RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE

MINISTÈRE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ DE BATNA 2

FACULTÉ DES MATHÉMATIQUES ET D´INFORMATIQUE

DÉPARTEMENT DES MATHÉMATIQUES

THÈSE

Pour obtenir le titre de Docteur en Sciences

Spécialité :

MATHÉMATIQUES

Présentée par:

Ahlem MELAKHESSOU

Intitulée:

Codes sur les anneaux

Soutenue le: 23/12/2020, devant un jury composé de:

Guedjiba Said,	Professeur,	Université de batna 2,	Président
Guenda Kenza,	Professeur,	Université USTHB , Algérie,	Directeur de thèse
Noui Lemnouar,	Professeur,	Université de batna 2,	Co-directeur
Trabelsi Nadir,	Professeur,	Université de setif 2,	Examinateur
Badis Abdelhafid,	Professeur,	Université de Khenchela,	Examinateur
Melkemi Lamine,	Professeur,	Université de batna 1	Examinateur

Acknowledgements

First and foremost, I would like to thank ***Allah*** for this help and guidance. I would like to express our deepest gratitude to our supervisor, Pr.***Guenda Kenza*** for her ideas, all her help, her valuable guidance from the beginning, her encouragement, friendly approach and above all for her endless patience.

I would like also grateful to our co-supervisor, Pr.***Noui Lemnouar*** who never ceased to give all the help and support we needed in times of hardships.

My gratitude, indebtedness and deliberation are extended to the members of jury for devoting time and patience to read and examine the present research work: Pr. ***Guedjiba Said***, Pr. ***Trabelsi Nadir***, Pr. ***Badis Abdelhafid*** , and Pr. ***Melkemi Lamine***.

I am also greatly indebted to Pr. ***T. A. Gulliver*** University of Victoria Canada and Pr. ***Nuh Aydin*** Department of Mathematics and Statistics, Kenyon College, USA, for their scientific advice, knowledge, constructive criticism, insightful discussions.

My acknowledgment would be incomplete without thanking Mrs. ***Hebbache Zineb*** for all her help.

We would, also, like to thank my parents, husband and colleagues for their great support andpatience with us.

Abstract

This work has reached this level by producing two journal papers and four conference papers.

The first journal paper is entitled, « On Codes over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$ », it appeared in Journal of Applied Mathematics and Computing, 2017. In this paper we investigated linear codes with complementary dual (LCD) codes and formally self-dual codes over the ring $R = \mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$, where $v^3 = v$, for q odd. We give conditions on the existence of LCD codes and present construction of formally self-dual codes over R. Further, we give bounds on the minimum distance of LCD codes over $\mathbb{F}_q$ and extend these to codes over R.

The second journal paper is entitled, « $\mathbb{Z}_q(\mathbb{Z}_q + u\mathbb{Z}_q)-$Linear Skew Constacyclic Codes », it appeared in Journal of Algebra Combinatorics Discrete Structures and Applications. In this paper we study skew constacyclic codes over the ring $\mathbb{Z}_q R$, where $R = \mathbb{Z}_q + u\mathbb{Z}_q$, $q = p^s$ for a prime p and $u^2 = 0$. We give the definition of these codes as subsets of the ring $\mathbb{Z}_q^{\alpha} R^{\beta}$. Some structural properties of the skew polynomial ring $R[x, \Theta]$ are discussed, where Θ is an automorphism of R. We describe the generator polynomials of skew constacyclic codes over $\mathbb{Z}_q R$, also we determine their minimal spanning sets and their sizes. Further, by using the Gray images of skew constacyclic codes over $\mathbb{Z}_q R$ we obtained some new linear codes over $\mathbb{Z}_4$. Finally, we have generalized these codes to double skew constacyclic codes over $\mathbb{Z}_q R$.

The third paper is entitled, « Formally Self-dual Codes over A_k », it was presented at CMA-2014 (Tlemcen). In this paper we present several kinds of construction of formally self-dual codes over the ring

$$A_k = \mathbb{F}_2 \left[v_1, \ldots, v_k\right] / \left\langle v_i^2 = v_i, v_i v_j = v_j v_i \right\rangle.$$

The fourth paper is entitled, « LCD Codes over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$ », it was presented at CMA-2016 (Batna). The purpose of this work is to investigate linear codes with complementary dual(LCD) codes over the ring $R = \mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$, where $v^3 = v$, for q odd.

The fifth paper is entitled, « $\mathbb{Z}_q(\mathbb{Z}_q + v\mathbb{Z}_q + \ldots + v^{m-1}\mathbb{Z}_q)-$ Linear Cyclic, Skew Cyclic and Constacyclic Codes », it was presented at ECMI-SciTech'2017 (Constantine). In this paper, we study cyclic, skew cyclic and constacyclic codes over the ring $\mathbb{Z}_q(\mathbb{Z}_q + v\mathbb{Z}_q + \ldots + v^{m-1}\mathbb{Z}_q)$, where $q = p^s$, p is a prime and $v^m = v$. We give the definition of these codes as subsets of the ring $\mathbb{Z}_q^{\alpha}R^{\beta}$.

The sixth paper is entitled, « Double Skew $(1+u)-$Constacyclic Codes over $\mathbb{Z}_4(\mathbb{Z}_4 + u\mathbb{Z}_4)$ », it was presneted at IWCA-2019 (Oran). In this paper, we study skew constacyclic codes over the ring $\mathbb{Z}_4R$ where $R = \mathbb{Z}_4 + u\mathbb{Z}_4$, for $u^2 = 0$. We give the definition of these codes as subsets of the ring $\mathbb{Z}_4^{\alpha}R^{\beta}$. Further, we have generalized these codes to double skew $(1+u)-$constacyclic codes over $\mathbb{Z}_4R$.

Keywords: Formally self-dual codes, LCD codes, optimal codes, Gray map, automorphism, skew constacyclic codes, skew polynomial rings, double skew constacyclic codes.

Résumé

Ce travail a atteint ce niveau en produisant deux papiers et quatre papiers de conférence.

Le premier papier est intitulé, « On Codes over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$ », Journal of Applied Mathematics and Computing, 2017. Dans lequel, nous traitons les codes LCD est les codes formellement auto-duaux sur $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$, où $v^3 = v$, pour q impair. Nous avons donné des conditions sur l´existence des codes LCD et nous présentons la construction de codes formellement auto-duaux sur R. Nous donnons des borne sur la distance minimale des codes LCD sur $\mathbb{F}_q$ et nous avons étendu ces résultats aux codes sur R.

Le deuxième papier est intitulé « $\mathbb{Z}_q(\mathbb{Z}_q+u\mathbb{Z}_q)-$Linear Skew Constacyclic Codes », Journal of Algebra Combinatorics Discrete Structures and Applications. Dans lequel, nous avons étudions les codes tordus constacycliques sur l´anneau $\mathbb{Z}_qR$ où $R = \mathbb{Z}_q + u\mathbb{Z}_q$, $q = p^s$ pour un premier p et $u^2 = 0$. Nous donnons la définition de ces codes comme sous-ensembles de l´anneau $\mathbb{Z}_q^{\alpha}R^{\beta}$. Certaines propriétés structurales d´anneau polynomial tordus $R[x, \Theta]$ ont été discutées, où Θ est un automorphisme de R. Nous présenterons les polynomes générateurs de codes tordus constacycliques sur $\mathbb{Z}_qR$, nous déterminons leurs ensembles de enjambant minimales et leurs dimension. De plus, en utilisant les images Gray de codes tordus constacycliques sur $\mathbb{Z}_qR$, nous avons obtenu de nouveaux codes linéaires sur $\mathbb{Z}_4$. finalement, nous avons généralisé ces codes pour doubler les codes tordus constacycliques sur $\mathbb{Z}_qR$.

Le troisième travail que nous avons fait est intitulé, « Formally Self-dual Codes over A_k- », était présenté à la conférence CMA-2014 (Tlemcen). Dans ce travail, nous présentons Les différentes constructions des codes formellement auto-duaux sur l´anneau

$$A_k = \mathbb{F}_2 \left[v_1, \ldots, v_k\right] / \left\langle v_i^2 = v_i, v_iv_j = v_jv_i \right\rangle.$$

Le quatrième travail est intitulé, « LCD Codes over $\mathbb{F}_q+v\mathbb{F}_q+v^2\mathbb{F}_q$ », présenté à la conférence CMA-2016 (Batna). Dans ce travail, nous étudions les codes (LCD) sur l´anneau $R = \mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$, où $v^3 = v$, pour q impair.

Le cinquième travail est intitulé, « $\mathbb{Z}_q(\mathbb{Z}_q + v\mathbb{Z}_q + \ldots + v^{m-1}\mathbb{Z}_q)-$Linear Cyclic, Skew Cyclic and Constacyclic Codes », présenté à la conférence ECMI-SciTech'2017 (Constantine). Dans ce travail, nous étudions les codes cycliques, les codes tordus et les codes constacycliques sur l´anneau $\mathbb{Z}_q(\mathbb{Z}_q + v\mathbb{Z}_q + \ldots + v^{m-1}\mathbb{Z}_q)$, où $q = p^s$, p est un premier et $v^m = v$. Nous donnons la définition de ces codes comme sous-ensembles de l´anneau $\mathbb{Z}_q^{\alpha}R^{\beta}$.

Le sixième article était intitulé, " Double Skew $(1 + u)-$Constacyclic Codes over $\mathbb{Z}_4(\mathbb{Z}_4 + u\mathbb{Z}_4)$", IWCA-2019 (Oran). Dans ce travail, nous avons étudié les codes tordus constacyclicques sur l´anneau $\mathbb{Z}_4R$, où $R = \mathbb{Z}_4 + u\mathbb{Z}_4$, pour $u^2 = 0$. Nous avons donné la définition de ces codes comme des sous-ensembles de l´anneau $\mathbb{Z}_4^{\alpha}R^{\beta}$. De plus, nous avons généralisé ces codes pour les codes doublement tordus $(1 + u)-$constacycliques sur $\mathbb{Z}_4R$.

Mots Clés:

Code formellement auto-dual, code LCD, optimal code, Gray map, automorphism, code tordus constacycliques , anneau polynomial tordus , code doublement tordus constacycliques.

Notation

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

R =: finite rings.

w_L =: Lee weight.

LCD *codes* =: Linear codes with complementary dual.

$W_{n,k}$ =: Weighing matrix.

$\Theta(.)$ =: An automorphism.

$R[x, \Theta]$ =: Skew polynomial ring.

$Z(R[x, \Theta])$ =: Center of the ring $R[x, \Theta]$.

$\frac{R[x]}{\langle x^n - 1 \rangle}$ =: The quotient ring.

Contents

Introduction

The area of error-correcting codes allows the receiver to detect and correct error. Error-correcting codes are often based on algebra, arithmetic, geometry and the list is not exhaustive. We are on the bounds between computer science and mathematics.

The linear codes over finite rings are the subject of this thesis. Recently, this type of codes raised a great interest for their new role in algebraic coding theory and for their successful application in combined coding and modulation [**?**].

Linear codes with complementary dual (LCD) codes over finite fields were first studied by Massey [**?**], more recently by Carlet and Guilley [**?**] and Dougherty et al. [**?**]. LCD codes can be used to protect information against side channel attacks [**?**]. Formally self-dual codes are an important because they have weight enumerators that are invariant under the MacWilliams transform, and can have better parameters than self-dual codes [**?**].

Cyclic codes and their various generalizations such as constacyclic codes and quasi-cyclic (QC) codes have played a key role in this quest. One particularly useful generalization of cyclic codes has been the class of quasi-twisted (QT) codes that produced hundreds of new codes with best known parameters [**?**,**?**,**?**,**?**,**?**,**?**,**?**] recorded in the database [**?**]. Yet another generalization of cyclic codes, called skew cyclic codes, were introduced in [**?**] and they have been the subject of an increasing research activity over the past decade. This is due to their algebraic structure and their applications to DNA codes and quantum codes [**?**,**?**,**?**]. Skew constacyclic codes over various rings have been studied in [**?**,**?**,**?**,**?**,**?**,**?**,**?**,**?**,**?**,**?**] as a generalization of skew cyclic codes over finite fields.

Recently, P. Li et al. [**?**] gave the structure of $(1+u)$-constacyclic codes over the ring $\mathbb{Z}_2\mathbb{Z}_2[u]$

and Aydogdu et al. [?] studied $\mathbb{Z}_2\mathbb{Z}_2[u]$-cyclic and constacyclic codes. Further, Jitman et al. [?] considered the structure of skew constacyclic codes over finite chain rings. More recently A. Sharma and M. Bhaintwal studied skew cyclic codes over ring $\mathbb{Z}_4 + u\mathbb{Z}_4$, where $u^2 = 0$.

This thesis is organized as follows.

- In the first chapter we includes basic concepts and definitions of classical coding theory over finite rings, in particular, we give the preliminaries about linear codes over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$ and linear codes over $\mathbb{Z}_q + u\mathbb{Z}_q$.

- In the second chapter, we present several kinds of construction of formally self-dual codes over $A_k = \mathbb{F}_2 [v_1, \ldots, v_k] / \langle v_i^2 = v_i, v_i v_j = v_j v_i \rangle$.

- In the third chapter consider LCD codes over R. Necessary and sufficient conditions and the existence of LCD codes over R are given and LCD codes are constructed from weighting matrices. Tables of LCD codes up length 40 are given from skew matrices and conferences matrices over the fields $\mathbb{F}_p$ with p a prime number such that $3 < p \leq 23$. We present three constructions of formally self-dual over R. Further, LCD codes are constructed which are also formally self-dual codes. We give bounds on the minimum distance on LCD codes over the fields $\mathbb{F}_q$, hence we translate these bounds to the minimum distance of the free LCD codes over R.

- In the fourth chapter we give some results on skew constacyclic codes over the ring R. We study the algebraic structure of skew constacyclic codes over the ring $\mathbb{Z}_q R$, we includes the work on the generator polynomials of these codes, their minimal spanning sets and their sizes. Then we determine the Gray images of skew constacyclic codes over R and $\mathbb{Z}_q R$. These codes are then further generalized to double skew constacyclic codes in the next section. Finally, we use the Gray images of skew constacyclic codes over $\mathbb{Z}_q R$ to obtain some new linear codes over $\mathbb{Z}_4$.

- In the fifth chapter we give some basic results about the ring $R = \mathbb{Z}_q + u\mathbb{Z}_q$, where $q = p^s$, p is a prime and $u^2 = 0$ and linear codes over $\mathbb{Z}_q R$, we construct the non-commutative

ring $R[x, \Theta]$, where the structure of this ring depends on the elements of the commutative ring R and an automorphism Θ of R. We give some results on skew constacyclic codes over the ring R. Then we determine the Gray images of skew constacyclic codes over R and $\mathbb{Z}_q R$. These codes are then further generalized to double skew constacyclic codes in the next section. Finally, we use the Gray images of skew constacyclic codes over $\mathbb{Z}_q R$ to obtain some new linear codes over $\mathbb{Z}_4$.

- In the fifth chapter, we introduce and study the algebraic structure of cyclic, constacyclic codes and their duals over the $\Re-$module $\mathbb{Z}_q^{\alpha}\Re^{\beta}$, where $\Re = \mathbb{Z}_q + u\mathbb{Z}_q + \ldots + u^{m-1}\mathbb{Z}_q$ and $u^m = 0$. Moreover, we investigate the structure properties of cyclic polynomial ring $\mathbb{Z}_q\Re[x]$ and the set $\mathbb{Z}_q[x]/\langle x^{\alpha}-1\rangle \times \Re[x]/\langle x^{\beta}-1\rangle$ and constacyclic polynomial ring $\mathbb{Z}_q\Re[x]$ and the set $\mathbb{Z}_q[x]/\langle x^{\alpha}-1\rangle \times \Re[x]/\langle x^{\beta}-\lambda\rangle$.

Chapter 1

Preliminaries

1.1 Notions in ring theory

The class of finite rings is interesting as the first natural class of rings which allows to bring forth problems and conjectures, check validity and demonstrate the efficiency of results in general theory of rings.

In the last 20–30 years increased interest in possible application of finite rings, different from the fields, in coding theory and cryptography [**?**]. We have the following notions and result given in [**?**].

A ring is a set R with an operation called addition:

$$\text{for any } a, b \in R, \text{ there is an element } a + b \in R,$$

and another operation called multiplication:

$$\text{for any } a, b \in R, \text{ there is an element } ab \in R,$$

that satisfy the following conditions:

1. Addition is associative, i.e;

$$(a + b) + c = a + (b + c) \text{ for all } a, b, c \in R.$$

2. There is an element of R, called the zero element and written 0, which has the property that

$$a + 0 = 0 + a = a \text{ for all } a, b \in R.$$

3. Every element $a \in R$ has a negative, an element of R written $-a$, which satisfies

$$a + (-a) = (-a) + a = 0.$$

4. Addition is commutative, i.e;

$$a + b = b + a \text{ for all } a, b \in R.$$

5. Multiplication is associative, i.e;

$$(ab)c = a(bc) \text{ for all } a, b, c \in R.$$

6. Multiplication is distributive over addition, i.e;

$$a(b + c) = ab + ac \text{ and } (a + b)c = ac + bc \text{ for all } a, b, c \in R.$$

Let's start with some useful definitions:

Definition 1.1. *Let a, b be in a ring R.*

1. *If $a \neq 0$ and $b \neq 0$ such that $ab = 0$ or $ba = 0$, therefore we say that a and b are zero divisors.*

2. *If $ab = ba = 1$, therefore we say that a is a unit or that a is invertible.*

Definition 1.2. *A ring R is integral if and only if $R \neq \{0\}$ and is no zero divisor, in other words*

$$ab = 0 \Rightarrow (a = 0 \text{ or } b = 0).$$

Definition 1.3. *A field is a commutative ring in which every non-zero element is invertible.*

Example 1.1.
- *$\mathbb{Z}$ is an integral domain but not a field.*
- *The set*

$$\mathbb{Z}[i] = \{a + bi,\ a, b \in \mathbb{Z}\},$$

is an integral domain, but it is not a field.

Definition 1.4. *Let R be a ring. The characteristic of R denoted by $char(R)$, is the smallest non-negative n such that*

$$n \cdot 1_R = \underbrace{1_R + 1_R + \ldots + 1_R}_{n \text{ times}} = 0.$$

If no such n exists then we define the $char(R) = 0$.

Example 1.2.
- *The characteristic of $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ is 0.*
- *The characteristic of $\mathbb{Z}_p$ is p, for any prime p.*

1.1.1 Ring homomorphism

Definition 1.5. *A ring homomorphism $\Phi : R \longrightarrow R'$ is an application that preserves both operations of R, so for all $a, b \in R$:*

1. $\Phi(a + b) = \Phi(a) + \Phi(b)$
2. $\Phi(ab) = \Phi(a)\Phi(b)$
3. $\Phi(1_R) = 1_{R'}$.

Definition 1.6. *Let R and R' be rings and let $\Phi : R \longrightarrow R'$ be a ring homomorphism. Then Φ is a ring isomorphism if and only if Φ is a bijection.*

1.1.2 Ideal and quotient rings

Definition 1.7. *Let I be a subset of a ring R. Then an additive subgroup of R having the property that*

$$rx \in I \text{ for } r \in R, x \in I,$$

is called a left ideal of R.
On the other hand we have

$$xr \in I \text{ for } r \in R, x \in I,$$

is called a right ideal of R. If an ideal happens to be both a right and a left ideal, then we call it an ideal (or a two-sided ideals) of R.

Example 1.3.

- *$n\mathbb{Z} = \{kn; k \in \mathbb{Z}\}$ for any $n \in \mathbb{Z}$ is an ideal in $\mathbb{Z}$.*
- *In $\mathbb{Z}_6$, the set $I = \{2k \in \mathbb{Z}_6; k \in \mathbb{Z}\}$ is an ideal.*

Definition 1.8. *An ideal I in R is said proper if $I \neq R$.*

Definition 1.9. *Let R be a ring, and let I be an ideal. We define the quotient ring as :*

$$R/I = \{r + I : \ r \in R\}$$

1.1.3 Maximal and prime ideals

Definition 1.10. *Let R be a ring and I an ideal of R. The ideal I is a prime ideal of R for any $a, b \in R$, we have that*

$$ab \in I \Rightarrow a \in I \text{ or } b \in I$$

Example 1.4. *The prime ideals of $\mathbb{Z}$ are $\{0\}$ and the $n\mathbb{Z}$ for n prime.*

Theorem 1.1. *If I is an ideal in the commutative ring R, then I is a prime ideal if and only if R/I is an integral domain.*

Example 1.5. *$\mathbb{Z}/6\mathbb{Z}$ is not integral domain, since 6 is not prime.*

Corollary 1.1. *In a commutative ring, a maximal ideal is prime.*

Theorem 1.2. *Let R be a unitary commutative ring and let M be an ideal of R. Then the factor ring R/M is a field if and only if M is a maximal ideal of R*

Lemma 1.1. *(**Zorn's Lemma**) Every inductively ordered set has a maximal element.*

Corollary 1.2. *Every non-invertible element of R is contained in a maximal ideal.*

Definition 1.11. *(**Principal ideals**) An ideal I of a ring R is called principal if there is an element $a \in I$ such that $I = \langle a \rangle$, where*

$$I = \langle a \rangle = \{ar : r \in R\}.$$

In other words, the ideal is generated by the element a.

