldots + u_\theta\mathbb{F}_{p^s}$. The advantage of this construction lies in its simplicity for defining Gray images and LCD codes over this ring. Additionally, we acknowledge the significance of the study on homogeneous weight, which has played a crucial role in defining the covering radius.

Chapter 5

MULTI-SECRET SHARING SCHEMES ON SIMPLEX AND MacDonald LINEAR CODES OVER $\mathfrak{R}$

Secret-sharing schemes are a crucial concept in cryptography, designed to safeguard high-value data [8]. Numerous research efforts have focused on developing linear codes over finite rings to achieve perfect secret sharing. Based on the definitions provided in [21–23, 26, 48], simplex and MacDonald codes can be defined over the product of three finite commutative rings, $\mathfrak{R} = \mathcal{R}_1\mathcal{R}_2\mathcal{R}_2$, with $\mathcal{R}_1 = \mathbb{Z}_q + v_1\mathbb{Z}_q, v_1^2 = 1$ is commutative ring and $\mathcal{R}_2 = \mathbb{Z}_q + v_1\mathbb{Z}_q + v_2\mathbb{Z}_q, \mathcal{R}_3 = \mathbb{Z}_q + v_1\mathbb{Z}_q + v_2\mathbb{Z}_q + v_3\mathbb{Z}_q$ are two other commutatives rings with $v_i^2 = 0$, for $2 \leq i \leq 3$. For this purpose, let us introduce some definitions that will be helpful later on [27, 28, 59, 65, 68].

5.1 Gray map and Gray images of linear codes over $\mathfrak{R}$

In this section, we introduce the Gray Map and Gray Images of linear codes over the ring $\mathfrak{R}$ to $\mathbb{Z}_q^9$. Let's commence with the definitions of

$$\begin{array}{rcccl} \phi_1 & : & \mathcal{R}_1 & \to & \mathbb{Z}_q^2 \\ & & x & \mapsto & \phi_1(x) = (x_1, x_2), \end{array} \tag{5.1}$$

$$\begin{array}{rcccl} \phi_2 & : & \mathcal{R}_2 & \to & \mathbb{Z}_q^3 \\ & & y & \mapsto & \phi_2(y) = (y_1, y_2, y_3), \end{array} \tag{5.2}$$

and

$$\begin{array}{rcccl} \phi_3 & : & \mathcal{R}_3 & \to & \mathbb{Z}_q^4 \\ & & z & \mapsto & \phi_3(z) = (z_1, z_2, z_3, z_4). \end{array} \tag{5.3}$$

By this maps Gray map Ψ, is defined by

$$\begin{array}{rcccl} \Psi & : & \mathcal{R}_1\mathcal{R}_2\mathcal{R}_3 & \to & \mathbb{Z}_q^9 \\ & & c = (x, y, z) & \mapsto & \Psi(c) = \Psi(\phi_1(x), \phi_2(y), \phi_3(z)), \end{array} \tag{5.4}$$

where $\Psi(c) = (x_1, x_2, y_1, y_2, y_3, z_1, z_2, z_3, z_4)$.

It is easy to see that this map can be extended from $\mathfrak{R}^n$ to $\mathbb{Z}_q^{9n}$. Therefore, the following theorem holds.

Theorem 5.1.1 *If C is a linear code over $\mathfrak{R}$ of length n, then $\Phi(C)$ is a linear code with parameters $[9n, k, d_H]$.*

5.2 MacDonald and simplex codes over $\mathfrak{R}$

Theorem 5.2.1 *Let $m^{\alpha}_{k,\mathcal{R}_1}$, $G^{\alpha}_{k,\mathcal{R}_2}$ and $\mathcal{G}^{\alpha}_{k,\mathcal{R}_3}$ be the generator matrices of length q^{2k}, q^{3k} and q^{4k} of linear α-simplex codes over $\mathcal{R}_1, \mathcal{R}_2$ and $\mathcal{R}_3$ respectively. Then, the generator matrix $\Theta^{\alpha}_{k,\mathfrak{R}}$ of linear α-simplex codes over $\mathfrak{R}$ of length $n = 3q^{9k}$, as follows*

$$\Theta^{\alpha}_{k,\mathfrak{R}} = \left[\overbrace{m^{\alpha}_{k,\mathcal{R}_1}}^{q^{9k}} \quad \overbrace{G^{\alpha}_{k,\mathcal{R}_2}}^{q^{9k}} \quad \overbrace{\mathcal{G}^{\alpha}_{k,\mathcal{R}_3}}^{q^{9k}} \right]. \tag{5.5}$$

Proof 5.2.2 *Construct the generator matrix $\Theta^{\alpha}_{k,\mathfrak{R}}$ of linear α-simplex codes over $\mathfrak{R}$, from the concatination of q^{7k} copies of the generator matrix $m^{\alpha}_{k,\mathcal{R}_1}$, q^{6k} copies of the generator matrix $G^{\alpha}_{k,\mathcal{R}_2}$ and q^{5k} copies of the generator matrix $\mathcal{G}^{\alpha}_{k,\mathcal{R}_3}$ given by*

$$\Theta^{\alpha}_{k,\mathfrak{R}} = \left[\overbrace{m^{\alpha}_{k,\mathcal{R}_1}}^{q^{2k}q^{7k}} \ \overbrace{G^{\alpha}_{k,\mathcal{R}_2}}^{q^{3k}q^{6k}} \ \overbrace{\mathcal{G}^{\alpha}_{k,\mathcal{R}_3}}^{q^{4k}q^{5k}} \right]. \tag{5.6}$$

■

We also, the $\alpha - MacDonald$ linear codes over $\mathfrak{R} = \mathcal{R}_1\mathcal{R}_2\mathcal{R}_2$ are given by the following theorem.

Corollary 5.2.3 *Let $m^{\alpha}_{k,u,\mathcal{R}_1}$, $G^{\alpha}_{k,u,\mathcal{R}_2}$ and $\mathcal{G}^{\alpha}_{k,u,\mathcal{R}_3}$ be the generator matrices of length $(q^{2k} - q^{2u})$, $(q^{3k} - q^{3u})$ and $(q^{4k} - q^{4u})$ of linear α-MacDonald codes over $\mathcal{R}_1, \mathcal{R}_2$ and $\mathcal{R}_3$ respectively.Then, the generator matrix $\Theta^{\alpha}_{\mathfrak{R},k,u}$ of α-MacDonald codes over $\mathfrak{R}$, as follows,*

$$\Theta^{\alpha}_{k,u,\mathfrak{R}} = \left[\overbrace{m^{\alpha}_{k,u,\mathcal{R}_1}}^{q^{9k}-q^{9u}} \ \overbrace{G^{\alpha}_{k,u,\mathcal{R}_2}}^{q^{9k}-q^{9u}} \ \overbrace{\mathcal{G}^{\alpha}_{k,u,\mathcal{R}_3}}^{q^{9k}-q^{9u}} \right]. \tag{5.7}$$

The generator matrix $\Theta^{\alpha}_{\mathfrak{R},k,u}$ of α-MacDonald codes over $\mathfrak{R}$ of length $n = 3[q^{9k} - q^{9u}]$.

Proof 5.2.4 *Same proof as Theorem 5.2.1.*

■

5.3 Gray images of linear α-simplex and α-MacDonald codes

According to Theorem 5.2.1 , if Φ is Gray map with the Lee weight minimal d_{Lee}, we have the following results .

Theorem 5.3.1 *The code $\Phi(S^{\alpha}_{k})$ is equivalent to $3q^{9k}$ copies of the simplex codes over $\mathbb{Z}_q$.*

Proof 5.3.2 *The code $\Phi(S^{\alpha}_{k})$ is equivalent to $3q^{9k}$ copies of the simplex code $[\Phi(S^{\alpha}_{k,\mathcal{R}_1}) \mid \Phi(S^{\alpha}_{k,\mathcal{R}_2}) \mid \Phi(S^{\alpha}_{k,\mathcal{R}_3})]$ with $\Phi(S^{\alpha}_{k,\mathcal{R}_1})$ is the $q^{2k}q^{7k}$ copies of the $S^{\alpha}_{k,\mathbb{Z}_q}$ simplex code over $\mathbb{Z}_q$, $\Phi(S^{\alpha}_{k,\mathcal{R}_2})$ is the $q^{3k}q^{6k}$ copies of the $S^{\alpha}_{k,\mathbb{Z}_q}$ simplex code over $\mathbb{Z}_q$, and $\Phi(S^{\alpha}_{k,\mathcal{R}_3})$ is the $q^{4k}q^{5k}$ copies of the $S^{\alpha}_{k,\mathbb{Z}_q}$ simplex code over $\mathbb{Z}_q$. Then we have the result.*

■

Proposition 5.3.3 *The generator matrix* $\Phi(\Theta^{\alpha}_{k,\mathfrak{R}})$ *is a permutation equivalent of the matrix*

$$\Phi(\Theta^{\alpha}_{k,\mathfrak{R}}) = \left[\overbrace{G^{\alpha}_{k,\mathbb{Z}_q} G^{\alpha}_{k,\mathbb{Z}_q} \dots G^{\alpha}_{k,\mathbb{Z}_q}}^{3^3 q^{9k}}\right], \tag{5.8}$$

with $G^{\alpha}_{k,\mathbb{Z}_q}$ *is a generator matrix of* $S^{\alpha}_{k,\mathbb{Z}_q}$*, simplex codes over* $\mathbb{Z}_q$*.*

Similarly, we can define α-MacDonald codes and their corresponding generator matrix.

Proposition 5.3.4 *The generator matrix of* $\Phi(\Theta^{\alpha}_{k,u,\mathfrak{R}})$*, for* $1 \leq u \leq k-1$ *is a permutation equivalent of the matrix*

$$\Phi(\Theta^{\alpha}_{k,u,\mathfrak{R}}) = \left[\overbrace{M^{\alpha}_{k,u,\mathbb{Z}_q} M^{\alpha}_{k,u,\mathbb{Z}_q} \cdots M^{\alpha}_{k,u,\mathbb{Z}_q}}^{\frac{3[q^{9k}-q^{9u}]}{q^k-q^u}}\right], \tag{5.9}$$

with $M^{\alpha}_{k,u,\mathbb{Z}_q}$ *is a generator matrix of* $\mathcal{M}^{\alpha}_{k,u,\mathbb{Z}_q}$*,* α*-MacDonald codes over* $\mathbb{Z}_q$*.*

5.4 Multi-secret sharing schemes on linear codes

Minimal linear codes belong to a subclass of codes utilized in secret-sharing systems and multi-secret-sharing schemes. In our work, we employ multi-secret sharing by utilizing the Gray images of α-MacDonald codes over $\mathfrak{R} = \mathcal{R}_1\mathcal{R}_2\mathcal{R}_3$ due to their minimal properties. According to [2, 24, 78, 82], we construct the Mutli-secret sharing schemes based on linear codes. We need an α-MacDonald code over $\mathbb{Z}_q$ with generator matrix $\Phi(\Theta^{\alpha}_{k,\mathfrak{R}})$ and using the Theorem 6 [82] and [19]. Let a codewords be the secret $S = (s_1, s_2, \dots, s_n)$ in $\mathbb{Z}_q^n$ is the secret space. The minimal access elements of a generator matrix $\Phi(\Theta^{\alpha}_{k,\mathfrak{R}})$ are the rows$\{g_1, g_2 \dots, g_n\}$, and all of the elements $\Phi(\Theta^{\alpha}_{k,\mathfrak{R}})$ are participants in this scheme. The calculates of the dealer share t is given by

$$t = \langle c, S\rangle = c.S^{\top}. \tag{5.10}$$

Where S is the dealer, $S^\top$ denotes transposition of S and c is the codeword. The following system defines the private secret S and the coalition corresponding to the rows of $\Phi(\Theta^\alpha_{k,\mathfrak{R}})$.

$$T^\top = \Phi(\Theta^\alpha_{k,\mathfrak{R}}).S^\top, \tag{5.11}$$

where $T = (t_1, t_2, \ldots, t_k)$, and t_i is the share attached to the row i of $\Phi(\Theta^\alpha_{k,\mathfrak{R}})$. The secret then be obtained by solving the n equations and n unknowns by following linear system.

$$\begin{cases} T^\top &= \Phi(\Theta^\alpha_{k,\mathfrak{R}}).S^\top \\ 0 &= H(\Theta^\alpha_{k,u,\mathfrak{R}}).S^\top. \end{cases} \tag{5.12}$$

And using Theorem 6 in [82],

$$rank(\Phi(\Theta^\alpha_{k,\mathfrak{R}})) = rank(\Phi(\Theta^\alpha_{k,u,\mathfrak{R}})^\top \Phi(\Theta^\alpha_{k,u,\mathfrak{R}})) \Leftrightarrow C \text{ } LCD \text{ } codes. \tag{5.13}$$

Example 5.4.1 *We consider* $\mathfrak{R} = (\mathbb{Z}_5 + v_1\mathbb{Z}_5)(\mathbb{Z}_5 + v_1\mathbb{Z}_5 + v_2\mathbb{Z}_5)(\mathbb{Z}_5 + v_1\mathbb{Z}_5 + v_2\mathbb{Z}_5 + v_3\mathbb{Z}_5)$. *For* $k = 2$, $u = 1$, *a generator matrix of Gray images of* α*-MacDonald code is,*

$$\Phi(\Theta^\alpha_{2,1,\mathfrak{R}}) = \overbrace{\begin{bmatrix} 1000011112222233333444444 \\ 0123412340123401234012340 \end{bmatrix}}^{5^8\times 1464843} = \overbrace{\begin{bmatrix} g_1 \\ g_2 \end{bmatrix}}^{5^8\times 1464843},$$

and

$$rank(\Phi(\Theta^\alpha_{2,1,\mathfrak{R}})) = rank(\Phi(\Theta^\alpha_{2,1,\mathfrak{R}})^\top \Phi(\Theta^\alpha_{2,1,\mathfrak{R}})) = 2.$$

The parity-check matrix $H(\Theta^\alpha_{2,1,\mathfrak{R}})$ *of this code is,*

$$H(\Theta^\alpha_{2,1,\mathfrak{R}}) = \overbrace{\begin{bmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&3 \\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2 \\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1 \\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&4&4 \\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&4&3 \\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&4&2 \\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&4&1 \\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&3&0 \\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&3&4 \\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&3&3 \\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&3&2 \\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&3&1 \\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&2&0 \\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&2&1 \\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&2&3 \\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&2&2 \\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&2&1 \\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0 \\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&1&1 \\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&3 \\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&2 \\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1
\end{bmatrix}}^{5^8\times 1464843} = \overbrace{\begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \\ y_8 \\ y_9 \\ y_{10} \\ y_{11} \\ y_{12} \\ y_{13} \\ y_{14} \\ y_{15} \\ y_{16} \\ y_{17} \\ y_{18} \\ y_{19} \\ y_{20} \\ y_{21} \\ y_{22} \end{bmatrix}}^{5^8\times 1464843}.$$

There are 25 *codewords of* $\Phi\left(\mathcal{M}_{2,1}^{\alpha}\right)$. *These codewords are*

$$(\overbrace{00000000000000000000000}^{5^8\times 1464843}), (\overbrace{10000111122222333344444}^{5^8\times 1464843}),$$
$$(\overbrace{01234123401234012340123}^{5^8\times 1464843}), (\overbrace{02413241302413024130241}^{5^8\times 1464843}),$$
$$(\overbrace{03142314203142031420314}^{5^8\times 1464843}), (\overbrace{04321432104321043210432}^{5^8\times 1464843}),$$
$$(\overbrace{11234234023401340124012}^{5^8\times 1464843}), (\overbrace{12413302424130302414130}^{5^8\times 1464843}),$$
$$(\overbrace{13142420320314314204203}^{5^8\times 1464843}), (\overbrace{14321043221043321044321}^{5^8\times 1464843}),$$
$$(\overbrace{20000222244444111133333}^{5^8\times 1464843}), (\overbrace{21234340140123123403401}^{5^8\times 1464843}),$$
$$(\overbrace{22413413041302130243024}^{5^8\times 1464843}), (\overbrace{23142031442031142033142}^{5^8\times 1464843}),$$
$$(\overbrace{24321104343210104323210}^{5^8\times 1464843}), (\overbrace{30000333311111444422222}^{5^8\times 1464843}),$$
$$(\overbrace{31234401212340401232340}^{5^8\times 1464843}), (\overbrace{32413024113024413022413}^{5^8\times 1464843}),$$
$$(\overbrace{33142142014203420312031}^{5^8\times 1464843}), (\overbrace{34321210410432432102104}^{5^8\times 1464843}),$$
$$(\overbrace{40000444433333222211111}^{5^8\times 1464843}), (\overbrace{41234012334012234011234}^{5^8\times 1464843}),$$
$$(\overbrace{42413130230241241301302}^{5^8\times 1464843}), (\overbrace{43142203131420203141420}^{5^8\times 1464843}),$$
$$(\overbrace{44321321032104210431043}^{5^8\times 1464843}).$$

Now, we examine a Multi secret-sharing scheme based on $\Phi\left(\mathcal{M}_{2,1}^{\alpha}\right)$. *Let the secret vector be* $S = \overbrace{11234234023401340124012}^{5^8\times 1464843}$, *we calculate the shares as follows*

$$t_1^{\top} = g_1 S^{\top} =< (\overbrace{10000111122222333344444}^{5^8\times 1464843}), (\overbrace{11234234023401340124012}^{5^8\times 1464843}) >= 0$$
$$t_2^{\top} = g_2 S^{\top} =< (\overbrace{01234123401234012340123}^{5^8\times 1464843}), (\overbrace{11234234023401340124012}^{5^8\times 1464843}) >= 0.$$

Moreover, $y_i S^{\top} =< y_i, (\overbrace{11234234023401340124012}^{5^8\times 1464843}) >= 0$, *for* $1 \leq i \leq 22$. *Using Equa-*

tion 5.12, we should solve the following linear system to recover the secret.