Example 1.6. $2\mathbb{Z} = \{0, \pm 2, \pm 4, \ldots, \}$ *is a principal ideal and is generated by 2.*

Definition 1.12. *(**local ring**) The ring R is local if and only if it has a unique maximal ideal.*

1.1.4 Finite chain ring

Definition 1.13. *A finite commutative ring with identity $1 \neq 0$ is called a finite chain ring if its ideals are linearly ordered by inclusion.*

A finite chain ring is also a principal ideal ring. If $\langle \gamma \rangle$ is the maximal ideal of the finite chain ring R, then $\langle \gamma \rangle$ is nilpotent with nilpotency index some integer e. The ideals of R form the following chain

$$0 = \langle \gamma^e \rangle \subsetneq \langle \gamma^{e-1} \rangle \subsetneq \ldots \subsetneq \langle \gamma \rangle \subsetneq R.$$

The nilradical of R is $\langle \gamma \rangle$.
Hence all the all the elements of $\langle \gamma \rangle$ are nilpotent. Then the elements of $R/\langle \gamma \rangle$ are units. Since $\langle \gamma \rangle$ is a maximal ideal, the residue ring $R/\langle \gamma \rangle$ is a field which we denote by K.
Consider the surjective ring morphism $(-)$:

$$\begin{array}{rcl} - : R & \to & K \\ a & \mapsto & \bar{a} = a \mod \gamma \end{array}$$

$|K| = q = p^r$ for a certain integer r, then

$$|R| = |K| \cdot |\langle\gamma\rangle| = |K| \cdot |K|^{e-1} = |K|^e = p^{er}.$$

1.1.5 Module

Let R be a commutative ring with unity.

Definition 1.14. *An $R-$module is an abelian group $(M, +)$ together with an action of R, i.e a map*

$$\begin{aligned} R \times M &\to M \\ (r, m) &\mapsto rm \end{aligned}$$

satisfying the following conditions:

1. *$r(m + n) = rm + rn$ for all $r \in R, m, n \in M$.*
2. *$(r + s)m = rm + sm$ for all $r, s \in R, m \in M$.*
3. *$(rs)m = r(sm)$ for all $r, s \in R, m \in M$.*
4. *For all $m \in M$ one has $1m = m$.*

If the ring R is a field K, an R-module is by definition exactly the same as an K-vector space.

Definition 1.15. *Let M be an $R-$module. A subset $N \subseteq M$ is said to be a submodule of M if:*

1. *N is a subgroup of $(M, +)$.*
2. *For all $r \in R$, and for all $m \in N$ one has $rm \in N$.*

1.1.6 Free module

Definition 1.16. *Let M be an $R-$module and let subset $N \subseteq M$. Then*

- *N is linearly independent, that is*

$$r_1x_1 + r_2x_2 + \ldots + r_nx_n = 0 \Rightarrow r_1 = r_2 = \ldots = r_n = 0,$$

  for $r_i \in R$ and distinct $x_1, x_2, \ldots, x_n \in N$.

- *N spans M if every $m \in M$ can be written as*

$$m = r_1x_1 + r_2x_2 + \ldots + r_nx_n,$$

  where $r_1, r_2, \ldots, r_n \in R$ and $x_1, x_2, \ldots, x_n \in N$.

- *N is a basis of M if M is linearly independent and N spans M.*

Definition 1.17. *Let N be a subset of an R-module M. If M has a nonempty basis N, then M is a free R-module on the set N.*

Example 1.7. *1. R-module R has the base $\{1\}$. Then R is a free $R-$module.*

2. The vector space $\mathbb{F}^n$ over a field $\mathbb{F}$ is a free F-module.

Proposition 1.3. *If M is a finitely generated free $R-$module, then the cardinality of any basis of M is finite. Furthermore, any two bases have the same cardinality.*

Definition 1.18. *Let M be a finitely generated free R-module. Then the cardinality of any basis of M is called the rank of the free module M.*

1.1.7 Frobenius rings

For algebraic coding theory, the most important class of ring is the class of Frobenius ring [**?**]. One of the most sinificant implications

Definition 1.19. *If R and R' are two rings, then an R-R'-bimodule is an abelian group $(M, +)$ such that:*

1. If M is a left R-module and a right R'-module.

2. For all $r \in R$, $r' \in R'$ and $m \in M$ we have:

$$(rm)r' = r(mr').$$

Let R be a unitary ring, the group characters of the additive group R is noted by $\widehat{R} = Hom_{\mathbb{Z}}(R, \mathbb{C}^{\times})$. This group has a structure of an $R-R-$bimodule defined by:

$$\chi^r(x) = \chi(rx),$$

for all $r, x \in R$, and $\chi \in \widehat{R}$.

Definition 1.20. *A finite ring R is called a Frobenius ring if ${}_R\widehat{R} =_R R$.*

We can see that if R is a finite Frobenius ring, then R and $\widehat{R}$ are isomorphic too.

1.1.8 Chinese remainder theorem

Let R be a commutative ring, and let $I_1, I_1, \ldots, I_n$ be ideals in R. The ideal $I_1 + I_2 + \ldots + I_n$ is the ideal formed of sums $a_1 + a_2 + \ldots + a_n$, where $a_i \in R$ for $i = 1, 2, \ldots, n$.

Definition 1.21. *1. We say that $I_1, I_2, \ldots, I_n$ are foreign if we have $I_1 + I_2 + \ldots + I_n = R$.*

2. We say that $I_1, I_2, \ldots, I_n$ are foreign in twos if I_i and I_j for all $i \neq j$.

Theorem 1.4. *Let $I_1, I_1, \ldots, I_n$ be ideals in R, such that*

$$I_i + I_j = R, \ i \neq j.$$

Then the morphism of ring

$$\varphi : R \to R/I_1 \oplus R/I_2 \oplus \ldots \oplus R/I_n$$

conclude isomorphism ring

$$R/I_1 \cap I_2 \cap \ldots \cap I_n \to \oplus_{i=0}^{n} R/I_i$$

1.1.9 Polynomial rings

Let R be a commutative ring with unity. The ring of polynomials over R is the ring $R[x]$. It defined to be the set of all formal sums

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0,$$

where $a_i \in R$ are called the coefficients of f.

For two polynomials $f(x) = \sum_i a_i x_i$ and $g(x) = \sum_i b_i x_i$

- their sum $(f+g)(x)$ is defined to be the polynomial

$$\sum_i (a_i + b_i)x_i.$$

- their product $(fg)(x)$ is the polynomial

$$(\sum_i a_i x_i)(\sum_i a_i x_i) = (\sum_i c_k x_k),$$

where $c_k = \sum_{k=i+j} a_i b_i$.

Definition 1.22. *Let R be an integral domain. Then the units in $R[x]$ are precisely the units in R.*

Theorem 1.5. ***(Division Algorithm)*** *Let $\mathbb{F}$ be a field, and let $f, g \in \mathbb{F}[x]$, where $g(x) \neq 0$. There*

$$f(x) = g(x)q(x) + r(x),$$

where $f, g \in \mathbb{F}[x]$, with $r(x) = 0$ or $\deg r(x) < \deg r(x)$.

1.2 Linear codes over finite rings

Definition 1.23. *Let R be a ring. A code over R of length n is subset C of R^n. If C is an $R-$submodule of R^n, then C is linear.*

The vectors of C are called the words of the code C.

Example 1.8. *Let C_1 be a code over $\mathbb{Z}_4^3$ such as*

$$C_1 = \{000, 121, 202, 323\},$$

then C_1 is linear because:

$$121 + 202 = 323 \in C_1$$

$$121 + 323 = 000 \in C_1$$

$$202 + 323 = 121 \in C_1$$

Let C_2 be a code over $\mathbb{Z}_4$ such as

$$C_2 = \{000, 011, 203\}$$

is non-linear because:

011 *and* $203 \in C_1$ *but* $011 + 203$ *is not in* C_2.

1.3 The parameters of a code defined over ring R

We define over R^n a metric, called **Hamming distance** denoted by $d_H(x, y)$ between two vector $x, y \in R^n$ is the number of coordinates which have different entries.

$$d_H(x, y) =\mid \{i : x_i \neq y_i\} \mid .$$

The Hamming weight a vector x is the number of its nonzero entries and is denoted by $w_H(x)$.

The minimum distance denoted by $d_{min}(C)$ of a code C defined over R is the smallest Hamming distance between any two code words of the code

$$d_{min}(C) = \{min\ d_H(x, y) | x, y \in C\}.$$

The minimum weight is the smallest of the weights of a non-zero code words. That is

$$w_{min}(x) = \{min\ w_H(x) | x \in C\}.$$

Lemma 1.2. *Let C be a linear code, then $d_{min}(C) = w_{min}(C)$.*

1.4 Codes over some rings

1.4.1 Linear codes over the ring $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$

In this subsection, we present some basic results on linear codes over the ring $R = \mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$, where $v^3 = v$ and q odd [**?**, **?**]. The ring R is equivalent to the ring $\frac{\mathbb{F}_q[v]}{\langle v^3 - v\rangle}$. This shows that R is a finite commutative, principal ring with the following non-trivial maximal ideals

$$\langle v\rangle,\ \langle 1 - v\rangle,\ \langle 1 + v\rangle.$$

Hence by the Chinese remainder theorem we have

$$R = R/\langle v\rangle \oplus R/\langle 1 - v\rangle \oplus R/\langle 1 + v\rangle. \tag{1.1}$$

It is convenient to write the decomposition given in (**??**) using orthogonal idempotents R which is given by

$$R = \eta_1 R \oplus \eta_2 R \oplus \eta_3 R = \eta_1\mathbb{F}_q \oplus \eta_2\mathbb{F}_q \oplus \eta_3\mathbb{F}_q, \tag{1.2}$$

where $\eta_1 = 1 - v^2$, $\eta_2 = \frac{v+v^2}{2}$, $\eta_3 = \frac{v^2-v}{2}$.

Each element x of R can be expressed uniquely as

$$x = a_0 + va_1 + v^2a_2,$$

where $a_i \in \mathbb{F}_q, i = 0, 1, 2$.

A linear code C of length n over R is an R-submodule of R^n. An element of C is called a codeword of C. A generator matrix of C is a matrix whose rows generate C. The Hamming weight $w_H(c)$ of a codeword c is the number of nonzero components in c. The Euclidean inner product is

$$\langle x, y\rangle = x_0y_0 + x_1y_1 + \ldots + x_{n-1}y_{n-1},$$

where $x, y \in R^n$. The dual code $C^\perp$ of C with respect to the Euclidean inner product is defined as

$$C^\perp = \{x \in R^n;\ \langle x, y\rangle = 0, \forall y \in C\}.$$

A code C is self-dual if $C = C^{\perp}$ and C is self-orthogonal if $C \subseteq C^{\perp}$.

For a linear C code of length n over R, define

$$\begin{aligned} C_1 &= \left\{a \in \mathbb{F}_q^n;\ \exists b, c \in \mathbb{F}_q^n;\ \eta_1 a + \eta_2 b + \eta_3 c \in C\right\}, \\ C_2 &= \left\{b \in \mathbb{F}_q^n;\ \exists a, c \in \mathbb{F}_q^n;\ \eta_1 a + \eta_2 b + \eta_3 c \in C\right\}, \\ C_3 &= \left\{c \in \mathbb{F}_q^n;\ \exists a, b \in \mathbb{F}_q^n;\ \eta_1 a + \eta_2 b + \eta_3 c \in C\right\}. \end{aligned}$$

It is clear that C_1, C_2 and C_3 are linear codes of length n over $\mathbb{F}_q$. A direct consequence of the ring decomposition of R in (**??**) is that a linear code C over R can be uniquely expressed as

$$C = \eta_1 C_1 \oplus \eta_2 C_2 \oplus \eta_3 C_3. \tag{1.3}$$

Moreover, from (**??**) and the definition of the dual code we have that

$$C^{\perp} = \eta_1 C_1^{\perp} \oplus \eta_2 C_2^{\perp} \oplus \eta_3 C_3^{\perp}. \tag{1.4}$$

Further, C is self-dual if and only if C_1, C_2, and C_3 are self-dual over $\mathbb{F}_q$. If G_1, G_2 and G_3 are generator matrices of C_1, C_2 and C_3, respectively, then

$$G = \begin{bmatrix} \eta_1 G_1 \\ \eta_2 G_2 \\ \eta_3 G_3 \end{bmatrix}, \tag{1.5}$$

is a generator matrix of C. Often when working with codes over rings, an image to the underlying field is employed. For the ring R considered a Gray map is defined as follows.

Definition 1.24. *The Gray map Ψ from R^n to $\mathbb{F}_q^{3n}$ is defined by*

$$\Psi : R^n \to \mathbb{F}_q^{3n}$$
$$(r_0, r_1, \ldots, r_{n-1}) \mapsto (a_0, a_0 + b_0 + c_0, a_0 - b_0 + c_0, \ldots, a_{n-1} + b_{n-1} + c_{n-1}, a_{n-1} - b_{n-1} + c_{n-1}),$$

where $r_i = a_i + vb_i + v^2 c_i, i = 0, 1, \ldots, n-1$.

For $r = a + vb + v^2 c$ in R, the Lee weight of r is defined as

$$w_L(a + vb + v^2 c) = w_H(a, a + b + c, a - b + c),$$

where w_H denotes the Hamming weight of v over $\mathbb{F}_q$. Let d_H denotes the minimum Hamming distance of a code C. For a codeword $c = (c_0, c_1, \ldots, c_{n-1})$, the Lee weight is defined as $w_L(c) = \sum_{i=0}^{n-1} w_L(c_i)$ and the Lee distance between codewords c and c' is defined as $d_L(c, c') = w_L(c - c')$. The minimum Lee distance for a code C is then $d_L(C) = \min d_L(c, c')$, $c \neq c'$, $\forall c, c' \in C$.

Definition 1.25. *A linear code C of length n over R and minimum Lee distance d_L is called an $[n, |C|, d]_R$ code. Further if it is with minimum Hamming distance d_H, then it is denoted $[n, |C|, d_H]_R$. If C has minimum Lee distance d_L and is free $R-$ submodule that is isomorphic as a module to R^k, then the integer k is called the rank of C and the code is denoted as $[n, k, d_L]_R$.*

Proposition 1.6. *[?] Let C be an $[n, |C|, d_L]_R$ code. Then $\Psi(C)$ is a $[3n, k, d = d_L]$ linear code over $\mathbb{F}_q$. Further, if $C^\perp$ is the dual of C, then $\Psi(C)^\perp = \Psi\left(C^\perp\right)$.*

Remark 1.1. *If there exists an $[n, k, d_H]$ code C over $\mathbb{F}_q$, then there exists a $[3n, k, d_H]_R$ code $\mathcal{C} = \eta_1 C \oplus \eta_2 C \oplus \eta_3 C$.*

Lemma 1.3. *If C is a linear code of length n over R with generator matrix G, then*

$$\Psi(G) = \begin{bmatrix} \Psi(\eta_1 G_1) \\ \Psi(\eta_2 G_2) \\ \Psi(\eta_3 G_3) \end{bmatrix} = \begin{bmatrix} G_1 & 0 & 0 \\ 0 & G_2 & 0 \\ 0 & 0 & G_3 \end{bmatrix}, \tag{1.6}$$

and $d_H(\Psi(C)) = \min\{d_H(C_1), d_H(C_2), d_H(C_3)\}$.

Cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$

We now give some useful results on cyclic codes over R. A code C is said to be cyclic if it satisfies

$$(c_{n-1}, c_0, \ldots, c_{n-2}) \in C, \text{ whenever } (c_0, c_1, \ldots, c_{n-1}) \in C.$$

It is well known that cyclic codes of length n over R can be considered ideals in the quotient ring $\frac{R[x]}{\langle x^n - 1 \rangle}$ via the following R-module isomorphism

$$\begin{array}{ccc} R^n & \to & R[x]/\langle x^n - 1 \rangle \\ (c_0, c_1, \ldots, c_{n-1}) & \mapsto & c_0 + c_1 x + \ldots + c_{n-1} x^{n-1} \end{array}$$

Definition 1.26. *The reciprocal of the polynomial* $h(x) = h_0 + h_x x + \ldots + h_k x^k$ *is defined as*

$$h^*(x) = x^{deg(h(x)}h(x^{-1}).$$

If $h(x) = h^*(x)$*, then the polynomial* $h(x)$ *is called self-reciprocal.*

Proposition 1.7. *[?] Let* C *be a cyclic code of length* n *over* R*. Then there exist polynomials* $f_i(x)$ *which are divisors of* $x^n - 1$ *in* $\mathbb{F}_q[x]$ *such that* $C = \langle \eta_1 f_1(x), \eta_2 f_2(x), \eta_3 f_3(x) \rangle$ *and* $|C| = q^{3n-deg(f_1(x)+f_2(x)+f_3(x))}$*. Further*

$$C^{\perp} = \langle \eta_1 h_1^*(x), \eta_2 h_2^*(x), \eta_3 h_3^* \rangle,$$

where $h_i(x) \in \mathbb{F}_q[x]$ *such that* $x^n - 1 = f_1(x)h_1(x) = f_2(x)h_2(x) = f_3(x)h_3(x)$*.*

Definition 1.27. *Let* C *be a linear code of length* n *over* $\mathbb{F}_q$ *and* $(c_0, c_1, \ldots, c_{n-1}) = (c^1|c^2|\ldots|c^l)$ *be a codeword in* C *divided into* l *equal parts of length* m *where* $n = ml$*. If* $\varphi_l = (\sigma(c^1)|\sigma(c^2)|\ldots|\sigma(c^l)) \in C$*, where* φ *is the usual cyclic shift of* C*, then the linear code* C *which is permutation equivalent to* C *is called a quasi-cyclic code of index* l*.*

Proposition 1.8. *If* C *is a cyclic code of length* n *over* R*, then* $\Psi(C)$ *is a* 3*-quasi cyclic code of length* $3n$ *over* $\mathbb{F}_q$*.*

Proof. The result follows from Definition **??** and the definition of the Gray map Ψ. □

Corollary 1.3. *There is no cyclic self-dual cyclic code of length* n *over* R*.*

Proof. We know that $C = \eta_1 C_1 \oplus \eta_2 C_2 \oplus \eta_3 C_3$. From [**?**, Theorem 1] we have that C_1, C_2 and C_3 are self-dual cyclic code over $\mathbb{F}_q$ if and only if q is power of 2 and n is even. Since we assumed that q is odd, the result follows. □

1.4.2 Linear codes over the ring $\mathbb{Z}_q + u\mathbb{Z}_q$

Consider the ring $R = \mathbb{Z}_q + u\mathbb{Z}_q$, where $q = p^s$, p is a prime and $u^2 = 0$. The ring R is isomorphic to the quotient ring $\mathbb{Z}_q[u]/\langle u^2 \rangle$. The ring R is not a chain ring, whereas it is a local ring with the maximal ideal $\langle u, p \rangle$. But R is not principal since the ideal $\langle p, u \rangle$ can not

be generated by any single element of this ideal [**?**]. Each element r of R can be expressed uniquely as

$$r = a + ub, \text{ where } a, b \in \mathbb{Z}_q.$$

The ideals of R are of the following forms [**?**]

1. $\langle p^i \rangle$ for $0 \leq i \leq s$,
2. $\left\langle p^k u \right\rangle$ for $0 \leq i \leq s-1$,
3. $\langle p^j + u \rangle$ for $1 \leq i \leq s-1$,
4. $\langle p^j, u \rangle$ for $1 \leq i \leq s-1$.

Lemma 1.4. *Let $R = \mathbb{Z}_q + u\mathbb{Z}_q$, where $\mathbb{Z}_q$ is a subring of R. Then an element $\lambda \in R$ is unit in $\mathbb{Z}_q$ if and only if λ is unit in R.*

Proof. Assume that $\lambda = \alpha$ is unit in R where $\alpha \in \mathbb{Z}_q$. Then there exists an element $\beta = \beta_1 \in R$ such that $\lambda.\beta = 1$ so $\alpha.\beta_1 = 1$ which implies that $\alpha \neq 0$, so α is unit in $\mathbb{Z}_q$. Conversely, suppose that α is unit in $\mathbb{Z}_q$ and we will prove that λ is unit in R. then, let $\lambda^{-1} = \alpha^{-1}$. Since α is unit in $\mathbb{Z}_q$ then $\alpha\alpha^{-1} = 1$, thus $\lambda\lambda^{-1} = 1$. This implies that λ is unit in R. □

For a linear code C_β of length β over R, its torsion $Tor(C_\beta)$ and residue $Res(C_\beta)$ codes are codes over $\mathbb{Z}_q$, defined as follows

$$Tor(C_\beta) = \{b \in \mathbb{Z}_q^\beta : ub \in C_\beta\}$$

and

$$Res(C_\beta) = \{a \in \mathbb{Z}_q^\beta : a + ub \in C_\beta \text{ for some } b \in \mathbb{Z}_q^\beta\}.$$

Definition 1.28. *A linear code C_β of length β over the ring $\mathbb{Z}_q + u\mathbb{Z}_q$ is $\mathbb{Z}_q + u\mathbb{Z}_q-$submodule of $(\mathbb{Z}_q + u\mathbb{Z}_q)^\beta$.*

The dual of linear codes over $\mathbb{Z}_q + u\mathbb{Z}_q$

We introduce an inner product on $(\mathbb{Z}_q + u\mathbb{Z}_q)^\beta$. Further, the Euclidean inner product defined by

$$\langle v', w' \rangle = \sum_{i=0}^{\beta-1} v'_i w'_i,$$

for $v' = (v'_0, v'_1, \ldots, v'_{\beta-1})$ and $w' = (w'_0, w'_1, \ldots, w'_{\beta-1})$ in R^β.

Definition 1.29. *Let C_β be a linear code over R of length β. then we define the dual of C_β as*

$$C_\beta^\perp = \{v' \in R^n; \langle v', w' \rangle = 0, \forall w' \in C\}.$$

Note that from the definition of the Euclidean inner product, $C^\perp$ is also a linear code over R of length β.

Chapter 2

Formally self-dual codes over A_k

Binary formally self-dual codes have been extensively studied. For results on these codes, we refer the reader to [**?**,**?**]. A code is called isodual if C is equivalent to $C^{\perp}$, and is called formally self-dual if C and $C^{\perp}$ have the same weight enumerator. In this chapter we present several kinds of construction formally self-dual codes over $A_k = \mathbb{F}_2[v_1, \ldots, v_k] / \langle v_i^2 = v_i, v_i v_j = v_j v_i \rangle$. Apart of this chapter already appeared in [**?**].

2.1 Linear codes over the ring A_k

We begin by defining the finite commutative ring A_k and codes over these ring. The following results are analogous to the ones obtained in [**?**], [**?**], [**?**] for the ring A_k.

The rings are defined as follows.
For integers $k \geqslant 1$, let $A_k = \mathbb{F}_2[v_1, \ldots, v_k] / \langle v_i^2 = v_i, v_i v_j = v_j v_i \rangle$. For example

- For $k = 1$, $A_1 = \mathbb{F}_2[v_1] / \langle v_1^2 = v_1 \rangle$.
- For $k = 2$, $A_2 = \mathbb{F}_2[v_1, v_2] / \langle v_1^2 = v_1, v_1 v_2 = v_2 v_1 \rangle$.

Lemma 2.1. *The ring A_k has characteristic 2 and cardinality 2^{2^k}. The only unit in the ring A_k is 1.*

The ring A_k is not local ring with maximal ideal $\langle w_1, \ldots, w_n \rangle$, where $w_i \in \{v_i, 1 + v_i\}$ of cardinality 2^{2^k-1}.

2.1.1 Gray map

From [?], [?] we define the Gray map is deductively extending it from the Gray map on A_k as follows:

- for $k = 1$ the Gray map is defined as

$$\phi_1 : A_1 \to \mathbb{F}_2^2$$
$$a + bv_1 \mapsto \phi_1(a + bv_1) = (a, a + b)$$

  For A_1 this is realized as

$$0 \to 00$$

$$1 \to 11$$

$$v \to 01$$

$$1 + v \to 10.$$

- We extend this map inductively as follows. For $k \geq 2$ the Gray map is defined as

$$\phi_k : A_k \to A_{k-1}^2$$
$$\alpha + \beta v_k \mapsto \phi_k(\alpha + \beta v_k) = (\alpha, \alpha + \beta),$$

  where $\alpha, \beta \in A_{k-1}$

Then define

$$\Phi_k : A_k \to \mathbb{F}_2^{2^k}$$

by

$$\Phi_1(\gamma) = \phi_1(\gamma),$$

$$\Phi_2(\gamma) = \phi_1(\phi_2(\gamma))$$

and

$$\Phi_k(\gamma) = \phi_1(\phi_2(\ldots(\phi_{k-2}(\phi_{k-1}(\gamma))\ldots).$$

2.1.2 Dual codes over A_k

We begin with the following definitions. In the space A_k^n, with $w, v \in A_k^n$, we attach the standard Euclidean inner-product:

$$v.w = \sum v_i w_i,$$

and define

$$C^{\perp} = \{v;\ v.w = 0 \text{ for all } w \in C\}.$$

A code is called self-dual if $C = C^{\perp}$. It is called isodual if C is equivalent to $C^{\perp}$.
The Hamming weight enumerator $wt_C(x, y)$, define by

$$wt_C(x, y) = \sum_{v \in C} x^{n-wt(v)} y^{wt(v)},$$

where $wt\,(v)$ is the number of non-zero coordinates of v. The code C is called formally self-dual if $w_C\,(x, y) = w_{C^{\perp}}(x, y)$.
Since the ring A_k is a Frobenius ring, we have

$$\mid C \mid\mid C^{\perp} \mid = \mid A_k^n \mid .$$

2.2 Different constructions of formally self-dual codes over A_k

In this section, we present three constructions of formally self-dual codes over the finite ring $A_k = \mathbb{F}_2\,[v_1, \ldots, v_k]\,/\,\langle v_i^2 = v_i, v_i v_j = v_j v_i\rangle$.

Theorem 2.1. *[?, Theorem 1] If C is a formally self-dual code over A_k, then the image under the corresponding Gray map is a binary formally self-dual code.*

The proof of the next theorems is the same as that for [?, Theorem 3.1] given over R_k.

Theorem 2.2. *Let M be an $n \times n$ matrix over A_k such $M^t = M$. Then the code generated $G = [I_n \,|\, M]$ is an isodual code and hence a formally self-dual code of length $2n$.*

Proof. Let the matrix

$$G = [I_n \,|\, M]$$

$$G = \left[\begin{array}{c|cccc} & M_{11} & M_{12} & \dots & M_{1n} \\ & M_{21} & M_{22} & \dots & M_{2n} \\ I_n & & & \ddots & \\ & & & & \\ & M_{n1} & M_{n2} & \dots & M_{nn} \end{array}\right].$$

This is a matrix of type $2n \times n$. Consider the following matrix

$$G' = \left[\begin{array}{cccc|c} M_{11} & M_{21} & \dots & M_{n1} & \\ M_{12} & M_{22} & \dots & M_{n2} & \\ & & \ddots & & I_n \\ & & & & \\ M_{1n} & M_{2n} & \dots & M_{nn} & \end{array}\right].$$

G and G' generate codes with free rank $k \times n$. We need to show that $C' = C^{\perp}$. Let u the $i-th$ row of G and $j-th$ row of G'. Since A_k has characteristic 2 and $M^t = M$, then we have $\langle u, v \rangle_k = M_{ij} + M_{ji} = 0$. There for $C' = C^{\perp}$ and C is equivalent to $C^{\perp}$. □

Example 2.1. *Let $k = 1$ and $n = 2$, and let the matrix*

$$M = \left[\begin{array}{cc} 1 & v \\ v & 1 \end{array}\right].$$

We have $M = M^t$. Then

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

generates a formally self-dual code of length 4 over A_1.

Example 2.2. *Let $k = 2$ and $n = 3$ and let the matrix*

$$M = \begin{bmatrix} 1 & v_1 & 1+v_1 \\ v_1 & v_2 & v_1v_2 \\ 1+v_1 & v_1v_2 & 1+v_1v_2 \end{bmatrix}.$$

We have $M = M^t$. Then

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & v_1 & 1+v_1 \\ 0 & 1 & 0 & v_1 & v_2 & v_1v_2 \\ 0 & 0 & 1 & 1+v_1 & v_1v_2 & 1+v_1v_2 \end{bmatrix}$$

generates a formally self-dual code of length 6 over A_2.

An $n \times n$ square matrix M is called circulant if it is in the following form

$$M = \begin{bmatrix} M_{11} & M_{12} & M_{13} & \dots & M_{1n} \\ M_{1n} & M_{11} & M_{12} & \dots & M_{1n-1} \\ M_{1n-1} & M_{1n} & M_{11} & \dots & M_{1n-2} \\ \vdots & \vdots & \vdots & \vdots & \\ M_{12} & M_{13} & M_{14} & \dots & M_{11} \end{bmatrix}.$$

Theorem 2.3. *Let M be a circulant matrix over A_k of order n. Then $G = [I_n \,|\, M]$ generates an isodual code and hence a formally self- dual code over A_k.*

Proof. Consider

$$M = \begin{bmatrix} M_{11} & M_{12} & \dots & M_{1n} \\ M_{1n} & M_{11} & \dots & M_{1n-1} \\ & & \ddots & \\ M_{12} & M_{13} & \dots & M_{11} \end{bmatrix}$$

the circulant matrix over A_k of $n \times n$. Let C be the code generated by

$$G = [I_n \,|\, M]$$

$$G = \left[\begin{array}{c|cccc} & M_{11} & M_{12} & \dots & M_{1n} \\ I_n & M_{1n} & M_{11} & \dots & M_{1n-1} \\ & & & \ddots & \\ & M_{12} & M_{13} & \dots & M_{11} \end{array}\right]$$

of $2n \times n$. And C' generated by

$$G' = \left[\begin{array}{cccc|c} M_{11} & M_{1n} & \dots & M_{12} & \\ M_{12} & M_{11} & \dots & M_{13} & \\ & & \ddots & & I_n \\ M_{1n} & M_{1n-1} & \dots & M_{11} & \end{array}\right]$$

of $2n \times n$. Let v be the $i-th$ row of G, and let w be the $j-th$ row of G'. Then $\langle v, w \rangle_k = M_{ij} + M_{ij} = 0$. Since the ring A_k has characteristic 2 and, therefore C' and $C^{\perp}$ are orthogonal. Since they both have rank n, then $C' = C^{\perp}$. We show that C is equivalent to C'. Let σ be the permutation of rows such that after applying it to G', the first column of $\sigma(M^t)$ is the same as the first column of M. For every column of M is then equal to a column of $\sigma(M^t)$,

for the matrix M is circulant. So that $\tau(\sigma(M^t)) = M$, when τ apply the necessary column permutation. We apply another column permutation ρ so that $\sigma(I_n) = I_n$. We obtain that that C and C' are equivalent and therefore C is formally self-dual. □

As straight formal result from theorem and definition we obtain that, If C is a linear code over A_k of length $2n$, generated by $[I_n \,|\, M]$, where M is a circulant matrix, then $\phi_k(C)$ is a binary formally self-dual code of length $2^{k+1}n$.

Example 2.3. *Consider* $v = (1, 1 + v_1v_2, v_2, v_1, v_1 + v_2)$ *the first row of the matrix circulant*

$$M = \begin{bmatrix} 1 & 1+v_1v_2 & v_2 & v_1 & v_1+v_2 \\ v_1+v_2 & 1 & 1+v_1v_2 & v_2 & v_1 \\ v_1 & v_1+v_2 & 1 & 1+v_1v_2 & v_2 \\ v_2 & v_1 & v_1+v_2 & 1 & 1+v_1v_2 \\ 1+v_1v_2 & v_2 & v_1 & v_1+v_2 & 1 \end{bmatrix}$$

And let

$$G = \left[\begin{array}{c|ccccc} & 1 & 1+v_1v_2 & v_2 & v_1 & v_1+v_2 \\ & v_1+v_2 & 1 & 1+v_1v_2 & v_2 & v_1 \\ I_5 & v_1 & v_1+v_2 & 1 & 1+v_1v_2 & v_2 \\ & v_2 & v_1 & v_1+v_2 & 1 & 1+v_1v_2 \\ & 1+v_1v_2 & v_2 & v_1 & v_1+v_2 & 1 \end{array}\right]$$

the generator matrix of C*. And let*

$$G' = \left[\begin{array}{ccccc|c} 1 & v_1+v_2 & v_1 & v_2 & 1+v_1v_2 & \\ 1+v_1v_2 & 1 & v_1+v_2 & v_1 & v_2 & \\ v_2 & 1+v_1v_2 & 1 & v_1+v_2 & v_1 & I_5 \\ v_1 & v_2 & 1+v_1v_2 & 1 & v_1+v_2 & \\ v_1+v_2 & v_1 & v_2 & 1+v_1v_2 & 1 & \end{array}\right]$$

the generator matrix of C'. It is easy to see that G' generates $C^\perp$, and C is equivalent to $C' = C^\perp$ hence the codes are isodual.

Theorem 2.4. *Let M be a circulant matrix over A_k of order $n-1$. Then the matrix*

$$G = \left[\begin{array}{c|ccc} & \alpha & \omega & \ldots & \omega \\ & \omega & & & \\ I_n & \vdots & & M & \\ & \omega & & & \end{array}\right],$$

where $\alpha, \omega \in A_k$, is generator matrix of a formally self-dual code over A_k.

Proof. Let

$$M = \begin{bmatrix} M_{11} & M_{12} & \ldots & M_{1n-1} \\ M_{1n-1} & M_{11} & \ldots & M_{1n-2} \\ & & \ddots & \\ M_{12} & M_{13} & \ldots & M_{11} \end{bmatrix},$$

a circulant matrix over A_k of order $n-1$. We have

$$G = \left[\begin{array}{c|cccc} & \alpha & \omega & \dots & \omega \\ & \omega & M_{11} & \dots & M_{1n-1} \\ I_n & & & & \ddots \\ & \omega & M_{12} & \dots & M_{11} \end{array}\right],$$

where $\alpha, \omega \in A_k$.

And let G' be given as

$$G' = \left[\begin{array}{cccc|c} \alpha & \omega & \dots & \omega & \\ \omega & M_{11} & \dots & M_{12} & \\ & & \ddots & & I_n \\ \omega & M_{1n-1} & \dots & M_{11} & \end{array}\right]$$

Let $C = \langle G \rangle$ and $C' = \langle G' \rangle$. Both C and C' are codes of free rank n. Let v be the first row of G and w be the first row of G'. Then $\langle u, w \rangle_k = \alpha + \alpha = 0$. Let v be the first row of G, and let w be the $j-th$ row of G'. We have $\langle u, w \rangle_k = \omega + \omega = 0$. Let v be the $i-th$ row of G, and let w be the $j-th$ row of G'. We have $\langle u, w \rangle_k = M_{ij} + M_{ij} = 0$. Hence we have $C' = C^{\perp}$. We see that C and C' will have same weight enumerator. Hence C and $C^{\perp}$ have the same weight enumerators. □

Example 2.4. *Let $n = 3$, $\alpha = 1 + v_1$, $w = 1 + v_2$ and*

$$M = \begin{bmatrix} 1 & 1 + v_1 v_2 \\ v_1 + v_2 & 1 \end{bmatrix}$$

Then

$$G = \begin{bmatrix} 1 & 0 & 0 & 1+v_1 & 1+v_2 & 1+v_2 \\ 0 & 1 & 0 & 1+v_2 & 1 & 1+v_1v_2 \\ 0 & 0 & 1 & 1+v_2 & v_1+v_2 & 1 \end{bmatrix}$$

generates a formally self dual code.

Chapter 3

On codes over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$

In this chapter, we consider LCD and formally self-dual codes over the ring $R = \mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$, where $v^3 = v$ and q is an odd prime power. We give conditions on the existence of LCD codes over this ring. Further, several constructions of LCD codes are given, in particular from weighing matrices. Constructions of formally self-dual codes over R are also presented. In addition, bounds on the minimum distance of LCD codes over $\mathbb{F}_q$ are given and extended to codes over R. LCD codes and formally self-dual codes are of practical as well as theoretical interest. For example, LCD codes over $\mathbb{F}_q$ can easily be decoded [**?**], and this property also applies to LCD codes over R because this ring can be seen as the direct product $\mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q$. Further, LCD codes can be used to obtain optimal entanglement-assisted quantum codes [**?**]. Apart of this chapter already appeared in [**?**].

3.1 LCD codes over R

A linear codes with complementary dual (LCD) code is defined as a linear code C whose dual code $C^\perp$ satisfies

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

LCD codes have been shown to provide an optimum linear coding solution [**?**].

For LCD codes over R, we have the following result.

Theorem 3.1. *A code $C = \eta_1 C_1 \oplus \eta_2 C_2 \oplus \eta_3 C_3$ of length n over R is an LCD code if and only if C_1, C_2 and C_3 are LCD codes over $\mathbb{F}_q$.*

Proof. A linear code $C = \eta_1 C_1 \oplus \eta_2 C_2 \oplus \eta_3 C_3$ has dual code $C^\perp = \eta_1 C_1^\perp \oplus \eta_2 C_2^\perp \oplus \eta_3 C_3^\perp$. We have that

$$C \cap C^\perp = \eta_1(C_1 \cap C_1^\perp) + \eta_2(C_2 \cap C_2^\perp) + \eta_3(C_3 \cap C_3^\perp).$$

Due to the direct sum we have

$$C \cap C^\perp = \{0\}$$

if and only if

$$C_i \cap C_i^\perp = \{0\},$$

for $i = 1, 2, 3$. Thus C is an LCD code. □

Theorem 3.2. *If C is an LCD code over $\mathbb{F}_q$, then $\mathcal{C} = \eta_1 C \oplus \eta_2 C \oplus \eta_3 C$ is an LCD code over R. If C is an LCD code of length n over R, then $\Psi(C)$ is an LCD code of length $3n$ over $\mathbb{F}_q$.*

Proof. The first part is deduced from Theorem **??**. From Proposition **??** we have that $\Psi\left(C\right)^\perp = \Psi(C^\perp)$. Since Ψ is bijective and $C \cap C^\perp = \{0\}$, the result follows. □

We next give a necessary and sufficient condition on the existence of LCD codes over R. First we require the following result due to Massey [**?**].

Proposition 3.3. *If G is a generator matrix for an $[n, k]$ linear code C over $\mathbb{F}_q$, then C is an LCD code if and only if the $k \times k$ matrix GG^t is nonsingular.*

Theorem 3.4. *If G is a generator matrix for a linear code C over R, then C is an LCD code if and only if GG^t is nonsingular.*

Proof. The generator matrix of C can be expressed in canonical form as

$$G = \begin{bmatrix} \eta_1 G_1 \\ \eta_2 G_2 \\ \eta_3 G_3 \end{bmatrix}. \tag{3.1}$$

Since the η_i are orthogonal idempotents, a simple calculation gives

$$GG^t = \begin{bmatrix} \eta_1 G_1 G_1^t & 0 & 0 \\ 0 & \eta_2 G_2 G_2^t & 0 \\ 0 & 0 & \eta_3 G_3 G_3^t. \end{bmatrix}. \tag{3.2}$$

From Proposition **??** a necessary and sufficient condition for a code over $\mathbb{F}_q$ with generator matrix G_i to be LCD is that $G_i G_i^t$ be non singular. Hence the proof follows from the generator matrix given in (**??**). □

We now give conditions on the existence of cyclic LCD codes over R using the generator polynomial. This is an extension of the following result due to Massey [**?**].

Lemma 3.1. *Let C be a cyclic code over $\mathbb{F}_q$ generated by $f(x)$, then C is LCD if and only if $f(x)$ is self-reciprocal.*

Theorem 3.5. *A cyclic code $C = \langle \eta_1 f_1(x), \eta_2 f_2(x), \eta_3 f_3(x) \rangle$ is an LCD code over R if and only if for all $1 \leq i \leq 3$, $f_i(x)$ is a self-reciprocal polynomial.*

Proof. The result follow from Proposition **??** and Lemma **??**. □

3.1.1 Existence of LCD codes over R

In this section, we show that the class of LCD codes are is an abundant class of codes over R.

3.1.2 LCD codes from Weighing Matrices

In [**?**], the authors constructed LCD codes from orthogonal matrices and left the existence of LCD codes from other classes of combinatorial objects as an open problem. Thus, in this section we construct LCD codes over $\mathbb{F}_q$ and R from weighing matrices.
We start with the following definition.

Definition 3.1. *A weighing matrix $W_{n,k}$ of order n and weight k is an $n \times n$ $(0, 1, -1)$-matrix such that $WW^t = kI_n$; $k \leq n$. A weighing matrix $W_{n,n}$, respectively $W_{n,n-1}$, is called a Hadamard matrix, respectively conference matrix. A matrix W is symmetric if $W = W^t$. A matrix W is skew-symmetric (or skew) if $W = -W^t$.*

Tables of weighing matrices are given in [**?**]. Weighing matrices have been used to construct self-dual codes [**?**]. The following results show that it is also possible to construct LCD codes from weighing matrices.

Proposition 3.6. *Let $W_{n,k}$ be a weighing matrix of order n and weight k. We have the following results.*

(i) let α be a nonzero element of $\mathbb{F}_q$ such that $\alpha^2 + k \neq 0 \bmod q$. Then the matrix

$$G = [\alpha I_n \mid W_{n,k}] \tag{3.3}$$

generates an LCD $[2n, n]$ code over $\mathbb{F}_q$.

(ii) Let $W_{n,k}$ be a skew weighing matrix of order n, and α and β nonzero elements of $\mathbb{F}_q$ such that $\alpha^2 + \beta^2 + k \neq 0 \bmod q$. Then the matrix

$$G = [\alpha I_n \mid \beta I_n + W_{n,k}] \tag{3.4}$$

generates a $[2n, n]$ LCD code over $\mathbb{F}_q$.

Proof. The result follows from Definition **??** and Proposition **??**. □

Hence from Remark **??** and Proposition **??** we have the following result.