$$\overbrace{\begin{bmatrix}
1&0&0&0&0&1&1&1&1&2&2&2&2&2&3&3&3&3&3&4&4&4&4&4\\
0&1&2&3&4&1&2&3&4&0&1&2&3&4&0&1&2&3&4&0&1&2&3&4\\
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&3\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&4&4\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&4&3\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&4&2\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&4&1\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&3&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&3&4\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&3&3\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&3&2\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&3&1\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&2&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&2&4\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&2&3\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&2&2\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&2&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&4\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&3\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&2\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1
\end{bmatrix}}^{5^8\times 1464843}
\cdot
\overbrace{\begin{bmatrix}s_1\\s_2\\s_3\\s_4\\s_5\\s_6\\s_7\\s_8\\s_9\\s_{10}\\s_{11}\\s_{12}\\s_{13}\\s_{14}\\s_{15}\\s_{16}\\s_{17}\\s_{18}\\s_{19}\\s_{20}\\s_{21}\\s_{22}\\s_{23}\\s_{24}\end{bmatrix}}^{5^8\times 1464843}
=
\overbrace{\begin{bmatrix}0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\end{bmatrix}}^{5^8\times 1464843}
\tag{5.14}$$

we have, this linear system wich are repeated $5^8 \times 1464843$ *times.*

$$
\begin{array}{l}
\{s_1 \\
\quad s_2 + 2s_3 + 3s_4 + 4s_5 + s_6 + 2s_7 + 3s_8 + 4s_9 \\
\quad\quad s_1 \\
\quad\quad\quad s_2 \\
\quad\quad\quad\quad s_3 \\
\quad\quad\quad\quad\quad s_4 \\
\quad\quad\quad\quad\quad\quad s_5 \\
\quad\quad\quad\quad\quad\quad\quad s_6 \\
\quad\quad\quad\quad\quad\quad\quad\quad s_7 \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad s_8 \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad s_9 \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad s_{10} \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad s_{11} \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad s_{12} \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad s_{13} \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad s_{14} \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad s_{15} \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad s_{16} \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad s_{17} \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad s_{18} \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad s_{19} \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad s_{20} \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad s_{21} \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad s_{22}
\end{array}
\begin{array}{l}
+ s_6 + s_7 + s_8 + s_9 + 2s_{10} + 2s_{12} + 2s_{13} + 2s_{14} + 3s_{15} + 3s_{16} + 2s_{17} + 3s_{18} + 3s_{19} + 4s_{20} + s_{21} + 4s_{22} + 4s_{23} + 4s_{24} = 0 \\
\quad + s_{11} + 2s_{12} + 3s_{13} + 4s_{14} \quad + s_{16} + 2s_{17} + 3s_{18} + 4s_{19} \quad + s_{21} + 2s_{22} + 3s_{23} + 4s_{24} = 0 \\
\quad\quad + 3s_{24} = 0 \\
\quad\quad\quad + 2s_{24} = 0 \\
\quad\quad\quad\quad + s_{24} = 0 \\
\quad\quad\quad\quad\quad + 4s_{23} + 4s_{24} = 0 \\
\quad\quad\quad\quad\quad\quad + 4s_{23} + 3s_{24} = 0 \\
\quad\quad\quad\quad\quad\quad\quad + 4s_{23} + 2s_{24} = 0 \\
\quad\quad\quad\quad\quad\quad\quad\quad + 4s_{23} + s_{24} = 0 \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad + 3s_{23} = 0 \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad + 3s_{23} + 4s_{24} = 0 \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad + 3s_{23} + 3s_{24} = 0 \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad + 3s_{23} + 2s_{24} = 0 \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad + 3s_{23} + s_{24} = 0 \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad + 2s_{23} = 0 \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad + 2s_{23} + 1s_{24} = 0 \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad + 2s_{23} + 3s_{24} = 0 \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad + 2s_{23} + 2s_{24} = 0 \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad + 2s_{23} + s_{24} = 0 \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad + s_{23} = 0 \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad + s_{23} + s_{24} = 0 \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad + s_{23} + s_{24} = 0 \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad + s_{23} + 2s_{24} = 0 \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad s_{22} + s_{23} + s_{24}
\end{array}
$$

Remark 5.4.2 *The code* $\Phi\left(\mathcal{M}_{2,1}^{\alpha}\right)$ *is an LCD code but det* $\begin{bmatrix}\Phi(\Theta_{2,1,\mathfrak{R}}^{\alpha})\\ H(\Theta_{2,1,\mathfrak{R}}^{\alpha})\end{bmatrix} = 0$ *, then this system does not recover the secret.*

Example 5.4.3 *Let* $\mathfrak{R} = (\mathbb{Z}_3 + v_1\mathbb{Z}_3)(\mathbb{Z}_3 + v_1\mathbb{Z}_3 + v_2\mathbb{Z}_3)(\mathbb{Z}_3 + v_1\mathbb{Z}_3 + v_2\mathbb{Z}_3 + v_3\mathbb{Z}_3)$*. For* $k = 3$*, a generator matrix of the code* $\Phi\left(\mathcal{M}_{3,1}^{\alpha}\right)$ *is given by*

$$\Phi(\Theta_{3,1,\mathfrak{R}}^{\alpha}) = \overbrace{\begin{bmatrix} 100000000 & 11111111 & 222222222 \\ 010011222 & 00111222 & 000111222 \\ 001212012 & 12012012 & 012012012 \end{bmatrix}}^{3^9\times 48427561} = \overbrace{\begin{bmatrix} g_1 \\ g_2 \\ g_3 \end{bmatrix}}^{3^9\times 48427561},$$

and

$$rank(\Phi(\Theta_{3,1,\mathfrak{R}}^{\alpha})) = rank(\Phi(\Theta_{3,1,\mathfrak{R}}^{\alpha})^{\top}\Phi(\Theta_{3,1,\mathfrak{R}}^{\alpha})) = 3,$$

the parity-check matrix $H(\Theta_{3,1,\mathfrak{R}}^{\alpha})$ *of this code is*

$$H(\Theta_{3,1,\mathfrak{R}}^{\alpha}) = \overbrace{\begin{bmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&2&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&2\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&2\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&1\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&1\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&2&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&0&1\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&1&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&2&2\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&0&2\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&2&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&2&2\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&2&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&1&0&1&2\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&0&2&2\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&2&0&1&2\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&2&0&2&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1
\end{bmatrix}}^{3^9\times 48427561} = \overbrace{\begin{bmatrix} y_1\\y_2\\y_3\\y_4\\y_5\\y_6\\y_7\\y_8\\y_9\\y_{10}\\y_{11}\\y_{12}\\y_{13}\\y_{14}\\y_{15}\\y_{16}\\y_{17}\\y_{18}\\y_{19}\\y_{21}\\y_{21}\\y_{22}\\y_{23}\end{bmatrix}}^{3^9\times 48427561}, \tag{5.15}$$

there are 27 *codewords of* $\Phi\left(\mathcal{M}_{3,1}^{\alpha}\right)$*. These codewords are*

$$(\overbrace{000000000000000000000000000}^{3^9\times 48427561}),(\overbrace{001212012120120120120120}^{3^9\times 48427561}),$$
$$(\overbrace{002121021210210210210210}^{3^9\times 48427561}),(\overbrace{010011222001112220001112}^{3^9\times 48427561}),$$
$$(\overbrace{011220201121202010121202}^{3^9\times 48427561}),(\overbrace{012102210211022100211022}^{3^9\times 48427561}),$$
$$(\overbrace{020022111002221110002221}^{3^9\times 48427561}),(\overbrace{021201120122011200122011}^{3^9\times 48427561}),$$

$$(\overbrace{022110102212101020212101}^{3^9\times 48427561}),(\overbrace{100000000111111112222222}^{3^9\times 48427561}),$$
$$(\overbrace{101212012201201202012012}^{3^9\times 48427561}),(\overbrace{102121021021021022102102}^{3^9\times 48427561}),$$
$$(\overbrace{110011222112220002220001}^{3^9\times 48427561}),(\overbrace{111220201202010122010121}^{3^9\times 48427561}),$$
$$(\overbrace{112102210022100212100211}^{3^9\times 48427561}),(\overbrace{120022111110002222221110}^{3^9\times 48427561}),$$
$$(\overbrace{121201120200122012011200}^{3^9\times 48427561}),(\overbrace{122110102020212102101021}^{3^9\times 48427561}),$$
$$(\overbrace{200000000222222221111111}^{3^9\times 48427561}),(\overbrace{201212012012012011201201}^{3^9\times 48427561}),$$
$$(\overbrace{202121021102102101021021}^{3^9\times 48427561}),(\overbrace{210011222220001111122200}^{3^9\times 48427561}),$$
$$(\overbrace{212202010111212012020112}^{3^9\times 48427561}),(\overbrace{211220201010121201202012}^{3^9\times 48427561}),$$
$$(\overbrace{212102210100211021022100}^{3^9\times 48427561}),(\overbrace{221201120011200121200122}^{3^9\times 48427561}),$$
$$(\overbrace{222110102101020201020202}^{3^9\times 48427561}).$$