Corollary 3.1. *Under the condition of Proposition* **??** *the following matrix*

$$\mathcal{G} = \begin{bmatrix} \eta_1 G \\ \eta_2 G \\ \eta_3 G \end{bmatrix}, \tag{3.5}$$

is the generator matrices of a $[2n, n]$ LCD code over R.

Example 3.1. *Let $q = 3$, $n = 6$, and $\alpha = 2$ so that $\alpha^2 + 4 \neq 0 \bmod 3$. Then for the weighing matrix $W_{6,4}$ given by*

$$W_{6,4} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 \\ -1 & 0 & 0 & 1 & -1 & 1 \\ -1 & 0 & 0 & -1 & 1 & 1 \\ -1 & -1 & 1 & 0 & 0 & -1 \\ -1 & 1 & -1 & 0 & 0 & -1 \\ 0 & -1 & -1 & 1 & 1 & 0 \end{bmatrix},$$

$G = [2I \mid W_{6,4}]$ generates a $[12, 6, 5]$ LCD code over $\mathbb{F}_3$.

Next we show that if q is odd there always exists a suitable matrix to construct an LCD codes.

Theorem 3.7. *[?, Theorem 7.32] Assume $q \equiv 3 \bmod 4$, η be the quadratic character of $\mathbb{F}_q$ and $b_{ij} = \eta(j - i)$ for $1 \leqslant i, j \leqslant q$, $i \neq j$. Then we have a Hadamard matrix given by*

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & -1 & b_{12} & b_{13} & \dots & b_{1q} \\ 1 & b_{21} & -1 & b_{23} & \dots & b_{2q} \\ 1 & b_{31} & b_{32} & -1 & \dots & b_{3q} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 1 & b_{q1} & b_{q2} & b_{q3} & \dots & -1 \end{bmatrix}. \tag{3.6}$$

Corollary 3.2. *For all nonzero $\alpha \in \mathbb{F}_q$ such that $q \equiv 3 \bmod 4$, the code generated by*

$$G = [\alpha I_{q+1} \mid H], \tag{3.7}$$

*where H is the Hadamard matrix of order $q+1$ given in (**??**), is an LCD code over $\mathbb{F}_q$ of length $2(q+1)$.*

Proof. If $q \equiv 3 \bmod 4$, then From [**?**, Lemma 3.3] $\alpha^2 + 1$ has no solution in $\mathbb{F}_q$. The result then follows from Proposition **??** and Theorem **??**. □

Example 3.2.

$$H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \end{bmatrix}.$$

*Gives an $[8, 4, 4]$ LCD code over $\mathbb{F}_3$. According to [**?**] this is an optimal code.*

In [**?**] the authors constructed self-dual codes from conference matrices. We note that if $\alpha^2 + k = 0$ has solution, the matrix $[\alpha I_n \mid W_{n,k}]$ generates a self-dual code over $\mathbb{F}_q$. Then exists $\alpha' \neq 0$ such that $\alpha'^2 + k \neq 0$, from Proposition **??** $[\alpha' I \mid W_{n,k}]$ generates an LCD code with the same parameters as the self-dual code. This result also holds for the minimum distance of LCD codes generated by $G = [\alpha' I \mid \beta I + W_{n,k}]$. It is easy to verify that whenever we have a skew matrix $W_{n,k}$, we can construct a skew matrix $W_{2n,2k+1}$ where

$$W_{2n,2k+1} = \begin{bmatrix} W_{n,k} & -W_{n,k} - I \\ W_{n,k} + I & W_{n,k}. \end{bmatrix} \tag{3.8}$$

The above results were used to construct the LCD codes over $\mathbb{F}_p$, p prime, $3 < p \leq 23$, given in Tables 1, 2, 3, and 4. It is worth noting that for many parameters a self-dual code cannot be constructed from weighing matrices, whereas for the same parameters (except for the case $p = 3$) it was always possible to construct LCD codes.

Table 3.1: LCD codes from conference matrices with $N = 8$, 12 and 16 from Proposition **??**

p	α	β	d	α	d	α	β	d
5	2	1	4	1	6	2	1	7
7	1	3	5	1	6	2	1	7
11	1	2	5	1	6	1	0	7
13	2	3	5	1	6	1	6	7
17	2	8	5	1	6	2	3	7
19	1	8	5	1	6	2	7	7
23	3	4	5	1	6	3	0	7

Table 3.2: LCD codes from conference matrices with $N = 20$, 24 and 28 from Proposition **??**

p	α	d	α	β	d	α	d
5	2	8	1	0	9	1	10
7	1	8	2	3	9	2	10
11	1	8	1	0	9	1	10
13	1	8	5	5	9	1	10
17	1	8	1	6	9	1	10
19	1	8	2	8	9	1	10
23	1	8	1	0	9	1	10

Table 3.3: LCD codes from conference matrices with $N = 32$, 36 and 40 from Proposition **??**

p	α	β	d	α	d	α	β	d
5	2	2	10	1	12	2	0	13
7	1	3	11	1	12	1	0	13
11	1	5	11	1	12	1	0	13
13	2	6	11	1	12	1	4	13
17	1	0	11	1	12	1	0	13
19	1	0	11	1	12	1	0	13
23	1	2	11	1	12	1	0	13

Table 3.4: LCD codes from the skew matrix $W_{14,9}$ from Proposition **??**

p	α	β	d
5	2	0	8
7	2	2	10
11	1	3	10
13	2	4	11
17	1	2	11
19	2	3	11
23	2	6	11

3.1.3 General construction of LCD codes

We start with the following lemma.

Lemma 3.2. *If $R = \mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$ with $q = p^r$ a power of an odd prime, then the following hold:*

(i) there exists $\alpha \in R$ such that $\alpha^2 + 1 = 0$ if $q \equiv 1 \bmod 4$,

(ii) there exist $\alpha, \beta \in R$ such that $\alpha^2 + \beta^2 + 1 = 0$ if $q \equiv 3 \bmod 4$, and

(iii) for every q there exist $\alpha, \beta, \gamma, \delta \in R$ such that $\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = 0$ in R.

Proof. It is easy to show that if there exist solutions over $\mathbb{F}_q$ for cases (i)-(iii), then these solutions also hold over R since $\mathbb{F}_q$ is a subring of R. Hence we only need show that these solutions exist over $\mathbb{F}_q$.

From [**?**, Lemma 3.3], if $q \equiv 1 \bmod 4$ then -1 is a square in $\mathbb{F}_q$, which proves (i). From [**?**, p. 281], if $q \equiv 3 \bmod 4$ then there exist $\alpha, \beta \in \mathbb{F}_q$ such that $\alpha^2 + \beta^2 + 1 = 0$, which proves (ii). From [**?**, Theorem 370], we have that every prime is the sum of four squares, which proves (iii). □

The next result shows that it is always possible to construct LCD codes over R.

Theorem 3.8. *If P is the generator matrix of a self-dual code over R, then the generator matrix $G = [I \mid P]$ generates an LCD code over R. If $G = [I \mid P]$ is the generator matrix of a linear code over R, then the following hold:*

(i) If $q \equiv 1 \bmod 4$ and $\alpha^2 + 1 = 0$, then the code over R with generator matrix $G' = [I \mid P \mid \alpha P]$ generates an LCD code over R.

(ii) If $q \equiv 3 \bmod 4$ and $\alpha, \beta \in \mathbb{F}_q$ such that $\alpha^2 + \beta^2 + 1 = 0$, then $G' = [I \mid P \mid \alpha P \mid \beta P]$ generates an LCD code over R.

(iii) If $R = \mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$ with $q = p^r$, then $G' = [I \mid P \mid \alpha P \mid \beta P \mid \delta P \mid \gamma P]$ such that $\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = p$ generates an LCD code over R.

Proof. Part (i) is just a verification. The other parts follow from Lemma **??**. □

3.2 Construction of formally self-dual codes over R

Recall that a code C is called formally self-dual if C and $C^{\perp}$ have the same weight enumerator. Codes which are equivalent to their dual are called isodual codes, and isodual codes are also formally self-dual. we present three constructions of formally self-dual codes over R. First, we give the following result which links formally self-dual codes over R to formally self-dual codes over $\mathbb{F}_q$.

Theorem 3.9. *If C is formally self-dual codes over R, then the image under the corresponding Gray map is formally self-dual code.*

Proof. The result follows from Theorem **??** and the fact that the Gray map is an isometry. □

An $n \times n$ square matrix M is called λ-circulant if it is in the following form

$$M = \begin{bmatrix} M_{11} & M_{12} & M_{13} & \dots & M_{1n} \\ \lambda M_{1n} & M_{11} & M_{12} & \dots & M_{1n-1} \\ \lambda M_{1n-1} & \lambda M_{1n} & M_{11} & \dots & M_{1n-2} \\ \vdots & \vdots & \vdots & \vdots & \\ \lambda M_{12} & \lambda M_{13} & \lambda M_{14} & \dots & M_{11} \end{bmatrix}.$$

If $\lambda = 1$ this matrix is circulant and there is a vast literature on double circulant and bordered double circulant self-dual codes [**?**].

The proof of the next theorem is the same as that for [**?**, Theorem 6.1] given over $\mathbb{F}_q + v\mathbb{F}_q$. It is given here for completeness.

Theorem 3.10. *Let M be a λ-circulant matrix over R of order n. Then the code generated by $G = [I_n \mid M]$ is a formally self-dual code over R.*

Proof. Let C be the code generated by $G = [I_n \mid M]$ and C' be the code generated by $G' = [M^t \mid -I_n]$. It easy to verify that the codes C and C' are orthogonal codes, and since they both have free rank n, $C' = C^{\perp}$. Let C'' be the code generated by $G'' = [M^t \mid I_n]$. Since $wt(a) = wt(-a)$ for any a in R the codes C' and C'' have the same weight enumerator. In order to complete the proof, we show that C'' is equivalent to C, therefore C is formally self-dual. Let σ be the permutation

$$\sigma = (1, n)(2, n-1)\dots(k-1, n-k+2)(k, n-k+1),$$

where $k = n/2$. If M' is the matrix obtained by applying σ on the rows of M and M'' is the matrix obtained by applying σ on the columns of M', then $M'' = M^t$. Hence, M and M^t are equivalent. Similarly, by applying a suitable column permutation we obtain that G and G'' are equivalent. Thus, C and C'' are equivalent and therefore C is formally self-dual. □

Example 3.3. *Let $q = 3$, $n = 4$, $\lambda = 1 + v$ and M be the following λ-circulant matrix*

$$M = \begin{bmatrix} 2v + 2v^2 & 2 + v + v^2 & 1 + 2v & 2 \\ 2 + 2v & 2v + 2v^2 & 2 + 2v + 2v^2 & 1 + 2v \\ 1 + 2v^2 & 2 + 2v & 2v + 2v^2 & 2 + 2v + 2v^2 \\ 2 + v^2 & 1 + 2v^2 & 2 + 2v & 2v + 2v^2 \end{bmatrix}.$$

Then $G = [I_4 \mid M]$ generates a formally self-dual code of length 8 over $\mathbb{F}_3 + v\mathbb{F}_3 + v^2\mathbb{F}_3$. The Gray image of this code is a $[24, 12, 9]$ formally self-dual code over $\mathbb{F}_3$. This is an optimal code.

Example 3.4. *Let $q = 5$, $n = 3$, $\lambda = 2 + v$ and M be the following λ-circulant matrix*

$$M = \begin{bmatrix} 3v + 2v^2 & 4v & 3 + 2v \\ 1 + 2v + 2v^2 & 3v + 2v^2 & 4v \\ 3v + 4v^2 & 1 + 2v + 2v^2 & 3v + 2v^2 \end{bmatrix}.$$

Then $[I_3 \mid M.]$ generates a formally self-dual code of length 6 over $\mathbb{F}_5 + v\mathbb{F}_5 + v^2\mathbb{F}_5$. The Gray image of this code is a $[18, 9, 7]$ formally self-dual code over $\mathbb{F}_5$.

Theorem 3.11. *Let M be an $(n-1)\times(n-1)$ λ-circulant matrix. Then the code generated by*

$$G = \left[\begin{array}{c|ccc} & \alpha & \omega & \cdots & \omega \\ & \omega & & & \\ I_n & \vdots & & M & \\ & \omega & & & \end{array}\right]$$

where $\alpha, \omega \in R$, is a formally self-dual code over R.

Proof. The proof is similar to that of Theorem **??**. □

Example 3.5. *Let $q = 3$, $\alpha = 2 + v + 2v^2$, $\omega = 2 + 2v$, $\lambda = 1 + v^2$, $n = 3$ and*

$$M = \begin{bmatrix} 2 & 1+v \\ 1+2v+v^2 & 2 \end{bmatrix}.$$

Then

$$G = \begin{bmatrix} 1 & 0 & 0 & 2+v+2v^2 & 2+2v & 2+2v \\ 0 & 1 & 0 & 2+2v & 2 & 1+v \\ 0 & 0 & 1 & 2+2v & 1+2v+v^2 & 2 \end{bmatrix},$$

generates a formally self-dual code of length 6 over $\mathbb{F}_3 + v\mathbb{F}_3 + v^2\mathbb{F}_3$. The Gray image of the code is an $[18, 9, 6]$ formally self-dual code over $\mathbb{F}_3$. This is an optimal code.

Using a proof similar to that of Theorem **??**, we have the following construction of formally self-dual codes over R.

Theorem 3.12. *Let A be an $n \times n$ matrix over R such that $A^t = A$. Then the code generated by $G = [I_n \,|\, A]$ is a formally self-dual code over R of length $2n$.*

Example 3.6. *Let $q = 5$, $n = 3$, and A be the matrix*

$$A = \begin{bmatrix} 4v+1 & v+v^2 & 4+4v \\ v+v^2 & 4v & 1+v \\ 4+4v & 1+v & 1+v \end{bmatrix}.$$

We have that $A = A^t$, so $[I_5 \mid A]$ generates a formally self-dual code of length 6 over $\mathbb{F}_5 + v\mathbb{F}_5 + v^2\mathbb{F}_5$. The Gray image of this code is a $[18, 9, 7]$ formally self-dual code over $\mathbb{F}_5$.

Example 3.7. *Let $q = 3$, $n = 5$, and A be the matrix*

$$A = \begin{bmatrix} 0 & v & 2+v & 1+2v+2v^2 & 2v+2v^2 \\ v & 2v+2v^2 & 2 & 1+v & 1+v^2 \\ 2+v & 2 & 2v^2 & 2+v+v^2 & 1+2v \\ 1+2v+2v^2 & 1+v & 2+v+v^2 & 1 & v \\ 2v+2v^2 & 1+v^2 & 1+2v & v & 2 \end{bmatrix}.$$

We have that $A = A^t$, so $[I_3 \mid A]$ generates a formally self-dual code of length 10 over $\mathbb{F}_3 + v\mathbb{F}_3 + v^3\mathbb{F}_3$. The Gray image of this code is a $[30, 15, 9]$ formally self-dual code over $\mathbb{F}_3$.

Proposition 3.13. *Let C_1, C_2, and C_3 be linear codes of length n over $\mathbb{F}_q$. C_1, C_2, and C_3 are isodual codes if and only if $C = \eta_1 C_1 \oplus \eta_2 C_2 \oplus \eta_3 C_3$ is an isodual code of length n over R.*

Proof. Let τ_1, τ_2, and τ_2 be monomial permutations such that $\tau_1(C_1) = C_1^{\perp}$, $\tau_2(C_2) = C_2^{\perp}$ and $\tau_3(C_3) = C_3^{\perp}$. Then $\eta_1\tau_1(C_1) \oplus \eta_2\tau_2(C_2) \oplus \eta_3\tau_3(C_3) = \eta_1 C_1^{\perp} \oplus \eta_2 C_2^{\perp} \oplus \eta_3 C_3^{\perp}$. Since $C^{\perp} = \eta_1 C_1^{\perp} \oplus \eta_2 C_2^{\perp} \oplus \eta_3 C_2^{\perp}$, it follows that C is equivalent to $C^{\perp}$. □

A formally self-dual code with only even weights is said to be an even formally self-dual code, otherwise it is an odd formally self-dual code. The next theorem is the same as the condition

given by Dougherty [**?**].

Theorem 3.14. *Linear odd formally self-dual codes exist over R for all lengths.*

3.2.1 Construction of LCD formally self-dual codes over R

LCD formally self-dual codes over R are constructed in this subsection.

Theorem 3.15. *With the same assumptions as in Theorem **??**. The code generated by $G = [I_n|A]$ is an LCD formally self-dual code over R if and only if GG^t is nonsingular.*

Proof. From Theorem **??**, we know that G generates a formally self-dual code. To prove that G generates an LCD codes we apply the conditions of Theorem **??** on the matrix $G = [I_n|A]$. □

Example 3.8. *Let $q = 3$, $n = 4$, and*

$$A = \begin{bmatrix} v & 0 & v & v \\ 0 & 0 & 0 & 0 \\ v & 0 & v & v \\ v & 0 & v & v \end{bmatrix},$$

so that $A = A^t$. It is easily determined that GG^t is nonsingular. Then $G = [I_3\,|A]$ generates an LCD formally self-dual code of length 8 over $\mathbb{F}_3 + v\mathbb{F}_3 + v^2\mathbb{F}_3$.

Theorem 3.16. *With the same assumptions as in Theorem **??**, the matrix $G = [I_n|M]$ generates an LCD formally self-dual code over R if and only if GG^t is nonsingular.*

Example 3.9. *Let $q = 5$, $n = 4$, $\lambda = 4v^2$ and M be the following λ-circulant matrix*

$$M = \begin{bmatrix} 2v^2 & 0 & v & 0 \\ 0 & 2v^2 & 0 & v \\ 4v & 0 & 2v^2 & 0 \\ 0 & 4v & 0 & 2v^2 \end{bmatrix}$$

It is easily determined that GG^t is nonsingular. Then $G = [I_4 \,|M]$ generates an LCD formally self-dual code of length 18 over $\mathbb{F}_5 + v\mathbb{F}_5 + v^2\mathbb{F}_5$.

Theorem 3.17. *With the same assumptions as in Theorem* **??**, *the code generated by*

$$G = \left[\begin{array}{c|cccc} & \alpha & \omega & \dots & \omega \\ & \omega & & & \\ I_n & \vdots & & M & \\ & \omega & & & \end{array}\right]$$

is an LCD formally self-dual code over R if and only if GG^t is nonsingular.

Example 3.10. *Let $q = 3$, $n = 3$, $\lambda = v^2$ and M be the following λ-circulant matrix*

$$M = \begin{bmatrix} v & v \\ v & v \end{bmatrix}.$$

If $\alpha = v$ and $\omega = v^2$, it is easily determined that for the matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & v & v^2 & v^2 \\ 0 & 1 & 0 & v^2 & v & v \\ 0 & 0 & 1 & v^2 & v & v \end{bmatrix},$$

GG^t is nonsingular. Then G generates an LCD formally self-dual code of length 6 over $\mathbb{F}_3 + v\mathbb{F}_3 + v^2\mathbb{F}_3$.

3.3 Bounds on LCD codes

we begin with the following bound was given by Dougherty et al. [**?**]

$$LCD[n,k]_q := \max\{d \text{ there exists an } [n,k,d]_q \text{ LCD code}\}.$$

They also gave estimates and results for this bound. For linear codes over F_q we have the following bound

$$\mathcal{B}(n,k)_q := \max\{d \text{ there exists an } [n,k,d]_q \text{ code }\}.$$

The next result gives an upper bound on d for an LCD code over $\mathbb{F}_q$

Proposition 3.18. *If an $[n, n/2, d]_q$ self-dual code C exists, then $LCD[3n, n/2]_q \geq d$. In particular, if C is an extremal self-dual code over $\mathbb{F}_2$, then $LCD[3n, n/2]_2 \geq \frac{4n}{24}+4$ if $n \neq 22 \bmod 24$, and $LCD[3n, n/2]_2 \geq \frac{4n}{24}+6$ if $n \equiv 22 \bmod 24$. For $\mathbb{F}_3$ and $n \equiv 0 \bmod 4$, $LCD[3n, n/2]_3 \geq 3n/12 + 3$.*

Proof. If there exists an $[n, n/2, d]_q$ self-dual code with generator matrix P, then the matrix $G = [I \mid P]$ satisfies $GG^t = I$, and hence by Proposition **??** G generates an LCD code with parameters $[3n, n/2, \geq d]$. In the binary case, the bound given corresponds to the condition on

extremal binary self-dual codes. In the ternary case, the bound corresponds to the condition on the existence of extremal ternary self-dual codes. □

The proof of the following result follows from Theorem **??** and the Singleton bound.

Proposition 3.19. *If there exists an $[n, k, d]_q$ code over $\mathbb{F}_q$, then*

$$\begin{aligned} d &\leq LCD[n+k,k]_q \leq \mathcal{B}(n+k,k)_q \leq n+1 \text{ if } q = 2^m, \\ d &\leq LCD[2n+k,k]_q \leq \mathcal{B}(2n+k,k)_q \leq 2n+1 \text{ if } q \equiv 1 \bmod 4, \\ d &\leq LCD[3n+k,k]_q \leq \mathcal{B}(3n+k,k)_q \leq 3n+1 \text{ if } q \equiv 3 \bmod 4, \\ d &\leq LCD[4n+k,k]_q \leq \mathcal{B}(4n+k,k)_q \leq 4n+1 \text{ for all } q. \end{aligned}$$

Proposition 3.20. *If q is odd, then*

$$LCD[q+1, q-2\mu]_q = B(q+1, q-2\mu)_q = 2\mu + 2,$$

for $1 \leq \mu \leq \frac{q-1}{2}$.

If q is even, then

$$LCD[q+1, q-1-2\mu]_q = B(q+1, q-1-2\mu) = 2\mu + 2 + 3,$$

for $1 \leq \mu \leq \frac{q-1}{2} - 1$.

Proof. From [**?**, Theorem 8], if $q+1-k$ is odd (this case correspond to q and k both even or odd), then the cyclic code generated by the polynomial $g_1(x) = \prod_{i=-\mu}^{\mu}(x-\alpha^i)$ is a $[q+1, q-2\mu, 2\mu+2]_q$ maximum distance separable (MDS) cyclic code. Since $g_1(x)$ is self-reciprocal, from Lemma **??** the code is LCD. Since the code is also MDS, the result follows.

If q is even and k is odd, then the polynomial $g_2(x) = \prod_{i=q/2-\mu}^{q/2}(x-\alpha^i)(x-\alpha^{-i})$ generates a $[q+1, q-1-2\mu, 2\mu+3]_q$ MDS cyclic code from [**?**, Theorem 8]. Since $g_2(x)$ is self-reciprocal, the code is LCD by Lemma **??**. The result then follows since the code is MDS. □

For codes over R, define the bound

$$LCD[n,k]_R := \max\{d \text{ there exists an} [n,k,d_L]_R \text{ free LCD code over R}\}.$$

From Remark **??** we have the following bound

$$LCD[n,k]_R \geq LCD[n,k]_q, \tag{3.9}$$

which gives the following result.

Corollary 3.3. *All of the lower bounds on $LCD[n,k]_q$ given in [?] are also lower bounds on $LCD[n,k]_R$.*

Chapter 4

$\mathbb{Z}_q(\mathbb{Z}_q + u\mathbb{Z}_q)-$Linear skew constacyclic codes

The classes of cyclic and constacyclic codes play a very signifiant role in the theory of error correcting codes. In D. Boucher et al. [**?**], generalized class of linear cyclic codes by using generator polynomials in non-commutative skew polynomial rings. In this paper, we study skew constacyclic codes over the ring $\mathbb{Z}_qR$, where $R = \mathbb{Z}_q + u\mathbb{Z}_q$, $q = p^s$ for a prime p and $u^2 = 0$. We give the definition of these codes as subsets of the ring $\mathbb{Z}_q^{\alpha}R^{\beta}$. Some structural properties of the skew polynomial ring $R[x, \Theta]$ are discussed, where Θ is an automorphism of R. We describe the generator polynomials of skew constacyclic codes over $\mathbb{Z}_qR$, also we determine their minimal spanning sets and their sizes. Further, by using the Gray images of skew constacyclic codes over $\mathbb{Z}_qR$ we obtained some new linear codes over $\mathbb{Z}_4$. Finally, we have generalized these codes to double skew constacyclic codes over $\mathbb{Z}_qR$. Apart of this chapter appeared in [**?**].

4.1 Skew polynomial ring over R

In this subsection we construct the non-commutative ring $R[x, \Theta]$. The structure of this ring depends on the elements of the commutative ring R and an automorphism Θ of R. Note that an automorphism Θ in R must fix every element of $\mathbb{Z}_q$, hence it satisfies $\Theta(a + ub) = a + \delta(u)b$.

Therefore, it is determined by its action on u. Let $\delta(u) = k + ud$, where k is a non-unit in $\mathbb{Z}_q$, $k^2 \equiv 0 \ mod \ q$ and $2kd \equiv 0 \ mod \ q$. Then,

$$\Theta(a + ub) = a + \delta(u)b = (a + kb) + udb, \tag{4.1}$$

for all $a + ub \in R$. Further, let Θ an automorphism of R and let m be its order. The skew polynomial ring $R[x, \Theta]$ is the set of polynomials over R in which the addition is defined as the usual addition of polynomials and the multiplication is defined by the rule

$$xa = \Theta(a)x.$$

The multiplication is extended to all elements in $R[x, \Theta]$ by associativity and distributivity. The ring $R[x, \Theta]$ is called a skew polynomial ring over R and an element in $R[x, \Theta]$ is called a skew polynomial. Further, an element $g(x) \in R[x, \Theta]$ is said to be a right divisor (resp. left divisor) of $f(x)$ if there exists $q(x) \in R[x, \Theta]$ such that

$$f(x) = q(x)g(x) \quad (\text{ resp. } f(x) = g(x)q(x)).$$

In this case, $f(x)$ is called a left multiple (resp. right multiple) of $g(x)$.

Example 4.1. *Define a map Θ on $R = \mathbb{Z}_4 + u\mathbb{Z}_4$ such that*

$$\Theta(a + ub) = a + (u + 1)b.$$

for all $a + ub \in R$. We can easily verify that Θ is an automorphism of order 2.

Lemma 4.1. *[**?**, Lemma 1] Let $f(x)$, $g(x) \in R[x, \Theta]$ be such that the leading coefficient of $g(x)$ is a unit. Then there exists $q(x)$, $r(x) \in R[x, \Theta]$ such that*

$$f(x) = q(x)g(x) + r(x), \ \textit{where } r(x) = 0 \ \textit{or } \deg(r(x)) < \deg(g(x)).$$

Definition 4.1. *[**?**, Definition 3.2] A polynomial $f(x) \in R[x, \Theta]$ is said to be a central polynomial if*

$$f(x)r(x) = r(x)f(x)$$

for all $r(x) \in R[x, \Theta]$.

Theorem 4.1. *The center $Z(R[x,\Theta])$ of $R[x,\Theta]$ is $R^{\Theta}[x^m]$; where m is the order of Θ and R^{Θ} is the subring of R fixed by Θ.*

Proof. We know $R = \mathbb{Z}_q + u\mathbb{Z}_q$ is the fixed ring of Θ. Since order of Θ is m, for any non-negative integer i, we have

$$x^{mi}a = (\Theta^m)^i(a)x^{mi} = ax^{mi}$$

for all $a \in R$. It gives $x^{mi} \in Z(R[x,\Theta])$, and hence all polynomials of the form

$$f = a_0 + a_1x^m + a_2x^{2m} + \cdots + a_lx^{lm}$$

with $a_i \in R$ are in the center. Conversely, let $f = f_0 + f_1x + f_2x^2 + \cdots + f_kx^k \in Z(R[x,\Theta])$ we have $fx = xf$ which gives that all f_i are fixed by Θ, so that $f_i \in R$. Further, choose $a \in R$ such that $\Theta(a) \neq a$. Then it follows from the relation $af = fa$ that $f_i = 0$ for all indices i not divides m. Thus

$$f(x) = a_0 + a_1x^m + a_2x^{2m} + \cdots + a_lx^{lm} \in R^{\Theta}[x^m].$$

□

Corollary 4.1. *Let $f(x) = x^\beta - 1$, then $f(x) \in Z(R[x,\Theta])$ if and only if $m \mid \beta$. Further, $x^\beta - \lambda \in Z(R[x,\Theta])$ if and only if $m \mid \beta$ and λ is fixed by Θ.*

4.2 Skew constacyclic codes over R

In this subsection we generalize the structure and properties from [**?**] to codes over $\mathbb{Z}_q + u\mathbb{Z}_q$. Hence the proofs of many of the theorems will be omitted.

We start with some structural properties of $R[x,\Theta]/\langle x^\beta - \lambda\rangle$. The Corollary **??**, shows that the polynomial $(x^\beta - \lambda)$ is in the center $Z(R[x,\Theta])$ of the ring $R[x,\Theta]$, hence generates a two-sided ideal if and only if $m \mid \beta$ and λ is fixed by Θ. Therefore, in this case $R[x,\Theta]/\langle x^\beta - \lambda\rangle$ is a well-defined residue class ring. If $m \nmid \beta$, then the quotient space $R[x,\Theta]/\langle x^\beta - \lambda\rangle$ which is not necessarily a ring is a left $R[x,\Theta]$-module with multiplication defined by

$$r(x)(f(x) + (x^\beta - \lambda)) = r(x)f(x) + (x^\beta - \lambda),$$

for any $r(x)$, $f(x) \in R[x, \Theta]$.

Next we define the skew $\lambda-$constacyclic codes over the ring R. A code of length β over R is a nonempty subset of R^β. A code C is said to be linear if it is a submodule of the $R-$module R^β. In this thesis, all codes are assumed to be linear unless otherwise stated.

Given an automorphism Θ of R and a unit λ in R, a code C_β is said to be skew constacyclic, or specifically, $\Theta - \lambda-$constacyclic if C_β is closed under the $\Theta - \lambda-$constacyclic shift:

$$\rho_{\Theta,\lambda} : R^\beta \to R^\beta$$

defined by

$$\rho_{\Theta,\lambda}((a_0, a_1, \ldots, a_{\beta-1})) = (\lambda\Theta(a_{\beta-1}), \Theta(a_0), \ldots, \Theta(a_{\beta-2})). \tag{4.2}$$

In particular, such codes are called skew cyclic and skew negacyclic codes when λ is 1 and -1, respectively. When Θ is the identity automorphism, he become classical constacyclic and we denote ρ_λ the constacyclic shift.

In the rest of paper, we restrict our study to the case where the length β of codes is a multiple of the order of Θ and λ is a unit in R^Θ, where R^Θ denotes the subring of R fixed by Θ.

The proofs of the next theorems are analogous to the proofs of [**?**] given for the ring $\mathbb{Z}_4+u\mathbb{Z}_4$, therefore we omit them.

Theorem 4.2. *[**?**, Theorem 3] A code C_β of length β in $R_\beta = R[x, \Theta]/\langle x^\beta - \lambda\rangle$ is a $\Theta - \lambda-$constacyclic code if and only if C_β is a left $R[x, \Theta]-$submodule of the left $R[x, \Theta]-$module R_β.*

Corollary 4.2. *[**?**, Corollary 2] A code C of length β over R is $\Theta - \lambda-$constacyclic code if and only if the skew polynomial representation of C is a left ideal in $R[x, \Theta]/\langle x^\beta - \lambda\rangle$.*

The following theorem is the generalization of the Theorems 4 and 5 of [**?**].

Theorem 4.3. *Let C_β be a skew contacyclic code of length β over R. Then, C_β is a free principally generated skew constayclic code if and only if there exists a minimal degree polynomial $g_\beta(x) \in C_\beta$ having its leading coefficient a unit such that $C_\beta = \langle g_\beta(x)\rangle$ and $g_\beta(x) \mid x^\beta - \lambda$. Moreover, C_β has a basis $\{g_\beta(x), xg_\beta(x), \ldots, x^{\beta-deg(g_\beta(x))-1}\}$ and $|C_\beta| = |R|^{\beta-deg(g_\beta(x))}$.*

4.2.1 The dual of skew constacyclic codes over R

In this subsection, we study duals of $\Theta - \lambda-$constacyclic codes over R. Further, the Euclidean inner product defined by

$$\langle v', w' \rangle = \sum_{i=0}^{\beta-1} v'_i w'_i,$$

for $v' = (v'_0, v'_1, \ldots, v'_{\beta-1})$ and $w' = (w'_0, w'_1, \ldots, w'_{\beta-1})$ in R^β.

Definition 4.2. *Let C_β be a $\Theta - \lambda-$constacyclic code of length β over R. Then its dual $C_\beta^\perp$ is defined as*

$$C_\beta^\perp = \{v' \in R^\beta;\ \langle v', w' \rangle = 0 \text{ for all } w' \in C_\beta\}.$$

Lemma 4.2. *Let C_β be a code of length β over R, where β is a multiple of the order of the automorphism Θ and λ is fixed by Θ. Then C_β is $\Theta - \lambda-$constacyclic if and only if $C_\beta^\perp$ is $\Theta - \lambda^{-1}-$constacyclic. In particular, if $\lambda^2 = 1$, then C_β is $\Theta - \lambda-$constacyclic if and only if $C_\beta^\perp$ is $\Theta - \lambda-$constacyclic.*

Proof. Note that, for each unit λ in $R, \lambda \in R^\Theta$ if and only if $\lambda^{-1} \in R^\Theta$, since $\lambda \in R^\Theta$, so is λ^{-1}. Let $v' = (v'_0, v'_1, \ldots, v'_{\beta-1}) \in C_\beta$ and $w' = (w'_0, w'_1, \ldots, w'_{\beta-1}) \in C_\beta^\perp$ be two arbitrary elements. Since C_β is $\Theta - \lambda-$constacyclic code,

$$\rho_{\Theta,\lambda}^{\beta-1}(v') = \left(\Theta^{\beta-1}(\lambda v'_1), \Theta^{\beta-1}(\lambda v'_2), \ldots, \Theta^{\beta-1}(\lambda v'_{\beta-1}), \Theta^{\beta-1}(v'_0)\right) \in C_\beta.$$

Then, we have

$$\begin{aligned}
0 &= \langle \rho_{\Theta,\lambda}^{\beta-1}(v'), w' \rangle \\
&= \langle (\Theta^{\beta-1}(\lambda v'_1), \Theta^{\beta-1}(\lambda v'_2), \ldots, \Theta^{\beta-1}(\lambda v'_{\beta-1}), \Theta^{\beta-1}(v'_0)), (w'_0, \ldots, w'_{\beta-1}) \rangle \\
&= \lambda \langle (\Theta^{\beta-1}(v'_1), \Theta^{\beta-1}(v'_2), \ldots, \Theta^{\beta-1}(v'_{\beta-1}), \Theta^{\beta-1}(\lambda^{-1} v'_0)), (w'_0, \ldots, w'_{\beta-1}) \rangle \\
&= \lambda \left(\Theta^{\beta-1}(\lambda^{-1} v'_0) w'_{\beta-1} + \sum_{j=1}^{\beta-1} \Theta^{\beta-1}(v'_j) w'_{j-1} \right).
\end{aligned}$$

As β is a multiple of the order of Θ and λ^{-1} is fixed by Θ, it follows that

$$\begin{aligned}
0 = \Theta(0) &= \Theta(\lambda \Theta^{\beta-1}(\lambda^{-1} v'_0) w'_{\beta-1} + \sum_{j=1}^{\beta-1} \Theta^{\beta-1}(v'_j) w'_{j-1}) \\
&= \lambda (v'_0 \Theta(\lambda^{-1} w'_{\beta-1}) + \sum_{j=1}^{\beta-1} v'_j \Theta(w'_{j-1})) \\
&= \lambda \langle \rho_{\Theta,\lambda^{-1}}(w'), v' \rangle.
\end{aligned}$$

This implies that, $\rho_{\Theta,\lambda^{-1}}(w') \in C_\beta^\perp$. In addition, assume that $\lambda^2 = 1$. Then $\lambda = \lambda^{-1}$. Therefore; C_β is a $\Theta - \lambda-$constacyclic code.

The converse follows from the fact that $(C_\beta^\perp)^\perp = C_\beta$. □

4.3 $\mathbb{Z}_q R-$Linear skew constacyclic codes

In this section, we study skew $\lambda-$constacyclic codes over the ring $\mathbb{Z}_q R$.

We known that the ring $\mathbb{Z}_q$ is a subring of the ring R. Let (α, β) denote $n = \alpha + 2\beta$ where α and β are positive integers. We construct the ring

$$\mathbb{Z}_q R = \{(e, r);\ e \in \mathbb{Z}_q, r \in R\}.$$

The ring $\mathbb{Z}_q R$ is not an $R-$module under the operation of standard multiplication. To make $\mathbb{Z}_q R$ an $R-$module, we follow the approach in [**?**] and define the map

$$\eta : R \to \mathbb{Z}_q$$
$$a + ub \mapsto a.$$

It is clear that the mapping η is a ring homomorphism. Now, for any $d \in R$, we define the multiplication $*$ by

$$d * (e, r) = (\eta(d)e, dr).$$

This multiplication can be naturally generalized to the ring $\mathbb{Z}_q^\alpha R^\beta$ as follows.
For any $d \in R$ and $v = (e_0, e_1, \ldots, e_{\alpha-1}, r_0, r_1, \ldots, r_{\beta-1}) \in \mathbb{Z}_q^\alpha R^\beta$ define

$$dv = (\eta(d)e_0, \eta(d)e_1, \ldots, \eta(d)e_{\alpha-1}, dr_0, dr_1, \ldots, dr_{\beta-1}),$$

where $(e_0, e_1, \ldots, e_{\alpha-1}) \in \mathbb{Z}_q^\alpha$ and $(r_0, r_1, \ldots, r_{\beta-1}) \in R^\beta$.

The following results are analogous to the ones obtained in [**?**, **?**] for the ring $\mathbb{Z}_2(\mathbb{Z}_2 + u\mathbb{Z}_2)$.

Lemma 4.3. *The ring $\mathbb{Z}_q^\alpha R^\beta$ is an R-module under the above definition.*

The above Lemma allows us to give the next definition.

Definition 4.3. *A non-empty subset C of $\mathbb{Z}_q^\alpha R^\beta$ is called a $\mathbb{Z}_q R$-linear code if it is an $R-$submodule of $\mathbb{Z}_q^\alpha R^\beta$.*

We note that the ring R is isomorphic to $\mathbb{Z}_q$ as an additive group. Hence, for some positive integers k_0, k_1 and k_2, any $\mathbb{Z}_qR$-linear code C is isomorphic to a group of the form

$$\mathbb{Z}_q^{k_0} \times \mathbb{Z}_q^{2k_1} \times \mathbb{Z}_q^{k_2}.$$

Definition 4.4. *If $C \subseteq \mathbb{Z}_q^{\alpha}R^{\beta}$ is a $\mathbb{Z}_qR$-linear code, group isomorphic to $\mathbb{Z}_q^{k_0} \times \mathbb{Z}_q^{2k_1} \times \mathbb{Z}_q^{k_2}$, then C is called a $\mathbb{Z}_qR$-additive code of type $(\alpha, \beta, k_0, k_1, k_2)$, where k_0, k_1, and k_2 are as defined above.*

The following results and definitions are analogous to the ones obtained in [**?**].

Let C be a $\mathbb{Z}_qR$-linear code and let C_α (respectively C_β) be the canonical projection of C on the first α (respectively on the last β) coordinates. Since the canonical projection is a linear map, C_α and C_β are linear codes over $\mathbb{Z}_q$ and over R of length α and β, respectively. A code C is called separable if C is the direct product of C_α and C_β, i.e.,

$$C = C_\alpha \times C_\beta.$$

We introduce an inner product on $\mathbb{Z}_q^{\alpha}R^{\beta}$. For any two vectors

$$v = (v_0, \ldots, v_{\alpha-1}, v'_0, \ldots, v'_{\beta-1}), w = (w_0, \ldots, w_{\alpha-1}, w'_0, \ldots, w'_{\beta-1}) \in \mathbb{Z}_q^{\alpha} \times R^{\beta}$$

let

$$\langle v, w\rangle = u\sum_{i=0}^{\alpha-1} v_i w_i + \sum_{j=0}^{\beta-1} \acute{v}_j \acute{w}_j.$$

Let C be a $\mathbb{Z}_qR$-linear code. The dual of C is defined by

$$C^{\perp} = \{w \in \mathbb{Z}_q^{\alpha} \times R^{\beta},\ \langle v, w\rangle = 0, \forall v \in C\}.$$

If $C = C_\alpha \times C_\beta$ is separable, then

$$C^{\perp} = C_\alpha^{\perp} \times C_\beta^{\perp}. \tag{4.3}$$

Now we are ready to define the skew constacyclic codes over $\mathbb{Z}_q^{\alpha}R^{\beta}$. We start by the following Lemma.

Lemma 4.4. *Let $R = \mathbb{Z}_q + u\mathbb{Z}_q$, where $\mathbb{Z}_q$ is a subring of R. Then an element λ is unit in R if and only if $\eta(\lambda)$ is unit in $\mathbb{Z}_q$.*

Proof. Assume that λ is unit in R; where $\lambda = \lambda_1 + u\lambda_2$ and $\lambda_1, \lambda_2 \in \mathbb{Z}_q$, then we have $\lambda.v = v.\lambda = 1$ and since η is a ring homomorphism, then we have $\eta(\lambda.v) = \eta(v.\lambda) = \eta(1)$ thus $\eta(\lambda).v' = v'.\eta(\lambda) = 1$ which means that $\eta(\lambda)$ is unit in $\mathbb{Z}_q$, where $v' = \eta(v) \in \mathbb{Z}_q$.