Now, we examine a Multi-secret sharing schemes based on $\Phi\left(\mathcal{M}_{3,1}^{\alpha}\right)$. *Let the secret vector be* $S=(\overbrace{100000000111111112222222}^{3^9\times 48427561})$. *We calculate the shares as follows*

$$t_1^\top =< (\overbrace{10000000011111111222222222}^{3^9\times 48427561}), (\overbrace{10000000011111111222222222}^{3^9\times 48427561}) >= 0$$
$$t_2^\top =< (\overbrace{01001122200111222000111222}^{3^9\times 48427561}), (\overbrace{10000000011111111222222222}^{3^9\times 48427561}) >= 0$$
$$t_3^\top =< (\overbrace{00121201212012012012012012}^{3^9\times 48427561}), (\overbrace{10000000011111111222222222}^{3^9\times 48427561}) >= 0,$$

moreover $y_i S^\top =< y_i, (\overbrace{10000000011111111222222222}^{3^9\times 48427561}) >= 0$, *for* $1 \leq i \leq 23$. *By Equation 5.12, we need solve the following linear system to recover the secret.*

$$\overbrace{\begin{bmatrix}
1&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&2&2&2&2&2&2&2&2&2\\
0&1&0&0&1&1&2&2&2&0&0&1&1&1&2&2&2&0&0&0&1&1&1&2&2&2\\
0&0&1&2&1&2&0&1&2&1&2&0&1&2&0&1&2&0&1&2&0&1&2&0&1&2\\
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&2&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&2\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&2\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&1\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&1\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&2&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&0&1\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&1&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&2&2\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&0&2\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&2&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&2&2\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&2&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&1&2\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&2&2&2\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&0&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&2&0&1&2&2\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&2&0&2&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1
\end{bmatrix}}^{3^9\times 48427561}
\overbrace{\begin{bmatrix}s_1\\s_2\\s_3\\s_4\\s_5\\s_6\\s_7\\s_8\\s_9\\s_{10}\\s_{11}\\s_{12}\\s_{13}\\s_{14}\\s_{15}\\s_{16}\\s_{17}\\s_{18}\\s_{19}\\s_{20}\\s_{21}\\s_{22}\\s_{23}\\s_{24}\\s_{25}\\s_{26}\end{bmatrix}}^{3^9\times 48427561}
=
\overbrace{\begin{bmatrix}0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\end{bmatrix}}^{3^9\times 48427561} \tag{5.16}$$

similarly, the code $\Phi\left(\mathcal{M}_{3,1}^{\alpha}\right)$ *is LCD code but , det* $\begin{bmatrix}\Phi\left(\Theta_{3,1,\mathfrak{R}}^{\alpha}\right)\\ H(\Theta_{3,1,\mathfrak{R}}^{\alpha})\end{bmatrix} = 0$ *then this system does not recover the secret.*

Remark 5.4.4 *According to Examples 5.4.1 and 5.4.3, we can construct subcodes of the codes* $\Phi\left(\Theta_{2,1,\mathfrak{R}}^{\alpha}\right)$ *and* $\Phi\left(\Theta_{3,1,\mathfrak{R}}^{\alpha}\right)$ *by using Definition 1.2.29, witch recover the secret.*

Example 5.4.5 *We consider* $\mathfrak{R} = (\mathbb{Z}_5 + v_1\mathbb{Z}_5)(\mathbb{Z}_5 + v_1\mathbb{Z}_5 + v_2\mathbb{Z}_5)(\mathbb{Z}_5 + v_1\mathbb{Z}_5 + v_2\mathbb{Z}_5 + v_3\mathbb{Z}_5)$. *For* $k = 2$, $u = 1$, *a generator matrix of the subcode of Gray images of* α*-MacDonald code is,*

$$\Phi(C_2) = \overbrace{\begin{bmatrix}11222333444\\12134124123\end{bmatrix}}^{5^8\times 1464843} = \overbrace{\begin{bmatrix}g_1\\g_2\end{bmatrix}}^{5^8\times 1464843},$$

and

$$rank(\Phi(C_2)) = rank(\Phi(C_2)^\top \Phi(C_2)) = rank(\Phi(C_2)\Phi(C_2)^\top) = 2.$$

So the code $\Phi(C_2)$ *is LCD and det* $\begin{bmatrix} \Phi(C_2) \\ H(\Phi(C_2)) \end{bmatrix} \neq 0$. *The parity-check matrix* $H(\Phi(C_2))$ *of this code is,*

$$H(\Phi(C_2)) = \overbrace{\begin{bmatrix} 1&0&0&0&0&0&0&0&0&4&2 \\ 0&1&0&0&0&0&0&0&0&0&1 \\ 0&0&1&0&0&0&0&0&0&2&0 \\ 0&0&0&1&0&0&0&0&0&4&3 \\ 0&0&0&0&1&0&0&0&0&0&2 \\ 0&0&0&0&0&1&0&0&0&0&3 \\ 0&0&0&0&0&0&1&0&0&1&2 \\ 0&0&0&0&0&0&0&1&0&3&0 \\ 0&0&0&0&0&0&0&0&1&3&1 \end{bmatrix}}^{5^8\times 1464843} = \overbrace{\begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \\ y_8 \\ y_9 \end{bmatrix}}^{5^8\times 1464843}.$$

There are 25 *codewords of* $\Phi(C_2)$. *These codewords are*

$$\overbrace{(23301402012)}^{5^8\times 1464843}, \overbrace{(30430021130)}^{5^8\times 1464843}, \overbrace{(42014140203)}^{5^8\times 1464843}, \overbrace{(04143214321)}^{5^8\times 1464843}, \overbrace{(11222333444)}^{5^8\times 1464843},$$
$$\overbrace{(34023230401)}^{5^8\times 1464843}, \overbrace{(41102304024)}^{5^8\times 1464843}, \overbrace{(03231423142)}^{5^8\times 1464843}, \overbrace{(10310042210)}^{5^8\times 1464843}, \overbrace{(22444111333)}^{5^8\times 1464843},$$
$$\overbrace{(40240013340)}^{5^8\times 1464843}, \overbrace{(02324132413)}^{5^8\times 1464843}, \overbrace{(14403201031)}^{5^8\times 1464843}, \overbrace{(21032320104)}^{5^8\times 1464843}, \overbrace{(33111444222)}^{5^8\times 1464843},$$
$$\overbrace{(01412341234)}^{5^8\times 1464843}, \overbrace{(13041410302)}^{5^8\times 1464843}, \overbrace{(20120034420)}^{5^8\times 1464843}, \overbrace{(32204103043)}^{5^8\times 1464843}, \overbrace{(44333222111)}^{5^8\times 1464843},$$
$$\overbrace{(12134124123)}^{5^8\times 1464843}, \overbrace{(24213243241)}^{5^8\times 1464843}, \overbrace{(31342312314)}^{5^8\times 1464843}, \overbrace{(43421431432)}^{5^8\times 1464843}, \overbrace{(00000000000)}^{5^8\times 1464843},$$

Now, we examine a Multi secret-sharing scheme based on $\Phi(C_2)$. *Let the secret vector be* $S = \overbrace{24213243241}^{5^8\times 1464843}$, *we calculate the shares as follows*

$$t_1^\top = g_1 S^\top =< \overbrace{(11222333444)}^{5^8\times 1464843}, \overbrace{(24213243241)}^{5^8\times 1464843} >= 3$$
$$t_2^\top = g_2 S^\top =< \overbrace{(12134124123)}^{5^8\times 1464843}, \overbrace{(24213243241)}^{5^8\times 1464843} >= 2.$$

Moreover, $y_i S^\top =< y_i, \overbrace{(24213243241)}^{5^8\times 1464843} >= 0$, *for* $1 \leq i \leq 9$. *Using Equation 5.12, we should*

solve the following linear system to recover the secret.

$$\overbrace{\begin{bmatrix} 1&1&2&2&2&3&3&3&4&4&4\\ 1&2&1&3&4&1&2&4&1&2&3\\ 1&0&0&0&0&0&0&0&0&4&2\\ 0&1&0&0&0&0&0&0&0&0&1\\ 0&0&1&0&0&0&0&0&0&2&0\\ 0&0&0&1&0&0&0&0&0&4&3\\ 0&0&0&0&1&0&0&0&0&0&2\\ 0&0&0&0&0&1&0&0&0&0&3\\ 0&0&0&0&0&0&1&0&0&1&2\\ 0&0&0&0&0&0&0&1&0&3&0\\ 0&0&0&0&0&0&0&0&1&3&1 \end{bmatrix}}^{5^8\times 1464843} \cdot \overbrace{\begin{bmatrix} s_1\\ s_2\\ s_3\\ s_4\\ s_5\\ s_6\\ s_7\\ s_8\\ s_9\\ s_{10}\\ s_{11} \end{bmatrix}}^{5^8\times 1464843} = \overbrace{\begin{bmatrix} 3\\ 2\\ 0\\ 0\\ 0\\ 0\\ 0\\ 0\\ 0\\ 0\\ 0 \end{bmatrix}}^{5^8\times 1464843} \tag{5.17}$$

we have, this linear system wich are repeated $5^8 \times 1464843$ *times.*

$$\begin{cases} s_1 + s_2 + 2s_3 + 2s_4 + 2s_5 + 3s_6 + 3s_7 + 3s_8 + 4s_9 + 4s_{10} + 4s_{11} = 3\\ s_1 + 2s_2 + s_3 + 3s_4 + 4s_5 + s_6 + 2s_7 + 34s_8 + 4s_9 + 2s_{10} + 3s_{11} = 2\\ s_1 + 4s_{10} + 2s_{11} + = 0\\ s_2 + s_{11} = 0\\ s_3 + 2s_{10} = 0\\ s_4 + 4s_{10} + 3s_{11} + = 0\\ s_5 + 2s_{11} = 0\\ s_6 + 3s_{11} = 0\\ s_7 + s_{10} = 0\\ s_8 + 3s_{10} = 0\\ s_9 + 3s_{10} + s_{11} = 0. \end{cases}$$

According to Theorem 6 in [82] and the reference [19], this system has a unique solution. So, we recove the secret .

Example 5.4.6 *Let* $\mathfrak{R} = (\mathbb{Z}_3 + v_1\mathbb{Z}_3)(\mathbb{Z}_3 + v_1\mathbb{Z}_3 + v_2\mathbb{Z}_3)(\mathbb{Z}_3 + v_1\mathbb{Z}_3 + v_2\mathbb{Z}_3 + v_3\mathbb{Z}_3)$. *For* $k = 2$, *a generator matrix of subcode of* $\Phi\left(\Theta^{\alpha}_{2,1,\mathfrak{R}}\right)$ *is given by*

$$\Phi(C_3) = \overbrace{\begin{bmatrix} 1&1&2&2\\ 1&2&1&2 \end{bmatrix}}^{3^9\times 48427561} = \overbrace{\begin{bmatrix} g_1\\ g_2 \end{bmatrix}}^{3^9\times 48427561},$$

and

$$rank(\Phi(C_3)) = rank(\Phi(C_3)^\top \Phi(C_3)) = rank(\Phi(C_3\Phi(C_3)^\top) = 2,$$

the code $\Phi(C_3)$ *is LCD. The parity-check matrix* $H(\Phi(C_3))$ *of this code is*

$$H(\Phi(C_3)) = \overbrace{\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}}^{3^9\times 48427561} = \overbrace{\begin{bmatrix} y_1 \\ y_2 \end{bmatrix}}^{3^9\times 48427561} . \tag{5.18}$$

There are 9 *codewords of* $\Phi(C_3)$,

$$\overbrace{2001}^{3^9\times 48427561}, \overbrace{0210}^{3^9\times 48427561}, \overbrace{1122}^{3^9\times 48427561}, \overbrace{0120}^{3^9\times 48427561}, \overbrace{1002}^{3^9\times 48427561}, \overbrace{2211}^{3^9\times 48427561}, \overbrace{1212}^{3^9\times 48427561}, \overbrace{2121}^{3^9\times 48427561}, \overbrace{0000}^{3^9\times 48427561}.$$

Now, we examine a Multi-secret sharing schemes based on $\Phi(C_3)$. *Let the secret vector be* $S = \overbrace{2121}^{3^9\times 48427561}$. *We calculate the shares as follows*

$$t_1^\top =< (\overbrace{1122}^{3^9\times 48427561}), (\overbrace{2121}^{3^9\times 48427561}) >= 0$$
$$t_2^\top =< (\overbrace{1212}^{3^9\times 48427561}), (\overbrace{2121}^{3^9\times 48427561}) >= 2.$$

Moreover,

$$d_1^\top =< (\overbrace{1001}^{3^9\times 48427561}), (\overbrace{2121}^{3^9\times 48427561}) >= 0$$
$$d_2^\top =< (\overbrace{10110}^{3^9\times 48427561}), (\overbrace{2121}^{3^9\times 48427561}) >= 0.$$

By Equation 5.12, we should solve the following linear system to recover the secret.

$$\overbrace{\begin{bmatrix} 1 & 1 & 2 & 2 \\ 1 & 2 & 1 & 2 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}}^{3^9\times 48427561} \overbrace{\begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{bmatrix}}^{3^9\times 48427561} = \overbrace{\begin{bmatrix} 0 \\ 2 \\ 0 \\ 0 \end{bmatrix}}^{3^9\times 48427561}, \tag{5.19}$$

we have, this linear system wich are repeated $3^9 \times 48427561$ *times.*

$$\begin{cases} s_1 + \ s_2 + 2s_3 + 2s_4 = 0 \\ s_1 + 2s_2 + \ s_3 + 2s_4 = 2 \\ s_1 \qquad\qquad + \ s_4 = 0 \\ \qquad s_2 + 2s_3 \qquad\quad = 0 \end{cases}.$$

According to Theorem 6 in [82] and the reference [19], this system has a unique solution. So, we recove the secret $S = \overbrace{2121}^{3^9 \times 48427561}$.

5.5 Conclusion

We have studied α-simplex and α-MacDonald codes over $\mathfrak{R}$ using the concatenation of these codes over $\mathcal{R}_1, \mathcal{R}_2$ *and* $\mathcal{R}_3$ respectively. Lastly, we have applied the Multi-secret sharing schemes to subcodes of these Linear codes.

Conclusion and perspectives

This work addresses certain challenges in error-correcting code theory within the context of finite rings. Specifically, the computation of homogeneous weights is treated as a generalization of Hamming weight, applied to a novel class of finite rings denoted as $\mathcal{R}_{p^s,\theta}$. These rings are defined by extending the concept of homogeneous weights from $\mathbb{F}_q$. We introduce a novel approach to constructing generator matrices for these codes and Gray maps within $\mathcal{R}_{p^s,\theta}$. Additionally, we establish bounds for the covering radius of these codes. Furthermore, we explore properties of LCD codes associated with simplex and MacDonald codes on $\mathcal{R}_{p^s,\theta}$. We delve into a specific instance, the $\mathfrak{R}_{5,3}$ ring, providing definitions, properties, and illustrative examples. The work concludes with the application of multi-secret sharing schemes on simplex and MacDonald linear codes over the ring $\mathbb{Z}_q$. In the spirit of extending our contributions, we pose several questions, some of which aim to expand the scope of our work, while others stand as independent inquiries.

▷ Exploring additional codes on these rings, such as torsion codes and simplex linear codes of type β, is an intriguing avenue.

▷ Investigating alternative methods for constructing codes from these rings could offer valuable insights.

▷ Considering the case where the rings are not local, and exploring the implications for the codes defined on such rings, adds another layer of interest to our research.

Annexe

In this appendix, we will present some algebraic structures [61]. We will give some properties that we use in this thesis. We are going to define the rings, the ideals, and the modules which are basic tools to carry out the definitions of the codes on rings. We will be mainly interested in the families of the codes on the Frobenius rings [7, 27].

5.6 Generalities on Finite Rings, Ideals and Modules

5.6.1 Anneaux

Definition 5.6.1 *A ring is a set $\mathcal{S}$ endowed with two internal laws $+$ and $\times$ satisfying the conditions following*

1. *The couple $(\mathcal{S}, +)$ is a commutative group, and the neutral element is denoted $0_{\mathcal{S}}$.*
2. *The law $\times$ is associative, commutative, and left and right distributive with respect to the law $+$.*
3. *The law $\times$ has a neutral element noted $1_{\mathcal{S}}$.*

Definition 5.6.2 *Let $\mathcal{S}, +, \times$ be a ring and $\mathcal{B}$ is a subset of $\mathcal{S}$. We say that $\mathcal{B}$ is A subring of $\mathcal{S}$ when*

1. $1_{\mathcal{A}} \in \mathcal{B}$,
2. *$\mathcal{S}$ stable by $+$ and by $\times$,*

3. *For all* $x \in \mathcal{B}, (-x) \in \mathcal{B}$.

Let us give some useful definitions.

Definition 5.6.3 *[7] An invertible element of* $\mathcal{S}$ *is an element* $x \neq 0$ *of* $\mathcal{S}$ *which "divides" 1. In other words, we have* $xy = 1$ *for some* $y \neq 0$ *in* $\mathcal{S}$.

Definition 5.6.4 *An element* ϑ *of a ring* $\mathcal{S}$ *is divisor of zero if and only if it is nonzero and if there exists* $\kappa \in \mathcal{S}$ *nonzero such that* $\vartheta\kappa = 0$.

Definition 5.6.5 *A ring* $\mathcal{S}$ *is integral if and only if* $\mathcal{S} \neq \{0\}$ *and if* $\mathcal{S}$ *has no divisor of zero, in other words if we have*

$$\vartheta\kappa = 0 \Rightarrow (\vartheta = 0 \text{ or } \kappa = 0).$$

Definition 5.6.6 *A fiels is a ring with invertible non-zero elements*

Homomorphism of rings

Definition 5.6.7 *Let* $\mathcal{H}$ *and* $\mathcal{H}'$ *be two rings. A map* $f : \mathcal{H} \longrightarrow \mathcal{H}'$ *is a homomorphism of rings if and only if*

1. $f(\vartheta + \kappa) = f(\vartheta) + f(\kappa) for\ all\ \vartheta, \kappa \in \mathcal{H}$,
2. $f(\vartheta\kappa) = f(\vartheta)f(\kappa) for\ all\ \vartheta, \kappa \in \mathcal{H}$,
3. $f(1_{\mathcal{H}}) = 1_{\mathcal{H}'}$.

Remark 5.6.8 *A ring isomorphism is a bijective ring homomorphism. Its reciprocal bijection is a ring homomorphism.*

5.6.2 Ideals and quotient rings

All of the work in this study takes into account commutative rings.

Definition 5.6.9 *A subset* $\mathcal{I}$ *of a ring* $\mathcal{S}$ *is called ideal if and only if*

1. $\mathcal{I}$ *is a subgroup of* $(\mathcal{S}, +)$,

2. $\forall \vartheta \in \mathcal{S}, \forall x \in \mathcal{I} : \vartheta x \in \mathcal{I}$.