Conversely, suppose that $\eta(\lambda) = \lambda_1$ is unit in $\mathbb{Z}_q$ we should prove that $\lambda = \lambda_1 + u\lambda_2$ is unit in R. The fact that λ is unit in R means that $\lambda.\lambda^{-1} = 1$, therefore $\lambda.\lambda^{-1} = (\lambda_1 + u\lambda_2)(\lambda_1 + u\lambda_2)^{-1} = (\lambda_1 + u\lambda_2)(\lambda_1^{-1} + u\lambda_3) = \lambda_1\lambda_1^{-1} + u(\lambda_2\lambda_1^{-1} + \lambda_1\lambda_3)$, then we denote $\lambda_3 = \frac{-\lambda_2\lambda_1^{-1}}{\lambda_1} = -\lambda_2(\lambda_1^{-1})^2$ and since λ_1 is unit in $\mathbb{Z}_q$, then $\lambda_1\lambda_1^{-1} = 1$ which implies that $\lambda.\lambda^{-1} = 1$, so λ is unit in R. □

Definition 4.5. *Let Θ be an automorphism of R. A linear code C over $\mathbb{Z}_q^{\alpha}R^{\beta}$ is called skew constacyclic code if C satisfies the following two conditions.*

(i) C is an $R-$submodule of $\mathbb{Z}_q^{\alpha}R^{\beta}$,

(ii)

$$(\eta(\lambda)\Theta(e_{\alpha-1}), \Theta(e_0), \ldots, \Theta(e_{\alpha-2}), \lambda\Theta(r_{\beta-1}), \Theta(r_0), \ldots, \Theta(r_{\beta-2})) \in C$$

whenever

$$(e_0, e_1, \ldots, e_{\alpha-1}, r_0, r_1, \ldots, r_{\beta-1}) \in C$$

Remark 4.1. *$\Theta(e_i) = e_i$ for $0 \leq i \leq \alpha - 1$, as $e_i \in \mathbb{Z}_q$ (the fixed ring of Θ).*

In polynomial representation, each codeword $c = (e_0, e_1, \ldots, e_{\alpha-1}, r_0, r_1, \ldots, r_{\beta-1})$ of a skew constacyclic code can be represented by a pair of polynomials

$$\begin{aligned} c(x) &= \left(e_0 + e_1x + \cdots + e_{\alpha-1}x^{\alpha-1}, r_0 + r_1x + \cdots + r_{\beta-1}x^{\beta-1} \right) \\ &= (e(x), r(x)) \in \mathbb{Z}_q[x]/\langle x^{\alpha} - \eta(\lambda)\rangle \times R[x, \Theta]/\langle x^{\beta} - \lambda\rangle. \end{aligned}$$

Let $h(x) = h_0 + h_1x + \cdots + h_tx^t \in R\ [x, \Theta]$ and let $(f(x), g(x)) \in \mathbb{Z}_q[x]/\langle x^{\alpha} - \eta(\lambda)\rangle \times R[x, \Theta]/\langle x^{\beta} - \lambda\rangle$. The multiplication is defined by the basic rule

$$h(x)(f(x), g(x)) = (\eta(h(x))f(x), h(x)g(x)),$$

where $\eta(h(x)) = \eta(h_0) + \eta(h_1)x + \cdots + \eta(h_t)x^t$.

Lemma 4.5. *A code C of length (α, β) over $\mathbb{Z}_qR$ is a $\Theta - \lambda-$constacyclic code if and only if C is left $R[x, \Theta]-$submodule of $\mathbb{Z}_q[x]/\langle x^\alpha - \eta(\lambda)\rangle \times R[x, \Theta]/\langle x^\beta - \lambda\rangle$.*

Proof. Assume that C is a skew constacyclic code and let $c \in C$. We denote by $c(x) = (e(x), r(x))$ the associated polynomial of c. As $xc(x)$ is a skew constacyclic shift of c, $xc(x) \in C$. Then, by linearity of C, $r(x)c(x) \in C$ for any $r(x) \in R[x, \Theta]$. Thus C is left $R[x, \Theta]-$submodule of $\mathbb{Z}_q[x]/\langle x^\alpha - \eta(\lambda)\rangle \times R[x, \Theta]/\langle x^\beta - \lambda\rangle$. Conversely, suppose that C is a left $R[x, \Theta]-$submodule of $\mathbb{Z}_q[x]/\langle x^\alpha - \eta(\lambda)\rangle \times R[x, \Theta]/\langle x^\beta - \lambda\rangle$, then we have that $xc(x) \in C$. Thus, C is a $\Theta - \lambda-$constacyclic code.

The converse is straightforward. □

Theorem 4.4. *Let C be a linear code over $\mathbb{Z}_qR$ of length (α, β), and let $C = C_\alpha \times C_\beta$, where C_α is linear code over $\mathbb{Z}_q$ of length α and C_β is linear code over R of length β. Then C is a skew $\lambda-$constacyclic code if and only if C_α is a $\eta(\lambda)-$constacyclic code over $\mathbb{Z}_q$ and C_β is a skew $\lambda-$constacyclic code over R.*

Proof. Let $(e_0, e_1, \ldots, e_{\alpha-1}) \in C_\alpha$ and let $(r_0, r_1, \ldots, r_{\beta-1}) \in C_\beta$. If $C = C_\alpha \times C_\beta$ is a skew constacyclic code, then

$$(\eta(\lambda)\Theta(e_{\alpha-1}), \Theta(e_0), \ldots, \Theta(e_{\alpha-2}), \lambda\Theta(r_{\beta-1}), \Theta(r_0), \ldots, \Theta(r_{\beta-2})) \in C,$$

which implies that

$$(\eta(\lambda)\Theta(e_{\alpha-1}), \Theta(e_0), \ldots, \Theta(e_{\alpha-2})) \in C_\alpha$$

as Θ is fixed by $\mathbb{Z}_q$, then

$$(\eta(\lambda)e_{\alpha-1}, e_0, \ldots, e_{\alpha-2}) \in C_\alpha$$

and

$$(\lambda\Theta(r_{\beta-1}), \Theta(r_0), \ldots, \Theta(r_{\beta-2})) \in C_\beta.$$

Hence, C_α is a constacyclic code over $\mathbb{Z}_q$ and C_β is a $\Theta - \lambda-$constacyclic code over R.

On the other hand, suppose that C_α is a constacyclic code over $\mathbb{Z}_q$ and C_β is a $\Theta -$ $\lambda-$constacyclic code over R. Note that

$$(\eta(\lambda)e_{\alpha-1}, e_0, \ldots, e_{\alpha-2}) \in C_\alpha$$

and

$$(\lambda\Theta(r_{\beta-1}), \Theta(r_0), \ldots, \Theta(r_{\beta-2})) \in C_\beta.$$

Since $C = C_\alpha \times C_\beta$ and $\Theta(e_i) = e_i$, then

$$(\eta(\lambda)\Theta(e_{\alpha-1}), \Theta(e_0), \ldots, \Theta(e_{\alpha-2}), \lambda\Theta(r_{\beta-1}), \Theta(r_0), \ldots, \Theta(r_{\beta-2})) \in C,$$

so C is a skew constacyclic code over $\mathbb{Z}_qR$. □

Corollary 4.3. *Let $C = C_\alpha \times C_\beta$ be a skew $\lambda-$constacyclic code over $\mathbb{Z}_qR$, where β is a multiple of the order Θ and λ^{-1} is fixed by Θ. Then the dual code $C^\perp = C_\alpha^\perp \times C_\beta^\perp$ of C is a skew λ^{-1}-constacyclic code over $\mathbb{Z}_qR$.*

Proof. From Equation (**??**), we have $C^\perp = C_\alpha^\perp \times C_\beta^\perp$. Clearly, if C_α is a constacyclic code over $\mathbb{Z}_q$ then $C_\alpha^\perp$ is also a constacyclic code over $\mathbb{Z}_q$. Moreover, from Lemma (**??**), we have $C_\beta^\perp$ is a skew $\lambda-$constacyclic code over R. Hence the dual code $C^\perp$ is skew $\lambda^{-1}-$constacyclic over $\mathbb{Z}_qR$. □

4.4 Gray images of skew constacyclic codes over $\mathbb{Z}_qR$

In this section, we define a Gray map on $\mathbb{Z}_qR$, and then extend it to $\mathbb{Z}_q^\alpha R^\beta$. We discuss the Gray images of $\mathbb{Z}_qR-$skew constacyclic codes where λ is fixed by Θ. We start by recalling some results which we will need its in the next.

From [**?**, Definition 2] we have the following definition

Definition 4.6. *Let C_β be a linear code over R of length $\beta = N\ell$ and let λ be unit in R. If for any codeword*

$$\begin{pmatrix} c_{0,0}, c_{0,1}, \ldots, c_{0,\ell-1}, c_{1,0}, c_{1,1}, \ldots, c_{1,\ell-1}, \ldots, \\ c_{N-1,0}, c_{N-1,1}, \ldots, c_{N-1,\ell-1} \end{pmatrix} \in C_\beta,$$

then

$$\left(\begin{array}{c} \lambda\Theta(c_{N-1,0}), \lambda\Theta(c_{N-1,1}), \ldots, \lambda\Theta(c_{N-1,\ell-1}), \Theta(c_{0,0}), \Theta(c_{0,1}), \ldots, \Theta(c_{0,\ell-1}), \ldots, \\ \Theta(c_{N-2,0}), \Theta(c_{N-2,1}), \ldots, \Theta(c_{N-2,\ell-1}) \end{array} \right) \in C_\beta.$$

Then we say that C_β is a $\Theta - \lambda-$quasi-twisted code of length β. If ℓ is the least positive integer satisfies that $\beta = N\ell$, then C_β is said to be a $\Theta - \lambda-$quasi-twisted code with index ℓ. Furthermore, if Θ is the identity map, we call C_β a quasi-twisted code of index l over R.

According to [**?**], we define a Gray map ϕ over R by

$$\phi : R^\beta \to \mathbb{Z}_q^{2\beta}$$
$$\phi(a + ub) = (b, a + b),$$

where $a, b \in \mathbb{Z}_q^\beta$.

Furthermore, for $r = a + ub \in R$, we define a map

$$\Phi : \mathbb{Z}_q R \mapsto \mathbb{Z}_q^3$$

by

$$\Phi(e, r) = (e, \phi(r)) = (e, b, a + b),$$

and it can be extended componentwise $\mathbb{Z}_q^\alpha R^\beta$ to $\mathbb{Z}_q^n$ as

$$\Phi(e_0, e_1, \ldots, e_{\alpha-1}, r_0, r_1, \ldots, r_{\beta-1}) = (e_0, e_1, \ldots, e_{\alpha-1}, \phi(r_0), \phi(r_1), \ldots, \phi(r_{\beta-1})),$$

for all

$$(e_0, e_1, \ldots, e_{\alpha-1}) \in \mathbb{Z}_q^\alpha$$

and

$$(r_0, r_1, \ldots, r_{\beta-1}) \in R^\beta,$$

where $n = \alpha + 2\beta$. Φ is known as the Gray map on $\mathbb{Z}_q^\alpha R^\beta$. Let $a \in \mathbb{Z}_q^{2\beta}$ with $a = (a_0, a_1) = (a^{(0)} \mid a^{(1)})$, $a^{(i)} \in \mathbb{Z}_q^\beta$, for $i = 0, 1$. Let $\sigma^{\otimes 2}$ be a map from $\mathbb{Z}_q^{2\beta}$ to $\mathbb{Z}_q^{2\beta}$ given by

$$\sigma^{\otimes 2}(a) = (\sigma_\lambda(a^{(0)}) \mid \sigma_\lambda(a^{(1)})),$$

where σ_λ is a constacyclic shift from $\mathbb{Z}_q^\beta$ to $\mathbb{Z}_q^\beta$ given by

$$\sigma_\lambda(a^{(i)}) = (\lambda a^{i,\beta-1}, a^{(i,0)}, \ldots, a^{(i,\beta-2)}),$$

for every $a^{(i)} = (a^{(i,0)}, a^{(i,1)}, \ldots, a^{(i,\beta-1)})$ where $a^{(i,j)} \in \mathbb{Z}_q$, for $j = 0, 1, \ldots, \beta-1$. A linear code C_β of length 2β over $\mathbb{Z}_q$ is said to be a quasi-twisted of index 2 if $\sigma^{\otimes 2}(C_\beta) = C_\beta$.

In addition, for each $\Theta \in \mathrm{Aut(R)}$, let $T_\Theta : R^\beta \mapsto R^\beta$ be a linear transformation given by

$$T_\Theta(a_0, a_1 \ldots, a_{\beta-1}) = (\Theta(a_0), \Theta(a_1) \ldots, \Theta(a_{\beta-1})).$$

Remark 4.2. *C_β is a skew constacyclic code if and only if $T_\Theta \circ \rho_\lambda(C_\beta) = C_\beta$.*

Proposition 4.5. *With the previous notation, we have $T_\Theta \circ \phi \circ \rho_\lambda = \sigma^{\otimes 2} \circ \phi$.*

Proof. Let $r_i = a_i + ub_i$ be the elements of R for $i = 0, 1, \ldots, \beta-1$, we have

$$\rho_\lambda(r_0, r_1, \ldots, r_{\beta-1}) = (\lambda r_{\beta-1}, r_0, r_1, \ldots, r_{\beta-2}).$$

If we apply ϕ, we have

$$\begin{aligned} \phi(\rho_\lambda(r)) &= \phi(\lambda r_{\beta-1}, r_0, \ldots, r_{\beta-2}) \\ &= (\lambda b_{\beta-1}, b_0, \ldots, b_{\beta-2}, \lambda(a_{\beta-1} + b_{\beta-1}), a_0 + b_0, \ldots, a_{\beta-2} + b_{\beta-2}). \end{aligned}$$

where $\phi_i(r) = (b_i, a_i + ub_i)$, now we apply T_Θ in the above equation we get,

$$\begin{aligned} T_\Theta \circ \phi(\rho_\lambda(r)) &= T_\Theta(\lambda b_{\beta-1}, b_0, \ldots, b_{\beta-2}, \lambda(a_{\beta-1} + b_{\beta-1}), a_0 + b_0, \ldots, a_{\beta-2} + b_{\beta-2}) \\ &= (\Theta(\lambda b_{\beta-1}), \Theta(b_0), \ldots, \Theta(b_{\beta-2}), \lambda\Theta(a_{\beta-1} + b_{\beta-1}), \Theta(a_0 + b_0), \ldots, \Theta(a_{\beta-2} + b_{\beta-2})), \end{aligned}$$

since λ is fixed by Θ and by (**??**), for any $a \in \mathbb{Z}_q$, we have $\Theta(a) = a$. So, we have

$$T_\Theta \circ \phi \circ \rho_\lambda(r) = \begin{pmatrix} \lambda b_{\beta-1}, b_0, \ldots, b_{\beta-2}, \lambda(a_{\beta-1} + b_{\beta-1}), \\ (a_0 + b_0), \ldots, (a_{\beta-2} + b_{\beta-2}) \end{pmatrix}.$$

For the other direction,

$$\begin{aligned} \sigma^{\otimes 2}(\phi(r)) &= \sigma^{\otimes 2}(b_0, b_1, \ldots, b_{\beta-1}, a_0 + b_0, a_1 + b_1, \ldots, a_{\beta-1} + b_{\beta-1}) \\ &= \begin{pmatrix} \lambda b_{\beta-1}, b_0, \ldots, b_{\beta-2}, \lambda(a_{\beta-1} + b_{\beta-1}), \\ (a_0 + b_0), \ldots, (a_{\beta-2} + b_{\beta-2}) \end{pmatrix}, \end{aligned}$$

and the result follows. □

As a consequence of the above Proposition, we have the following theorem.

Theorem 4.6. *Let C_β be a code of length β over R. Then C_β is a skew $\lambda-$constacyclic code of length β over R if and only if $\phi(C_\beta)$ is a quasi-twisted code of length 2β over $\mathbb{Z}_q$ of index 2.*

Proof. The necessary part follows from Proposition **??**, i.e.,

$$\sigma^{\otimes 2} \circ \phi(C_\beta) = T_\Theta \circ \phi \circ \rho_\lambda(C_\beta) = \phi(C_\beta).$$

For the sufficient part, assume that $\phi(C_\beta)$ is a quasi-twisted code of index 2, then

$$\phi(C_\beta) = \sigma^{\otimes 2} \circ \phi(C_\beta) = T_\Theta \circ \phi \circ \rho_\lambda(C_\beta).$$

The injectivity of ϕ implies that $T_\Theta\left(\rho_\lambda(C_\beta)\right) = C_\beta$, i.e., C_β is a skew constacyclic code over R. □

Theorem 4.7. *Let $C = C_\alpha \times C_\beta$ be $\Theta - \lambda-$constacyclic code of length $n = \alpha + 2\beta$ over $\mathbb{Z}_q[x]/\langle x^\alpha - \eta(\lambda)\rangle \times R[x,\Theta]/\langle x^\beta - \lambda\rangle$.*

(i) If $\alpha = \beta$, then $\Phi(C)$ is a quasi-twisted code of index 3 and length 3α.

(ii) If $\alpha \neq \beta$ and $\lambda = 1$, then $\Phi(C)$ is a generalized quasi cyclic code of index 3.

Proof. Assume that $C = C_\alpha \times C_\beta$ is a skew $\lambda-$constacyclic code over $\mathbb{Z}_q R$ then by Theorem **??**, we have that C_α is a constacyclic codes over $\mathbb{Z}_q$ and C_β is skew constacyclic codes over R. Further, from Theorem **??**, we have that, if C_β is skew constacyclic code over R then $\phi(C_\beta)$ is a quasi twisted code of length 2β over $\mathbb{Z}_q$ of index 2. Which implies that

$$\Phi(e,r) = \begin{pmatrix} \lambda e_{\alpha-1}, e_0, \ldots, e_{\alpha-2}, \lambda b_{\beta-1}, b_0, \ldots, b_{\beta-2}, \\ \lambda(a_{\beta-1} + b_{\beta-1}), (a_0 + b_0), \ldots, (a_{\beta-2} + b_{\beta-2}) \end{pmatrix},$$

for any $(e_0, e_1, \ldots, e_{\alpha-1}, r_0, r_1, \ldots, r_{\beta-1}) \in C$. Therefore,

1. if $\alpha = \beta$, then $\Phi(C)$ is a quasi-twisted code of length 3α over $\mathbb{Z}_q$ of index 3.
2. if $\alpha \neq \beta$ and $\lambda = 1$, then according to [**?**], $\Phi(C)$ is a generalized quasi-cyclic code of index 3.

□

4.5 The generators and the spanning sets for $\mathbb{Z}_q R-$skew constacyclic codes

In this section, we find a set of generators for $\mathbb{Z}_q R-$skew constacyclic codes as a left $R[x,\Theta]-$submodules of $\mathbb{Z}_q[x]\langle x^\alpha - \eta(\lambda)\rangle \times R[x,\Theta]/\langle x^\beta - \lambda\rangle$. Let C be a $\mathbb{Z}_q R-$skew constacyclic codes, C and $R[x,\Theta]/\langle x^\beta - \lambda\rangle$ are $R[x,\Theta]-$modules and w define the following mapping:

$$\Psi : C \to R[x,\Theta]/\langle x^\beta - \lambda\rangle$$

where

$$\Psi(f_1(x), f_2(x)) = f_2(x).$$

It is clear that Ψ is a module homomorphism whose image is a $R[x,\Theta]-$submodule of $R[x,\Theta]/\langle x^\beta - \lambda\rangle$ and $ker(\Psi)$ is a submodule of C.

Proposition 4.8. *Let C be a skew constacyclic code of length n over $\mathbb{Z}_q R$. Then*

$$C = \langle (f(x), 0), (l(x), a(x) + ug(x))\rangle,$$

where $f(x) \mid (x^\alpha - \eta(\lambda))$ and $g(x) \mid a(x) \mid (x^\beta - \lambda)$.

Proof. Assume that β is a positive integer coprime to the characteristic of R, by similarly theory of cyclic codes over $\mathbb{Z}_2\mathbb{Z}_4$ (see. [**?**]) we have that

$$\Psi(C) = (a(x) + ug(x)) \text{ with } a(x), g(x) \in R[x,\Theta] \text{ and } g(x) \mid a(x) \mid (x^\beta - \lambda).$$

Note that:

$$\ker(\Psi) = \{(f(x), 0) \in C : f(x) \in \mathbb{Z}_q[x]/\langle x^\alpha - \eta(\lambda)\rangle\}.$$

Define the set I to be

$$I = \{f(x) \in \mathbb{Z}_q[x]/\langle x^\alpha - \eta(\lambda)\rangle : (f(x), 0) \in \ker(\Psi)\}.$$

Clearly, I is an ideal of $\mathbb{Z}_q[x]/\langle x^\alpha - \eta(\lambda)\rangle$. Therefore, there exist a polynomial

$$f(x) \in \mathbb{Z}_q[x]/\langle x^\alpha - \eta(\lambda)\rangle,$$

such that

$$I = \langle f(x) \rangle.$$

Now, for any element

$$(c_1(x), 0) \in \ker(\Psi),$$

we have

$$c_1(x) \in I = \langle f(x) \rangle$$

and there exists some polynomials

$$m(x) \in \mathbb{Z}_q[x]/\langle x^\alpha - \eta(\lambda) \rangle$$

such that

$$c_1(x) = m(x)f(x).$$

Thus

$$(c_1(x), 0) = m(x) * (f(x), 0),$$

which implies that $\ker(\Psi)$ is a left submodule of C generated by one element of the form $(f(x), 0)$ where $f(x) \mid (x^\alpha - \eta(\lambda))$. Thus, by the first isomorphism theorem, we have

$$C/\ker(\Psi) \cong \langle a(x) + ug(x) \rangle.$$

Let $(l(x), a(x) + ug(x)) \in C$, with

$$\Psi(l(x), a(x) + ug(x)) = \langle a(x) + ug(x)) \rangle.$$

Then any $\mathbb{Z}_q R-$skew constacyclic code of length (α, β) can be generated as left $R[x, \Theta]-$submodule of

$$\mathbb{Z}_q[x]/\langle x^\alpha - \eta(\lambda) \rangle \times R[x, \Theta]/\langle x^\beta - \lambda \rangle$$

by two elements of the form $(f(x), 0)$ and $(l(x), a(x) + ug(x))$, in other word, any element in the code C can be described as

$$d_1(x) * (f(x), 0) + d_2(x) * (l(x), a(x) + ug(x)),$$

where $d_1(x)$ and $d_2(x)$ are polynomials in the ring $R[x, \Theta]$. In fact, the element $d_1(x)$ can be restricted to be an element in the ring $\mathbb{Z}_q[x]$. We will write this as:

$$C = \langle (f(x), 0), (l(x), a(x) + ug(x)) \rangle,$$

where, $f(x) \mid (x^\alpha - \eta(\lambda))$ and $g(x) \mid a(x) \mid (x^\beta - \lambda)$. □

Lemma 4.6. *If* $C = \langle (f(x), 0), (l(x), a(x) + ug(x)) \rangle$ *is a* $\mathbb{Z}_q R-$*skew constacyclic code, then we may assume that deg* $(l(x)) \leq$ *deg* $(f(x))$.