Definition 5.6.10 *If an ideal* $\mathcal{I}$ *of* $\mathcal{S}$ *is not equal to the all ring, it is said to be proper in* $\mathcal{S}$.

Definition 5.6.11 *Let* $\mathcal{I}$ *an ideal of a ring* $\mathcal{S}$. *The quotient ring is defined, as*

$$\mathcal{S}/\mathcal{I} = \{\vartheta + \mathcal{I} : \vartheta \in \mathcal{S}\}.$$

Definition 5.6.12 *If an ideal* $\mathcal{I}$ *of* $\mathcal{S}$ *isn't equal to the all ring, it is considered proper in* $\mathcal{S}$.

Definition 5.6.13 *Let's assume that* $\mathcal{I}$ *is an ideal of the ring* $\mathcal{S}$. *The ideal* $\mathcal{I}$ *is a prime ideal of* $\mathcal{S}$ *if and only if*

$$\forall (\vartheta, \iota) \in \mathcal{S} \times \mathcal{S}, \vartheta.\iota \in \mathcal{I} \Rightarrow \vartheta \in \mathcal{I} \text{ or } \iota \in \mathcal{I}.$$

Example 5.6.14

1. *The ideals* $\{0\}$ *and the* $n\mathbb{Z}$ *for* n *prime are prime ideals in the ring of integers* $\mathbb{Z}$.

2. *A prime ideal is the inverse image of a prime ideal by a ring morphism.*

Theorem 5.6.15 *Let* $\mathcal{S}$ *be a unitary commutative ring, and* $\mathcal{I} \neq \mathcal{S}$ *a proper ideal of* $\mathcal{S}$, *then* $\mathcal{S}/\mathcal{I}$ *is an integral ring (ring integrates) if and only if* $\mathcal{I}$ *is a prime ideal of* $\mathcal{S}$.

Example 5.6.16 *The sets* $\mathbb{Z}/6\mathbb{Z}$ *and* $\mathbb{Z}/8\mathbb{Z}$ *are not integral because* $(4.2 = 0)$ *and 8 is not prime.*

Theorem 5.6.17 *Let* $\mathcal{S}$ *unitary commutative ring, an ideal* $\mathcal{I}$ *of* $\mathcal{S}$ *is maximal if and only if* $\mathcal{S}/\mathcal{I}$ *is a fiels.*

Corollary 5.6.18 *A maximal ideal contains all of* $\mathcal{S}$ *non-invertible elements.*

Definition 5.6.19 *If there exists an element* $\vartheta \in \mathcal{I}$ *such that* $\mathcal{I} =< \vartheta >$, *where*

$$< \vartheta >= \{\vartheta x : x \in \mathcal{S}\}.$$

then the ideal $\mathcal{I}$ of a ring $\mathcal{S}$ is ***principal***

Remark 5.6.20 *The ideal $\mathcal{I}$ is generated by the element ϑ and ϑ is a generator of $\mathcal{I}$. A ring of integrity where every ideal is principal.*

Definition 5.6.21 *1. If there is an integer $n \neq 0$ such that $\vartheta^n = 0$, then the element ϑ of a ring $\mathcal{S}$ is* ***nilpotent****.*

2. The set of nilpotent elements of $\mathcal{S}$ is called the ***Nilradical*** *of $\mathcal{S}$ and denoted $Nil(\mathcal{S})$.*

The statements that follow demonstrate the relation between $Nil(\mathcal{S})$ and the prime ideals of the ring.

Proposition 5.6.22 *The intersection of all the prime ideals of $\mathcal{S}$ is the nilradical of $\mathcal{S}$.*

Proposition 5.6.23 *A local ring has only one nilpotent maximal ideal.*

Proof 5.6.24 *Let $\mathcal{S}$ be a finite ring then it admits a finite number of ideals first $\{P_1, P_2, ..., P_s\}$ so $\mathcal{S}/P_i$, $1 \leq i \leq s$ are integral rings. Now a finite integral ring is a field, so the P_i are maximal ideals for $1 \leq i \leq s$. Which leads to $Nil(\mathcal{S}) = \bigcap_{i=1}^{s} P_i = P$.*

Definition 5.6.25 *The ring with a unique maximal ideal is a commutative* ***local ring****. This ideal is then constituted by the set of non-invertible elements.*

Therefore, following assertions are equivalent.

1. $\mathcal{S}$ has exactly one maximal ideal.
2. $\mathcal{S}$ is a local ring.
3. The divisors of zero of $\mathcal{S}$ are contained in a proper ideal.
4. The divisors of zero of $\mathcal{S}$ form an ideal.
5. The zero divisors of $\mathcal{S}$ form an additive commutative group.
6. For all x in $\mathcal{S}$, one of the two elements of the set $\{x, 1 + x\}$ is invertible.

5.6.3 Galois Ring

We introduce here the Galois rings, which are used in many branches of mathematics, particularly coding theory. [7, 20].

Definition 5.6.26 *If $\mathcal{S}$ is commutative, unitary, and the set of these zero divisors has the form $p\mathcal{S}$, where p is a prime number, then $\mathcal{S}$ is a Galois ring.*

Remark 5.6.27 *a. Galois fields can therefore be considered as Galois rings containing no zero divisors. The most used example in code theory is $\mathcal{S} = \mathbb{Z}_{p^m}$, the ring of integers modulo p^m.*

b. The additive order of the neutral element for multiplication by one is the characteristic denoted by the sing $car(\mathcal{S})$

c. The characteristic of a Galois ring $\mathcal{S}$ is

$$car(\mathcal{S}) = p^m, m \in \mathbb{N}.$$

d. The ring $\mathbb{Z}_{p^m}$ is a local ring for p prime number.

5.6.4 Modules

Definition 5.6.28 *An $\mathcal{S}$-module $(\mathcal{E}, +, .)$ is a set team of an internal law $+$ and an external law $\mathcal{S} \times \mathcal{E} \longrightarrow \mathcal{E}, (\alpha, \mathcal{E}) \longrightarrow \alpha m$ verifying*

(I) $(\mathcal{E}, +)$ is an abelian group.

(II) We also have the following four properties, for all $\tau, \upsilon \in \mathcal{S}$ and all $\vartheta, \vartheta' \in M$.

1. $\tau(\vartheta + \vartheta') = \tau\vartheta + \tau\vartheta'$,
2. $(\tau + \upsilon)\vartheta = \tau\vartheta + \upsilon\vartheta$,
3. $(\tau\upsilon)\vartheta = \tau(\upsilon\vartheta)$,
4. $1 \times \vartheta = \vartheta$.

Definition 5.6.29 *A part N of $\mathcal{E}$ is a* ***submodule*** *if and only if it contains 0, and if for all κ, ι of N, and all τ of $\mathcal{S}$, we have, $\kappa + \iota \in N$ and $\tau\kappa \in N$.*

Remark 5.6.30 *Let $(\mathcal{M}_i)_{i\in I}$ be a family of $\mathcal{S}$-modules with I be finite set or not. Then the set product $\prod_{i\in I} \mathcal{M}_i$ is an $\mathcal{S}$-module for the obvious laws; it is called the product $\mathcal{S}$-module of $\mathcal{M}_i$.*

The following definition is analogous to the one we have in vector spaces:

Definition 5.6.31 *Let $(\mathcal{M}_i)_{i\in I}$ be a family of $\mathcal{S}$-modules.* ***The direct*** *("external")* ***sum*** *of $\mathcal{M}_i$ nodes $\bigoplus_{i\in I} \mathcal{M}_i$ is the submodule of $\prod_{i\in I} \mathcal{M}_i$ consisting of the almost zero families $(\mathcal{M}_i)_{i\in I}$. If I is finite, the direct sum coincides with the direct product.*

Definition 5.6.32 *An $\mathcal{S}$-module M is to be of* ***finite type*** *if there exists a finite part $\mathbf{G}$ of M, such that M is generated by $\mathbf{G}$. It is* ***free*** *if it has a basis, i.e. A family $(x_i)_{i\in I}$ such that any element x of M can be written in a unique way $x = \sum_{i\in I} \alpha_i x_i$, with $(\alpha_i)_{i\in I}$ an almost null family of elements of $\mathcal{S}$.*

5.6.5 Frobenius ring

Definition 5.6.33 *If $\mathcal{H}, \mathcal{H}'$ are two rngs, then an $\mathcal{H}$-$\mathcal{H}'$- bimdule is an abilian group $(\mathcal{M}, +)$ such that*

1. *$\mathcal{M}$ is a laft $\mathcal{H}$-module and a right $\mathcal{H}'$-module.*
2. *Fr all $k \in \mathcal{H}$, $h \in \mathcal{H}'$ and $\vartheta \in \mathcal{M}$ we have, $(k\vartheta)h = k(\vartheta h)$.*

Let $\mathcal{H}$ be a untary finite ring. The group of characters of the additive group $\mathcal{H}$ is denoted by $\widehat{\mathcal{H}} = Hom_{\mathbb{Z}}(\mathcal{H}, \mathbb{C}^{\times})$. This group has a strcture of an $\mathcal{H}$-$\mathcal{H}'$-bimodule defined by

$$\chi^r(x) = \chi(rx) \text{ and } {}^r\chi(x) = \chi(xr),$$

for all $r, x \in \mathcal{H}$, and for all $\chi(x) \in \widehat{\mathcal{H}}$.
After all these concepts we arrive at the following definition.

Definition 5.6.34 *if* ${}_{\mathcal{H}}\widehat{\mathcal{H}} =_{\mathcal{H}} \mathcal{H}$ *then a finite ring* $\mathcal{H}$ *is called a Frbenius ring .*

Remark 5.6.35 *If* $\mathcal{H}$ *is a finite Frbenius ring, then* $\mathcal{H}$ *and* $\widehat{\mathcal{H}}$ *are isomrphic.*

Definition 5.6.36 *Let* $\mathcal{I}, \mathcal{J}$ *be two ideals of* $\mathcal{S}$ *then they are foreign (to each other) if* $\mathcal{I} + \mathcal{J} = \mathcal{S}$.

Let $\mathcal{H}$ is a commtative ring, and $\mathcal{I}_1, \mathcal{I}_2, \ldots, \mathcal{I}_n$ be idels in $\mathcal{H}$. The ideal $\mathcal{I}_1 + \mathcal{I}_2 + \ldots + \mathcal{I}_\iota + \ldots + \mathcal{I}_n$ is formd of sums $h_1 + h_2 + \ldots + h_n$, *where* $h_i \in \mathcal{H}$ *for* $\iota = 1, 2, \ldots, n$.

Definition 5.6.37 *a. The ideals* $\mathcal{I}_1, \mathcal{I}_2, \ldots, \mathcal{I}_j, \ldots, \mathcal{I}_n$ *are foreign in twos if* $\mathcal{I}_\iota$ *and* $\mathcal{I}_j$ *are foreign for all* $\iota \neq j$.

b. The ideals $\mathcal{I}_1, \mathcal{I}_2, \ldots, \mathcal{I}_n$ *are foreign if we have*

$$\mathcal{I}_1 + \mathcal{I}_2 + \ldots + \mathcal{I}_n = \mathcal{H}.$$

Theorem 5.6.38 *Let the ideals* $\mathcal{I}_1, \mathcal{I}_2, \ldots, \mathcal{I}_n$ *in* $\mathcal{H}$ *, sch that*

$$\mathcal{I}_\iota + \mathcal{I}_j = \mathcal{H},\ \iota \neq j.$$

We assume that $\mathcal{I}_1, \mathcal{I}_2, \ldots, \mathcal{I}_n$ *are foreign ideals in pairs. Then the ring morphism*

$$\phi : \mathcal{H} \longrightarrow \mathcal{H}/\mathcal{I}_1 \oplus \mathcal{H}/\mathcal{I}_2 \oplus \ldots \oplus \mathcal{H}/\mathcal{I}_n,$$

conclude a ring isomorphism

$$\mathcal{H}/\mathcal{I}_1 \cap \mathcal{I}_2 \cap \ldots \cap \mathcal{I}_n \longrightarrow \bigoplus_{\iota=0}^{n} \mathcal{H}/\mathcal{I}_\iota.$$

The class of finite Frobenius rings is wide enough, by the following proposition.

Proposition 5.6.39 *(1) All the finite principal ring is a Frobenius ring.*

(2) If $\mathcal{H}$ *and* $\mathcal{K}$ *are Frobenius rings, then* $\mathcal{H} \times \mathcal{K}$ *is a Frobenius ring.*

(3) If $\mathcal{H}$ *is a Frobenius ring, then* $\mathcal{M}_n(\mathcal{H})$ *the ring of all matrices of size* $n \times n$ *on* $\mathcal{H}$*, is a Frobenius ring.*

(4) If $\mathcal{H}$ *is a Frobenius ring, and* G *a finite group, then* $\mathcal{H}[G]$ *is a Frobenius ring.*

Bibliography

[1] T. Abualrub, I. Siap, and N. Aydin, $\mathbb{Z}_2\mathbb{Z}_4$-*additive cyclic codes*, IEEE Trans. Inform. Theory 60, pp.115-121, 2014.

[2] A. Alahmadi, A. Altassan, A. AlKenani, S. Çalkavur, S. Hatoon S and S. Patrick, *A Multi-secret sharing Scheme Based on LCD Codes*, Mathematics, 8, pp.272, 2020.

[3] M. AL-Ashker, *Simplex codes over the ring* $\mathbb{F}_2 + u\mathbb{F}_2$, The Arabian Journal for Science and Engineering, 30, pp.0227-285, 2005.

[4] M. Al-Ashker, *Simplex codes over the ring* $\sum_{n=0}^{s} u^n\mathbb{F}_2$, Turk .J. Math, 29, pp.221-233, 2005.

[5] T. Aoki, P. Gaborit, M. Harada, M. Ozeki, and P. Solé, *On the covering radius of* $\mathbb{Z}_4$*-codes and their lattices*, IEEE Trans. Inform. Theory 45, pp.2162-2168, 1999.

[6] A. Batoul .*Construction des codes auto-duaux*. Diss. universite de USTHB, Algerie, 2013.

[7] A. Batoul, *Les codes correcteurs d'erreurs définis sur les anneaux fini*, polycopie, 2016.

[8] M. Barbier, *Decodage en liste et application a la securite de l'information*. Diss. Ecole Polytechnique X, 2011.

[9] J. Bierbrauer, *Introduction to Coding Theory*, Chapman and Hall/CRC. Boca Raton. FL 2005.

[10] M. Bilal, J. Borges, S.T. Dougherty, and C. Fernández-Córdoba, *Maximum distance separable codes over* $\mathbb{Z}_4$ *and* $\mathbb{Z}_2\mathbb{Z}_4$, Des. Codes Cryptogr, 61, pp.31-40, 2011.

[11] J. Borges, S.T. Dougherty, and C. Fernández-Córdoba, *Characterization and constructions of self-dual codes over* $\mathbb{Z}_2\mathbb{Z}_4$, Adv. Math. Commun, 6, pp.287-303, 2012.

[12] J. Borges, C. Fernández-Córdoba, J. Rifá, *Every* $\mathbb{Z}_{2k}$*-code is a binary propelinear code*, Electronic Notes in Discrete Mathematics. Elsevier Science. Amsterdam, 10, pp.100-102, 2001.

[13] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifá, and M. Villanueva, $\mathbb{Z}_2\mathbb{Z}_4$*-linear codes: Generator matrices and duality*, Des. Codes Cryptogr. 54, pp.167-179, 2010.

[14] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifá, and M. Villanueva, *On* $\mathbb{Z}_2\mathbb{Z}_4$*-linear codes and duality*, V Jornades de Matemàtica Discreta i Algorísmica, Soria (Spain), pp.171-177, 2006.

[15] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifá, and M. Villanueva,*On* $\mathbb{Z}_2\mathbb{Z}_4$*-linear codes and duality*, VJMDA. Ciencias, 23. Secr. Publ. Intercamb. Ed., Valladolid, pp.171-177, 2006.

[16] J. Borges, C. Fernandez-Cóordoba, J. Pujol, J. Rifá and M. Villanueva, $\mathbb{Z}_2\mathbb{Z}_4$*-additive codes*. A MAGMA package. Autonomous University of Barcelona (UAB). Bellaterra. Barcelona, http://www.ccsg.uab.cat, 2007.

[17] M.C. Bhandari, M.K. Gupta, and 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 in Computer Science 1719, pp.170-180, 1999.

[18] J.V. Brawley, L. Carlitz, *Enumeration of matrices with prescribed row and column sums*, Linear Algebra Appl. 6, pp.165 -174, 1973.

[19] S. Calkavur, S. K. Nauman, C. Özel, H. Zekraoui, *The least-squares solutions in linear codes based multisecret-sharing approach*. International Journal of Information and Coding Theory, 5, pp.290-302, 2020.

[20] W. Cary, and Vera Pless, *Fundamentals of error-correcting codes*, Cambridge university press, 2010.

[21] K. Chatouh, K. Guenda, T. A. Gulliver and L. Noui, *Simplex and MacDonald codes over* R_q, J. Appl. Math. Comput. DOI 10.1007/s12190-016-1045-4, 2016.

[22] K. Chatouh, *Linear Codes over* $R = R_1R_2R_3$ *and Their Applications in Secret Sharing Schemes*, Studies on Scientific Developments in Geometry, Algebra, and Applied Mathematics Adnan Tercan Aydin Gezer , 46, 2022.

[23] K. Chatouh, Guenda K and Gulliver T.A, *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*. Computational and Applied Mathematics, 39, pp.3, 2020.

[24] K. Chatouh, K. Guenda, T.A. Gulliver and L. Noui, *Secret Sharing Schemes Based on Gray Images of Linear Codes over* $R_{q,m}$, International Conference on Coding and Cryptography ICCC, USTHB, Algiers, Algeria, November 2-5, 2015.

[25] K. Chatouh, K. Guenda, T.A. Gulliver and L. Noui, *On some classes of linear codes over* $\mathbb{Z}_2\mathbb{Z}_4$ *and their covering radii*, Journal of Applied Mathematics and Computing, pp.1-22, First online: 16 January 2016.

[26] K. Chatouh,L. Noui, M. Bin Mamat, *Codes over* $\mathbb{Z}_2(\mathbb{Z}_2 + u\mathbb{Z}_2)$ *and their covering radii*. Journal of Algebra, Number Theory: Advances and Applications, 16, pp.25-39, 2016.