Proof. Suppose that deg $(l(x)) \geq$ deg $(f(x))$ with deg $(l(x)) = i$. Consider an other $\mathbb{Z}_q R-$skew constacyclic code of length (α, β) with generators of the form

$$\begin{aligned} D &= \langle (f(x), 0), (l(x), a(x) + ug(x)) + x^i * (f(x), 0) \rangle \\ &= \langle (f(x), 0), (l(x) + x^i f(x), a(x) + ug(x)) \rangle. \end{aligned}$$

Clearly, $D \subseteq C$. However, we also have that:

$$(l(x), a(x) + ug(x)) = (l(x) + x^i f(x), a(x) + ug(x)) - x^i * (f(x), 0),$$

which implies that $(l(x), a(x) + ug(x)) \in C$. Therefore, $C \subseteq D$ implying $C = D$. □

Lemma 4.7. *If* $C = \langle (f(x), 0), (l(x), a(x) + ug(x)) \rangle$ *is a* $\mathbb{Z}_q R-$*skew constacyclic code, then we may assume that* $f(x) \mid \frac{x^\beta - \lambda}{g(x)} l(x)$.

Proof. Since

$$\frac{x^\beta - \lambda}{g(x)} * (l(x), a(x) + ug(x)) = (\frac{x^\beta - \lambda}{g(x)} l(x), 0),$$

it follow that

$$\Psi(\frac{x^\beta - \lambda}{g(x)} * (l(x), a(x) + ug(x))) = 0.$$

Therefore,

$$(\frac{x^\beta - \lambda}{g(x)} l(x), 0) \in \ \ker(\Psi) \subseteq C$$

and

$$f(x) \mid (\frac{x^\beta - \lambda}{g(x)}) l(x).$$

□

The above Lemma shows that if the $\mathbb{Z}_qR-$skew constacyclic code C has only one generator of the form $C = \langle l(x), a(x) + ug(x)\rangle$ then, $(x^\alpha - \eta(\lambda)) \mid \frac{x^\beta-\lambda}{g(x)}l(x)$ with $g(x) \mid a(x) \mid (x^\beta - \lambda)$. Thus from this discussion and Lemma **??** and **??**, we have the following results.

Theorem 4.9. *Let C be a skew constacyclic code of length n over $\mathbb{Z}_qR$. Then C can be identified uniquely as*

$$C = \langle (f(x), 0), (l(x), a(x) + ug(x))\rangle,$$

where $f(x) \mid (x^\alpha - \eta(\lambda))$ and $g(x) \mid a(x) \mid (x^\beta - \lambda)$. and $l(x)$ is a skew polynomial satisfying deg $(l(x)) \leq$ deg $(f(x))$ and $f(x) \mid \frac{x^\beta-\lambda}{g(x)}l(x)$.

Proof. Following from Proposition **??**, Lemma **??** and **??**, we can easily see that $C = \langle (f(x), 0), (l(x), a(x)+ ug(x))\rangle$,where the polynomials $f(x), l(x), a(x)$ and $g(x)$ are stated in the theorem. Now, we will prove the uniqueness of the generators. Since $\langle f(x)\rangle$ and $\langle a(x) + ug(x)\rangle$ are skew constacyclic codes over $\mathbb{Z}_q$ and R respectively, then, the skew polynomials $f(x), a(x)$ and $g(x)$ are unique. Now, suppose that

$$\begin{aligned} C &= \langle (f(x), 0), (l_1(x), a(x) + ug(x))\rangle \\ &= \langle (f(x), 0), (l_2(x), a(x) + ug(x))\rangle, \end{aligned}$$

then, we have

$$((l_1(x) - l_2(x)), 0) \in \text{ ker } (\Psi) = \langle f(x), 0\rangle,$$

which implies that

$$l_1(x) - l_2(x) = f(x)j(x),$$

for some skew polynomial $j(x)$, and since deg $(l_1(x) - l_2(x)) \leq$ deg $(l_1(x)) \leq$ deg $(f(x))$ then $j(x) = 0$ and $l_1(x) = l_2(x)$. □

Definition 4.7. *Let A be an $R-$module. A linearly independent subset B of A that spans A is called a basis of A. If an $R-$module has a basis, then it is called a free $R-$module.*

Note that if C is a $\mathbb{Z}_qR-$skew constacyclic code of the form

$$C = \langle (f(x), 0), (l(x), a(x) + ug(x))\rangle,$$

with $g(x) \neq 0$, then C is a free $R-$module. If C is not of this form then it is not a free $R-$module. But we still present a minimal spanning set for the code. The following theorem gives us a spanning minimal set for $\mathbb{Z}_q R-$skew constacyclic codes.

Theorem 4.10. *Let C be a skew constacyclic code of length n over $\mathbb{Z}_q R$, where $f(x), l(x), a(x)$ and $g(x)$ are as in Theorem* **??** *and*

$$f(x)h_f(x) = x^\alpha - \eta(\lambda), a(x)h_a(x) = x^\beta - \lambda, a(x) = g(x)m(x).$$

Let

$$\begin{aligned} S_1 &= \bigcup_{i=0}^{deg\ (h_f)-1} \{x^i * (f(x), 0)\}, \\ S_2 &= \bigcup_{i=0}^{deg\ (h_a)-1} \{x^i * (l(x), a(x) + ug(x))\}, \end{aligned}$$

and

$$S_3 = \bigcup_{i=0}^{deg\ (m)-1} \{x^i * (\eta(h_a(x))l(x), uh_a(x)g(x))\}.$$

Then

$$S = S_1 \cup S_2 \cup S_3,$$

forms a minimal spanning set for C and C has $q^{deg\ (h_f)}q^{2deg\ (h_a)}q^{deg\ (m)}$ codewords.

Proof. Let

$$C(x) = \eta(d(x))(f(x), 0) + e(x)(l(x), a(x) + ug(x)) \in \mathbb{Z}_q[x]/\langle x^\alpha - \eta(\lambda)\rangle \times R[x, \Theta]/\langle x^\beta - \lambda\rangle$$

be a codeword in C where $d(x)$ and $e(x)$ are skew polynomials in $R[x, \Theta]$. Now, if

$$\deg\ (\eta(d(x))) \leq \deg\ (h_f(x)) - 1,$$

then

$$\eta(d(x))(f(x), 0) \in \text{Span}(S_1).$$

Otherwise, by using right division algorithm we have

$$\eta(d(x)) = h_f(x)\eta(q_1(x)) + \eta(r_1(x)),$$

where $q_1(x), r_1(x) \in R[x, \Theta]$ and $\eta(r_1(x)) = 0$ or deg $(\eta(r_1(x))) \leq$ deg $(h_f(x)) - 1$.

Therefore,

$$\begin{aligned} \eta(d(x))(f(x), 0) &= (h_f(x)\eta(q_1(x)) + \eta(r_1(x)))(f(x), 0) \\ &= \eta(r_1(x))(f(x), 0). \end{aligned}$$

Hence, we can assume that

$$\eta(d(x))(f(x), 0) \in \text{Span}(S_1).$$

Now, if

$$\text{deg } (\eta(e(x))) \leq \text{deg } (h_a(x)) - 1,$$

then

$$\eta(e(x))(l(x), a(x) + ug(x)) \in \text{Span}(S_2).$$

Otherwise, again by the right division algorithm, we get polynomials $q_2(x)$ and $r_2(x)$ such that:

$$e(x) = q_2(x)h_a(x) + r_2(x),$$

where

$$r_2(x) = 0 \ \textit{or} \ \text{deg } (r_2(x)) \leq \text{deg } (h_a(x)) - 1.$$

So, we have

$$\begin{aligned} e(x)(l(x), a(x) + ug(x)) &= (q_2(x)h_a(x) + r_2(x))(l(x), a(x) + ug(x)) \\ &= q_2(x)(\eta(h_a(x))l(x), uh_a(x)g(x)) + r_2(x)(l(x), a(x) + ug(x)). \end{aligned}$$

Since

$$r_2(x) = 0 \ \textit{or} \ \text{deg } (r_2(x)) \leq \text{deg } (h_a(x)) - 1,$$

then

$$r_2(x)(l(x), a(x) + ug(x)) \in \text{Span}(S_2).$$

Let us consider

$$q_2(x)(\eta(h_a(x))l(x), uh_a(x)g(x)) \in \text{Span}(S),$$

we know that

$$x^\beta - \lambda = a(x)h_a(x) = g(x)m(x)h_a(x)$$

and also we have

$$f(x) \mid \frac{x^\beta - \lambda}{g(x)} l(x).$$

Therefore,

$$\frac{x^\beta - \lambda}{g(x)} l(x) = f(x)k(x).$$

Again, if

$$\deg\,(q_2(x)) \leq \deg\,(m(x)) - 1$$

then

$$q_2(x)(\eta(h_a(x))l(x), uh_a(x)g(x)) \in \mathrm{Span}(S_3).$$

Otherwise,

$$q_2(x) = \frac{x^\beta - \lambda}{h_a(x)g(x)} q_3(x) + r_3(x),$$

with

$$r_3(x) = 0 \ \textit{or} \ \deg\,(r_3(x)) \leq \deg\,(m(x)) - 1.$$

So,

$$\begin{aligned} q_2(x)(\eta(h_a(x))l(x), uh_a(x)g(x)) &= \left(\tfrac{x^\beta-\lambda}{h_a(x)g(x)} q_3(x)\eta(h_a(x))l(x), \tfrac{x^\beta-\lambda}{h_a(x)g(x)} q_3(x)uh_a(x)g(x)\right) \\ &+ r_3(x)(\eta(h_a(x))l(x), uh_a(x)g(x)) \\ &= \left(\tfrac{x^\beta-\lambda}{h_a(x)g(x)} q_3(x)\eta(h_a(x))l(x), 0\right) + r_3(x)(\eta(h_a(x))l(x), uh_a(x)g(x)). \end{aligned}$$

Since

$$\frac{x^\beta - \lambda}{g(x)} l(x) = f(x)k(x),$$

then

$$\left(\frac{x^\beta - \lambda}{h_a(x)g(x)} q_3(x)\eta(h_a(x))l(x), 0\right) \in \mathrm{Span}(S_1)$$

and hence

$$r_3(x)(\eta(h_a(x))l(x), uh_a(x)g(x)) \in \mathrm{Span}(S_3).$$

Consequently, $S = S_1 \cup S_2 \cup S_3$ forms a minimal spanning set for C. □

4.6 Double skew constacyclic codes over $\mathbb{Z}_q R$

In this subsection, we study double skew constacyclic codes over $\mathbb{Z}_q R$. Let $\acute{n} = \acute{\alpha} + 2\acute{\beta}$ and $\acute{\acute{n}} = \acute{\acute{\alpha}} + 2\acute{\acute{\beta}}$ be integers such that $n = \acute{n} + \acute{\acute{n}}$. We consider a partition of the set of the n coordinates into two subsets of $\acute{n}$ and $\acute{\acute{n}}$ coordinates, respectively, so that C is a subset of $\mathbb{Z}_q^{\acute{\alpha}} R^{\acute{\beta}} \times \mathbb{Z}_q^{\acute{\acute{\alpha}}} R^{\acute{\acute{\beta}}}$.

Definition 4.8. *A linear code C of length n over $\mathbb{Z}_q R$ is called a double skew constacyclic code if C satisfies the following conditions.*

(i) C is an $R-$submodule of $\mathbb{Z}_q^{\acute{\alpha}+\acute{\acute{\alpha}}} R^{\acute{\beta}+\acute{\acute{\beta}}}$.

(ii) $(\eta(\lambda)\Theta(\acute{e}_{\acute{\alpha}-1}), \Theta(\acute{e}_0), \ldots, \Theta(\acute{e}_{\acute{\alpha}-2}), \lambda\Theta(\acute{r}_{\acute{\beta}-1}), \Theta(\acute{r}_0), \ldots, \Theta(\acute{r}_{\acute{\beta}-2}) \mid$
$\eta(\lambda)\Theta(\acute{\acute{e}}_{\acute{\acute{\alpha}}-1}), \Theta(\acute{\acute{e}}_0), \ldots, \Theta(\acute{\acute{e}}_{\acute{\acute{\alpha}}-2}), \lambda\Theta(\acute{\acute{r}}_{\acute{\acute{\beta}}-1}), \Theta(\acute{\acute{r}}_0), \ldots, \Theta(\acute{\acute{r}}_{\acute{\acute{\beta}}-2})) \in C.$

whenever

$$(\acute{e}_0, \ldots, \acute{e}_{\acute{\alpha}-1}, \acute{r}_0, \ldots, \acute{r}_{\acute{\beta}-1} \mid \acute{\acute{e}}_0, \ldots, \acute{\acute{e}}_{\acute{\acute{\alpha}}-1}, \acute{\acute{r}}_0, \ldots, \acute{\acute{r}}_{\acute{\acute{\beta}}-1}) \in C.$$

Remark 4.3. *$\Theta(\acute{e}_i) = \acute{e}_i$ and $\Theta(\acute{\acute{e}}_i) = \acute{\acute{e}}_i$ for $0 \leq i \leq \alpha - 1$, as $\acute{e}_i, \acute{\acute{e}}_i \in \mathbb{Z}_q$ (the fixed ring of Θ).*

Denote by $\mathfrak{R}_{\acute{\alpha},\acute{\beta},\acute{\acute{\alpha}},\acute{\acute{\beta}}}$ the ring:

$$\mathbb{Z}_q[x]/\langle x^{\acute{\alpha}} - \eta(\lambda)\rangle \times R[x,\Theta]/\langle x^{\acute{\beta}} - \lambda\rangle \times \mathbb{Z}_q[x]/\langle x^{\acute{\acute{\alpha}}} - \eta(\lambda)\rangle \times R[x,\Theta]/\langle x^{\acute{\acute{\beta}}} - \lambda\rangle.$$

In polynomial representation, each codeword

$$c = (\acute{e}_0, \acute{e}_1, \ldots, \acute{e}_{\acute{\alpha}-1}, \acute{r}_0, \ldots, \acute{r}_{\acute{\beta}-1} \mid \acute{\acute{e}}_0, \acute{\acute{e}}_1, \ldots, \acute{\acute{e}}_{\acute{\acute{\alpha}}-1}, \acute{\acute{r}}_0, \ldots, \acute{\acute{r}}_{\acute{\acute{\beta}}-1})$$

of a double skew constacyclic code can be represented by four polynomials

$$c(x) = \begin{pmatrix} \acute{e}_0 + \acute{e}_1 x + \cdots + \acute{e}_{\acute{\alpha}-1} x^{\acute{\alpha}-1}, \\ \acute{r}_0 + \acute{r}_1 x + \cdots + \acute{r}_{\acute{\beta}-1} x^{\acute{\beta}-1}, \\ \acute{\acute{e}}_0 + \acute{\acute{e}}_1 x + \cdots + \acute{\acute{e}}_{\acute{\acute{\alpha}}-1} x^{\acute{\acute{\alpha}}-1}, \\ \acute{\acute{r}}_0 + \acute{\acute{r}}_1 x + \cdots + \acute{\acute{r}}_{\acute{\acute{\beta}}-1} x^{\acute{\acute{\beta}}-1} \end{pmatrix} = (\acute{e}(x), \acute{r}(x) \mid \acute{\acute{e}}(x), \acute{\acute{r}}(x)) \in \mathfrak{R}_{\acute{\alpha},\acute{\beta},\acute{\acute{\alpha}},\acute{\acute{\beta}}}.$$

Let

$$h(x) = h_0 + h_1 x + \cdots + h_t x^t \in R\,[x,\Theta]$$

and let

$$(\acute{f}(x), \acute{g}(x) \mid \acute{\acute{f}}(x), \acute{\acute{g}}(x)) \in \mathfrak{R}_{\acute{\alpha},\acute{\beta},\acute{\acute{\alpha}},\acute{\acute{\beta}}}.$$

We define the multiplication of $h(x)$ and $(\acute{f}(x), \acute{g}(x) \mid \acute{\acute{f}}(x), \acute{\acute{g}}(x))$ by

$$h(x)(\acute{f}(x), \acute{g}(x) \mid \acute{\acute{f}}(x), \acute{\acute{g}}(x)) = (\eta(h(x))\acute{f}(x), h(x)\acute{g}(x) \mid \eta(h(x))\acute{\acute{f}}(x), h(x)\acute{\acute{g}}(x)),$$

where $\eta(h(x)) = \eta(h_0)+\eta(h_1)x+\cdots+\eta(h_t)x^t$. This gives us the following Theorem. But before that, we need to give the following Remark.

Remark 4.4. *If* $c(x) = (\acute{e}(x), \acute{r}(x) \mid \acute{\acute{e}}(x), \acute{\acute{r}}(x))$ *represents the code word* c*, then* $xc(x)$ *represents the* $\acute{n}\acute{\acute{n}}-$*skew constacyclic shift of* c*.*

Theorem 4.11. *A linear code* C *is a double skew constacyclic code if and only if it is a left* $R[x,\Theta]-$*submodule of the left-module* $\mathfrak{R}_{\acute{\alpha},\acute{\beta},\acute{\alpha},\acute{\beta}}$*.*

Proof. Assume that C is a double skew constacyclic code. Let $c \in C$, and let the associated polynomial of c be $c(x) = (\acute{e}(x), \acute{r}(x) \mid \acute{\acute{e}}(x), \acute{\acute{r}}(x))$. Since $xc(x)$ is an $\acute{n}\acute{\acute{n}}-$skew constacyclic shift of c. (See Remark **??**), then $xc(x) \in C$. Further, by the linearity of C, it follows that $h(x)c(x) \in C$, for any $h(x) \in R[x,\Theta]$. Therefore C is a left $R[x,\Theta]-$submodule of $\mathfrak{R}_{\acute{\alpha},\acute{\beta},\acute{\alpha},\acute{\beta}}$. Converse is straightforward. □

4.7 New linear codes over $\mathbb{Z}_4$

Codes over $\mathbb{Z}_4$, sometimes called quaternary codes as well, have a special place in coding theory. Due to their importance, a database of quaternary codes was introduced in [**?**] and it is available online [**?**]. Hence we consider the case $q = 4$ to possibly obtain quaternary codes with good parameters. We conducted a computer search using Magma software [**?**] to find skew cyclic codes over $\mathbb{Z}_4(\mathbb{Z}_4+u\mathbb{Z}_4)$ whose Gray images are quaternary linear codes with better parameters than the currently best known codes. We have found ten such codes which are listed in the table below.

The automorphism of $R = \mathbb{Z}_4 + u\mathbb{Z}_4$ that we used is $\Theta(a + bu) = a + 3bu = a - bu$. In addition to the Gray map given in Section 4.1, there are many other possible linear maps

from $\mathbb{Z}_4 + u\mathbb{Z}_4$ to $\mathbb{Z}_4^\ell$ for various values of ℓ. For example, the following map was used in [**?**] $a + bu \to (b, 2a + 3b, a + 3b)$ which triples the length of the code. We used both of these Gray maps in our computations, and obtained new codes from each map.

We first chose a cyclic code C_α over $\mathbb{Z}_4$ generated by $g_\alpha(x)$. The coefficients of this polynomial is given in ascending order of the terms in the table. Therefore, the entry 31212201, for example, represents the polynomial $3+x+2x^2+x^3+2x^4+2x^5+x^7$. Then we searched for divisors of $x^\beta-1$ in the skew polynomial ring $R[x,\Theta]$ where $R = \mathbb{Z}_4+u\mathbb{Z}_4$ and $\Theta(a+bu) = a-bu$. For each such divisor $g_\beta(x)$ we constructed the skew cyclic code over $\mathbb{Z}_4R$ generated by $(g_\alpha(x), g_\beta(x))$ and its $\mathbb{Z}_4$-images under each Gray map described above. As a result of the search, we obtained ten new linear codes over $\mathbb{Z}_4$. They are now added to the database ([**?**]) of quaternary codes. In the table below, which Gray map is used to obtain each new code is not explicitly stated, but it can be inferred from the values of α, β and n, the length of the $\mathbb{Z}_4$ image. If $n = \alpha + 2\beta$, then it is the map given in section 4.1 and if $n = \alpha + 3\beta$ it is the map described in this section. For example, the second code in the table has length $57 = 15 + 3 \cdot 14$. This means that the Gray map that triples the length of a code over R is used to obtain this code.