[27] K. Chatouh, *Construction et étude des codes linéaires*. Diss. Université de Batna 2, 2017.

[28] J. Chen, Y. Huang, B. Fu, J. Li, *Secret sharing schemes from a class of linear codes over finite chain ring*, Journal of Computational Information Systems, 9, pp.2777-2784, 2013.

[29] C.J. Colbourn and M.K. Gupta, *On quaternary MacDonald codes*, Proc. Int. Conf. on Inform. Tech.: Coding and Computing, pp.212-215, 2003.

[30] G.D. Cohen, M.G. Karpovsky, H.F. Mattson, and J.R. Schatz, *Covering radius-Survey and recent results*, IEEE Trans. Inform. Theory 31, pp.328-343, 1985.

[31] I. Constantinescu, W. Heise, *A metric for codes over residue class rings of integers*, Problemy Peredachi Informatsii 33, pp.22-28, 1997

[32] P. Delsarte, *Four fundamental parameters of a code and their combinatorial significance*, Inform. Contr. 23, pp.407-438, 1973.

[33] P. Delsarte and J. M. Goethals, *Alternating bilinear forms over $GF(q)$*, J. Comb. Theory. 19, pp.26-50, 1975.

[34] A. Dertli, Y. Cengellenmis, and S. Eren, *Some results on the linear codes over the finite ring $F_2 + v_1F_2 + \ldots + v_rF_2$*. International Journal of Quantum Information, 14, 2016.

[35] A. Dertli, Y. Cengellenmis, and S. Eren, *Quantum codes over $F_2+uF_2+vF_2$*. Palestine Journal of Mathematics 4 , 547-552, 2015.

[36] S.T. Dougherty, E. Saltürk, *Counting codes over rings*, Des. Codes Cryptogr. 73, pp.151 -165, 2014.

[37] S.T. Dougherty, B. Yildiz, and S. Karadeniz, *Codes over R_k Gray maps and their binary images*, Finite Fields Appl, 17, pp.205-219, 2011.

[38] R. A. Fisher, *The theory of confounding in factorial experiments in relation to the theory of groups*, Ann. Eugenics. 11, pp.341-353, 1942.

[39] R.A. Fisher, *A system of confounding for factors with more than two alternatives, giving completely orthogonal cubes and higher powers*, Ann. Eugenics. 12, pp.2283-2290, 1945.

[40] M.S. Garg, *On Optimum Codes and their Covering Radii*, PhD thesis. IIT Kanpur. India, 1990.

[41] M. Greferath and S.E. Schmidt, *Gray isometries for finite chain rings and a nonlinear ternary (36, 3/sup 12/, 15) code.* IEEE Transactions on Information Theory 45, 2522-2524, 1999.

[42] K. Guenda, *Sur l'equivalence des codes*. Diss. universite de USTHB, Algerie, 2010.

[43] M.K. Gupta and C. Durairajan, *On the covering radius of Some modular codes*, Adv. Math. Commun., 8, pp.129-137, 2014.

[44] M.K. Gupta, D.G. Glynn, and T.A. Gulliver, *On Senary Simplex Codes*, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Lecture Notes in Computer Science, 2227, pp.112–121, 2001.

[45] M.K. Gupta, *On Some Linear Codes over* $\mathbb{Z}_{2^s}$, Ph.D. Thesis, IIT, Kanpur, 1999.

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

[47] I. Habibul, O. Prakash, *Skew constacyclic codes over* $F_q + uF_q + vF_q$. arXiv preprint arXiv:1710.07789, 2017.

[48] O. Haddouche, K. Chatouh, *Some Constructions of Linear Codes over a ring* $\mathcal{R}$, Fourth Edition of the International Conference on Research in Applied Mathematics and Computer Science ICRAMCS 2022, March 24-25-26, 2022

[49] O. Haddouche, H. Zekraoui and K. Chatouh, *Hommogenous on weights over the ring* $\mathfrak{R}_{5,3} = \mathbb{F}_5 + u_1\mathbb{F}_5 + u_2\mathbb{F}_5 + u_3\mathbb{F}_5$, Advances in Mathematics, Scientific Journal, 11, pp.1103 -1114, 2022.

[50] O. Haddouche, H. Zekraoui and K. Chatouh, *Homogeneous Weight and its Applications in Some Linear codes over* $\mathcal{R}_{p^s,\theta} = \mathbb{F}_{p^s} + u_1\mathbb{F}_{p^s} + \ldots + u_\theta\mathbb{F}_{p^s}$, The Jordanian Journal of Mathematics and Statistics. under review.

[51] O. Haddouche, K. Chatouh, *Simplex and MacDonald codes over* $\mathfrak{R}_{5,3}$, Mini-Congrès des Mathématiciens Algériens MCMA'2021, October 27-28, 2021.

[52] O. Haddouche, K. Chatouh, *Some Construction of Linear codes over* $\mathcal{R} = \mathcal{R}_1\mathcal{R}_2$, National Conference of Mathematics and Applications CNMA 2021, December 11, 2021.

[53] O. Haddouche, K. Chatouh, *Simplex and MacDonald LCD Linear Codes over* $\mathfrak{R}$, First National Conference on Mathematics and its Applications, CNMA'2021, December 13-14,2021, Bordj Bou Arreridj.

[54] A.R. Hammons, P.V. Kumar, A.R. Calderbank, N. J. A. Sloane, and P. Solé, *The* $\mathbb{Z}_4$*-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory 40, pp.301-319, 1994.

[55] T. Honold,*Characterization of finite Frobenius rings*, Arch. Math., 76, pp.406-415, 2001.

[56] W.C. Huffman and V. Pless, *Fundamentals of Error-correcting Codes*, New York: Cambridge University Press, 2003.

[57] T.W. Hungerford, and Springer Algebra. *Graduate texts in mathematics 73*. New York, 1974.

[58] M.L. John and S. Virgilio, *Bounds on the* p^r*-ary image of linear block codes over the finite semi-local frobenius ring* $F_{p^r} + vF_{p^r}$, Southeast-Asian J. of Sciences, 2012.

[59] E.D. Karnin, J.W. Greene, and M.E. Hellman, *On secret sharing systems*, IEEE Trans. Inf. Theory, IT-29, pp.35-41, Jan. 1983.

[60] S. Ling, and Chaoping Xing. Coding theory: a first course. Cambridge University Press, 2004.

[61] F. Liret, D. Martinais, *Algèbre 1 anneée, 2 édition*, Dunod.

[62] J.E. MacDonald, *Design methods for maximum minimum-distance error-correcting codes*, pp.43-57, 1960.

[63] F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publishing Company. Amsterdam. New York, Oxford 1977.

[64] J.L. Massey, *Some applications of coding theory in cryptography*, Codes and Ciphers: Cryptography and Coding IV, Formara Ltd, Esses, England, pp.33-47, 1995.

[65] J.L. Massey, *Linear codes with complementary duals.* Discrete Mathematics, 106, pp.337-342, 1992.

[66] M. Nadler, *A 32-point n=12, d=5 code*, IRE Transation on information Theory, 8, 1962.

[67] P.C. Pandian and C. Duruairajan, *On the covering radius of some code over* $R = \mathbb{Z}_2 + u\mathbb{Z}_2$, *where* $u^2 = 0$, Int, Journal of Research in Applied, Matural and Social Sciences 2, pp.61-70, 2014.

[68] R. Pellikaan, Xin-Wen Wu, S. Bulygin and R. Jurrius, *Error-correcting codes and cryptology*, Cambridge, 2012.

[69] F.P. Preparata, *A class of optimum nonlinear double-error-correcting codes*, Inform. Control. 13, pp.378-400, 1968.

[70] J. Pujol and J. Rifà, *Translation invariant propelinear codes*, IEEE Trans. Inform. Theory 43, pp.590-598, 1997.

[71] M.K. Raut and M.K. Gupta,*On octonary codes and their covering radii*, arXiv:1411.1822v3 [cs.IT] Dec. 2014.

[72] R.M. Roth. *Introduction to coding theory*. Cambridge University Press, 2006.

[73] C.E. Shannon, *A mathematical theory of communication*, The Bell System Technical Journal, 27, pp.379-423, 1948.

[74] P. Solé, *Codes over Rings, Series on Coding Theory and Cryptology*, 6, 2009.

[75] S.A. Spence, *Introduction to Algebraic Coding Theory*. Supplementary material for Math, 336, 2002.

[76] J.H. Van Lint, *Intrduction to coding theory*, Springer-Verlag New York. Inc. Secaucus NJ. USA, 1982.

[77] J. A. Wood, *Duality for modules over finite rings and applications to coding theory.* American journal of Mathematics, 555-575, 1999.

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

[79] B. Yildiz and S. Karadeniz, *Linear codes over* $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, Designs. Codes. Crypt, 54, pp. 61-81, 2010.

[80] B. Yildiz and I.G. Kelebek, *The homogeneous weight for* R_k*, related Gray map and new binary quasicyclic codes*, arXiv:1504.04111v1 [cs.IT] 16 Apr 2015.

[81] B. Yildiz and S. Karadeniz, *Cyclic codes over* $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, Designs. Codes. Crypt, 58, pp.221-234, 2011.

[82] L. Zihui. *Galois LCD codes over rings.* Advances in Mathematics of Communications, 2022.