When $x^\beta - 1 = g(x)h(x)$ we can use either the generator polynomial $g(x)$ or the parity check polynomial $h(x)$ to define the skew cyclic code over R. For the codes given in the table below we used the parity check polynomial because it has smaller degree. In general a linear code C over $\mathbb{Z}_4$ has parameters $[n, 4^{k_1}2^{k_2}]$, and when $k_2 = 0$, C is a free code. In this case C has a basis with k vectors just like a linear code over a field. All of the codes in the table below are free codes, hence we will simply denote their parameters by $[n, k, d]$ where d is the Lee weight over $\mathbb{Z}_4$.

Our computational results suggest that considering skew cyclic and skew constacyclic codes over $\mathbb{Z}_q(\mathbb{Z}_q + u\mathbb{Z}_q)$ is promising to obtain codes with good parameters over $\mathbb{Z}_q$.

Table 4.1: New quaternary codes

$\boldsymbol{\alpha}$	$\boldsymbol{\beta}$	$\mathbf{g}_{\boldsymbol{\alpha}}$	$\mathbf{g}_{\boldsymbol{\beta}}$	$\mathbb{Z}_4$ **Parameters**
15	14	31212201	$x^4 + (u+1)x^3 + x^2 + (3u+2)x + 3u + 3$	$[43, 8, 26]$
15	14	31212201	$x^4 + (u+1)x^3 + x^2 + (3u+2)x + 3u + 3$	$[57, 8, 38]$
15	14	3021310231	$x^3 + 2ux^2 + (3u+3)x + 2u + 3$	$[43, 6, 30]$
15	14	3021310231	$x^3 + 3x^2 + (3u+2)x + 1$	$[57, 6, 42]$
7	14	3121	$x^4 + (3u+3)x^3 + 3x^2 + (u+2)x + 3u + 3$	$[35, 8, 20]$
7	14	3121	$x^4 + (u+3)x^3 + (u+1)x^2 + (u+2)x + 3u + 3$	$[49, 8, 32]$
7	14	12311	$x^3 + (2u+1)x^2 + 3ux + 3u + 3$	$[35, 6, 22]$
7	14	12311	$x^3 + (2u+1)x^2 + ux + u + 1$	$[35, 6, 24]$
7	14	12311	$x^3 + ux^2 + (3u+3)x + 1$	$[49, 6, 35]$
7	14	12311	$x^3 + (u+2)x^2 + x + 1$	$[49, 6, 36]$

Chapter 5

$\mathbb{Z}_q(\mathbb{Z}_q + u\mathbb{Z}_q + \ldots + u^{m-1}\mathbb{Z}_q)-$ Linear cyclic and constacyclic codes

In this chapter, we study cyclic and constacyclic codes over the ring $\mathbb{Z}_q(\mathbb{Z}_q+u\mathbb{Z}_q+\ldots+u^{m-1}\mathbb{Z}_q)$, where $q = p^s$, p is a prime and $u^m = 0$. We give the definition of these codes as subsets of the ring $\mathbb{Z}_q(\mathbb{Z}_q + u\mathbb{Z}_q + \ldots + u^{m-1}\mathbb{Z}_q)$. These codes can be identified as submodules of the $\Re[x]-$module $\mathbb{Z}_q[x]/\langle x^\alpha - 1\rangle \times \Re[x]/\langle x^\alpha - \lambda\rangle$, were $\Re = \mathbb{Z}_q + u\mathbb{Z}_q + \ldots + u^{m-1}\mathbb{Z}_q$. Apart of this chapter appeared in [**?**].

5.1 Linear codes over the ring $\Re$

In this section, we introduce and study cyclic and constacyclic codes over the ring $\Re = \mathbb{Z}_q + u\mathbb{Z}_q + \ldots + u^{m-1}\mathbb{Z}_q$, where q is a prime power and $u^m = 0$. We generalize the structure and properties from [**?**] to codes over $\mathbb{Z}_q + u\mathbb{Z}_q + \ldots + u^{m-1}\mathbb{Z}_q$. Hence the proofs of many of the theorems will be omitted.

5.1.1 Cyclic codes over the ring $\Re$

Consider the ring $\Re = \mathbb{Z}_q + u\mathbb{Z}_q + \ldots + u^{m-1}\mathbb{Z}_q$, where $q = p^s$, p is a prime and $u^m = 0$. The ring $\Re$ is isomorphic to the quotient ring $\mathbb{Z}_q[u]/\langle u^m\rangle$. The ring $\Re$ is a commutative not chain

ring with maximal ideal $\langle p, u\rangle$. Each element r of $\Re$ can be expressed uniquely as

$$r = r_0 + ur_1 + \ldots + u^{m-1}r_{m-1}, \text{ where } r_i \in \mathbb{Z}_q, i = 0, 1, \ldots m-1.$$

Definition 5.1. *A linear code C_β of length β over the ring $\Re$ is $\Re-$submodule of $\Re^\beta$.*

Next we define the cyclic codes over the ring $\Re$. Let ρ be the standard cyclic shift operator on $\Re^\beta$.

A linear code C_β of length β over $\Re$ is cyclic if

$$\rho(c_0, c_1, \ldots, c_{\beta-1}) = (c_{\beta-1}, c_0, \ldots, c_{\beta-2}) \in C_\beta$$

whenever

$$(c_0, c_1, \ldots, c_{\beta-}) \in C_\beta.$$

We introduce an inner product on $(\mathbb{Z}_q + u\mathbb{Z}_q + \ldots + u^{m-1}\mathbb{Z}_q)^\beta$. Further, the Euclidean inner product defined by

$$\langle v', w'\rangle = \sum_{i=0}^{\beta-1} v'_i w'_i,$$

for $v' = (v'_0, v'_1, \ldots, v'_{\beta-1})$ and $w' = (w'_0, w'_1, \ldots, w'_{\beta-1})$ in $\Re^\beta$.

Definition 5.2. *Let C be a linear code over $\Re$ of length β. then we define the dual of C_β as*

$$C_\beta^\perp = \{v' \in \Re^\beta | \langle v', w'\rangle = 0, \forall w' \in C_\beta\}.$$

Lemma 5.1. *Let C_β be a code of length β over $\Re$. Then C_β is cyclic if and only if $C_\beta^\perp$ is cyclic over $\Re$ of length β.*

Proof. Let $v' = (v'_0, v'_1, \ldots, v'_{\beta-1}) \in C_\beta$ and $w' = (w'_0, w'_1, \ldots, w'_{\beta-1}) \in C_\beta^\perp$ be two arbitrary elements. Since C_β is cyclic code,

$$\rho^{\beta-1}(v') = (v'_1, v'_2, \ldots, v'_{\beta-1}, v'_0) \in C_\beta.$$

Then, we have

$$\begin{aligned} 0 &= \langle \rho^{\beta-1}(v'), w' \rangle \\ &= \langle (v'_1, v'_2, \ldots, v'_{\beta-1}, v'_0), (w'_0, \ldots, w'_{\beta-1}) \rangle \\ &= \langle (v'_1, v'_2, \ldots, v'_{\beta-1}, v'_0), (w'_0, \ldots, w'_{\beta-1}) \rangle \\ &= v'_0 w'_{\beta-1} + \sum_{j=1}^{\beta-1} v'_j w'_{j-1} \\ &= \langle \rho^{\beta-1}(w'), v' \rangle \end{aligned}$$

This implies that, $\rho(w') \in C_\beta^\perp$. Then C_β is a cyclic code. The converse follows from the fact that $(C_\beta^\perp)^\perp = C_\beta$. □

5.1.2 Constacyclic codes over the ring $\Re$

In this subsection, we define the $\lambda-$constacyclic codes over the ring $\Re$. Let ρ_λ be the standard $\lambda-$constacyclic shift operator on $\Re^\beta$. A linear code C_β of length β over $\Re$ is cyclic if

$$\rho_\lambda(c_0, c_1, \ldots, c_{\beta-1}) = (\lambda c_{\beta-1}, c_0, \ldots, c_{\beta-2}) \in C_\beta$$

whenever

$$(c_0, c_1, \ldots, c_{\beta-}) \in C_\beta.$$

Lemma 5.2. *Let C_β be a code of length β over $\Re$. Then C_β is $\lambda-$constacyclic if and only if $C_\beta^\perp$ is $\lambda^{-1}-$constacyclic over $\Re$ of length β..*

Proof. Let $v' = (v'_0, v'_1, \ldots, v'_{\beta-1}) \in C_\beta$ and $w' = (w'_0, w'_1, \ldots, w'_{\beta-1}) \in C_\beta^\perp$ be two arbitrary elements. Since C_β is cyclic code,

$$\rho_\lambda^{\beta-1}(v') = (\lambda v'_1, \lambda v'_2, \ldots, \lambda v'_{\beta-1}, v'_0) \in C_\beta.$$

Then, we have

$$\begin{aligned} 0 &= \langle \rho_\lambda^{\beta-1}(v'), w' \rangle \\ &= \langle (\lambda v'_1, \lambda v'_2, \ldots, \lambda v'_{\beta-1}, v'_0), (w'_0, \ldots, w'_{\beta-1}) \rangle \\ &= \lambda \langle (v'_1, v'_2, \ldots, v'_{\beta-1}, \lambda^{-1} v'_0), (w'_0, \ldots, w'_{\beta-1}) \rangle \\ &= \lambda(\lambda^{-1} v'_0 w'_{\beta-1} + \sum_{j=1}^{\beta-1} v'_j w'_{j-1}) \\ &= \lambda \langle \rho_{\lambda^{-1}}^{\beta-1}(w'), v' \rangle \end{aligned}$$

This implies that, $\rho_\lambda^{-1}(w') \in C_\beta^\perp$. Then C_β is a $\lambda^{-1}-$constacyclic code. The converse follows from the fact that $(C_\beta^\perp)^\perp = C_\beta$. □

5.2 Linear codes over ring $\mathbb{Z}_q\Re$

In this section, we present some basic results on linear codes over the ring $\mathbb{Z}_q(\mathbb{Z}_q + u\mathbb{Z}_q + \ldots + u^{m-1}\mathbb{Z}_q)$.

Let $n = \alpha + m\beta$ where α and β are positive integers. We consider the ring $\mathbb{Z}_q$ with q elements and the ring $\Re = \mathbb{Z}_q + u\mathbb{Z}_q + \ldots + u^{m-1}\mathbb{Z}_q$, where $u^m = 0$. We construct the ring

$$\mathbb{Z}_q\Re = \{(e, r) | e \in \mathbb{Z}_q \ and \ r \in \Re\}.$$

The ring $\mathbb{Z}_q\Re$ is not an $\Re-$ module under the operation of standard multiplication.

To make the ring $\mathbb{Z}_q\Re$ an $\Re-$ module, this is an extension of the following result due to Abualrbub [**?**].

$$\begin{aligned} \eta : \mathbb{Z}_q\Re &\to \mathbb{Z}_q \\ r_0 + ur_1 + \ldots + u^{m-1}r_{m-1} &\mapsto \eta(r_0 + ur_1 + \ldots + u^{m-1}r_{m-1}) = r_0. \end{aligned}$$

For $d \in \Re$, the multiplication is defined as

$$d * (e, r) = (\eta(d)e, de_2r).$$

This multiplication can be generalized over the ring $\mathbb{Z}_q^\alpha R^\beta$ in the following way:

for any $d \in \Re$ and $v = (e_0, e_1, \ldots, e_{\alpha-1}, r_0, r_1, \ldots, r_{\beta-1}) \in \mathbb{Z}_q^\alpha\Re^\beta$ define

$$dv = (\eta(d)e_0, \eta(d)e_1, \ldots, \eta(d)e_{\alpha-1}, dr_0, dr_1, \ldots, dr_{\beta-1}).$$

The following results are analogous to the ones obtained in [**?**, **?**] for the ring $\mathbb{Z}_2(\mathbb{Z}_2 + u\mathbb{Z}_2)$.

Lemma 5.3. *The ring $\mathbb{Z}_q^\alpha\Re^\beta$ is an $\Re$-module under the above definition.*

Lemma **??** allows us to give the next definition.

Definition 5.3. *A non-empty subset C of $\mathbb{Z}_q^\alpha\Re^\beta$ is called a $\mathbb{Z}_q\Re$-linear code if it is an $\Re$-submodule of $\mathbb{Z}_q^\alpha\Re^\beta$.*

The following results and definitions are analogous to the ones obtained in [**?**].

Let C be a $\mathbb{Z}_q\Re$-linear code and let C_α (respectively C_β) be the canonical projection of C on the first α (respectively on the last β) coordinates. Since the canonical projection is a linear map, C_α and C_β are linear codes over $\mathbb{Z}_q$ and over $\Re$ of length α and β, respectively. A code C is called separable if C is the direct product of C_α and C_β, i.e.,

$$C = C_\alpha \times C_\beta.$$

We introduce an inner product on $\mathbb{Z}_q^\alpha\Re^\beta$. For any two vectors

$$v = (v_0, \ldots, v_{\alpha-1}, v'_0, \ldots, v'_{\beta-1}), w = (w_0, \ldots, w_{\alpha-1}, w'_0, \ldots, w'_{\beta-1}) \in \mathbb{Z}_q^\alpha R^\beta$$

let

$$\langle v, w\rangle = u^{m-1}\sum_{i=0}^{\alpha-1} v_i w_i + \sum_{j=0}^{\beta-1} \acute{v}_j \acute{w}_j.$$

Let C be a $\mathbb{Z}_q\Re$-linear code. The dual of C is defined by

$$C^\perp = \{v \in \mathbb{Z}_q^\alpha\Re^\beta;\ \langle v, w\rangle = 0, \forall w \in C\}.$$

If $C = C_\alpha \times C_\beta$ is separable, then

$$C^\perp = C_\alpha^\perp \times C_\beta^\perp. \tag{5.1}$$

5.3 $\mathbb{Z}_q\Re-$ Linear cyclic codes

In this section give some useful results on cyclic codes over $\mathbb{Z}_q^\alpha\Re^\beta$. Let

$$\mathbb{Z}_q^\alpha R^\beta = \{(e_0, e_1, \ldots, e_{\alpha-1}, r_0, r_1, \ldots, r_{\beta-1}) | e_0, e_1, \ldots, e_{\alpha-1} \in \mathbb{Z}_q \text{ and } r_0, r_1, \ldots, r_{\beta-1} \in \Re\}.$$

A nonenempty sebset C of $\mathbb{Z}_q^\alpha\Re^\beta$ is called a $\mathbb{Z}_q\Re-$linear code if C is an $\Re-$submodule of $\mathbb{Z}_q^\alpha\Re^\beta$.

Definition 5.4. *Sebset C of $\mathbb{Z}_q^\alpha\Re^\beta$ is called $\mathbb{Z}_q\Re-$linear cyclic codes if*

1. *C is a linear code.*

2. If

$$(e_0, e_1, \ldots, e_{\alpha-1}, r_0, r_1, \ldots, r_{\beta-1}) \in C$$

then

$$(e_{\alpha-1}, e_0, \ldots, e_{\alpha-2}, r_{\beta-1}, r_0, \ldots, r_{\beta-2}) \in C.$$

In polynomial representation, the codewords $(e_{\alpha-1}, e_0, \ldots, e_{\alpha-2}, r_{\beta-1}, r_0, \ldots, r_{\beta-2})$ of cyclic code consisting of two polynomials

$$\begin{aligned} c(x) &= \begin{pmatrix} e_0 + e_1x + \ldots + e_{\alpha-1}x^{\alpha-1}, \\ r_0 + r_1x + \ldots + r_{\beta-1}x^{\beta-1} \end{pmatrix} \\ &= (e(x), r(x)) \in \mathbb{Z}_q[x]/\langle x^\alpha - 1\rangle \times \Re[x]/\langle x^\beta - 1\rangle. \end{aligned}$$

Let

$$f(x) = f_0 + f_1x + \ldots + f_tx^t \in \Re\ [x]$$

and let

$$(g(x), h(x)) \in \mathbb{Z}_q[x]/\langle x^\alpha - 1\rangle \times \Re[x]/\langle x^\beta - 1\rangle$$

the multiplucation is defined by tha basic rule

$$f(x) * (g(x), h(x)) = (\eta(f(x))g(x), f(x)h(x)).$$

Where

$$\eta(f(x)) = \eta(f_0) + \eta(f_1)x + \ldots + \eta(f_1)x^t.$$

The multiplication above is well-defined. Moreover, $\mathbb{Z}_q[x]/\langle x^\alpha - 1\rangle \times \Re[x]/\langle x^\beta - 1\rangle$ is an $\Re[x]$-module with respect this muliplucation.

Theorem 5.1. *Let C be a linear code over $\mathbb{Z}_q\Re$ of length (α, β), and let $C = C_\alpha \times C_\beta$, where C_α is linear code over $\mathbb{Z}_q$ of length α and C_β is linear code over $\Re$ of length β. Then C is a cyclic code if and only if C_α is a cyclic code over $\mathbb{Z}_q$ and C_β is a cyclic code over $\Re$.*

Proof. Let $(e_0, e_1, \ldots, e_{\alpha-1}) \in C_\alpha$ and let $(r_0, r_1, \ldots, r_{\beta-1}) \in C_\beta$. If $C = C_\alpha \times C_\beta$ is a cyclic code, then

$$(e_{\alpha-1}, e_0, \ldots, e_{\alpha-1}, r_{\beta-1}, r_0, \ldots, r_{\beta-1}) \in C,$$

then

$$(e_{\alpha-1}, e_0, \ldots, e_{\alpha-1}) \in C_\alpha$$

and

$$(r_{\beta-1}, r_0, \ldots, r_{\beta-1}) \in C_\beta.$$

Hence, C_α is a cyclic code over $\mathbb{Z}_q$ and C_β is a cyclic code over $\Re$.

On the other hand, suppose that C_α is a cyclic code over $\mathbb{Z}_q$ and C_β is a cyclic code over $\Re$. Note that

$$(e_{\alpha-1}, e_0, \ldots, e_{\alpha-1}) \in C_\alpha$$

and

$$(r_{\beta-1}, r_0, \ldots, r_{\beta-1}) \in C_\beta.$$

Since $C = C_\alpha \times C_\beta$, then

$$(e_{\alpha-1}, e_0, \ldots, e_{\alpha-1}, r_{\beta-1}, r_0, \ldots, r_{\beta-1}) \in C,$$

so C is a cyclic code over $\mathbb{Z}_q\Re$. □

Corollary 5.1. *Let $C = C_\alpha \times C_\beta$ is cyclic over $\mathbb{Z}_q\Re$, then its dual code $C^\perp$ is also cyclic and moreover we have $C = C_\alpha^\perp \times C_\beta^\perp$.*

Proof. From Equation (**??**), we have $C^\perp = C_\alpha^\perp \times C_\beta^\perp$. According to Lemma (**??**), we have $C_\beta^\perp$ cyclic code over R. On the other hand, we know that the dual code of evry cyclic code over $\mathbb{Z}_q$ is also cyclic. Hence the dual codes $C^\perp$ is cyclic over $\mathbb{Z}_q\Re$. □

5.4 $\mathbb{Z}_q\Re-$ Linear constacyclic codes

In this section, we study constacyclic codes over $\mathbb{Z}_q\Re$. And we show that $\mathbb{Z}_q\Re-$linear constacyclic code of length (α, β) can be identified as $\Re[x]$-submodules of $\mathbb{Z}_q[x]/\langle x^n-1\rangle \times \Re[x]/\langle x^n-\lambda\rangle$, where λ be an unit in $\Re$. Now we are ready to define the constacyclic codes over $\mathbb{Z}_q^\alpha\Re^\beta$. We start by the following Definition.

Definition 5.5. *A linear code C over $\mathbb{Z}_q^{\alpha}R^{\beta}$ is called constacyclic code if C satisfies the following two conditions.*

(i) C is an $\Re-$submodule of $\mathbb{Z}_q^{\alpha}\Re^{\beta}$,

(ii)

$$(e_{\alpha-1}, e_0, \ldots, e_{\alpha-2}, \lambda r_{\beta-1}, r_0, \ldots, r_{\beta-2}) \in C$$

whenever

$$(e_0, e_1, \ldots, e_{\alpha-1}, r_0, r_1, \ldots, r_{\beta-1}) \in C$$

In polynomial representation, each codeword $c = (e_0, e_1, \ldots, e_{\alpha-1}, r_0, r_1, \ldots, r_{\beta-1})$ of a constacyclic code can be represented by a pair of polynomials

$$\begin{aligned} c(x) &= \left(e_0 + e_1x + \cdots + e_{\alpha-1}x^{\alpha-1}, r_0 + r_1x + \cdots + r_{\beta-1}x^{\beta-1} \right) \\ &= (e(x), r(x)) \in \mathbb{Z}_q[x]/\langle x^{\alpha} - 1\rangle \times R[x]/\langle x^{\beta} - \lambda\rangle. \end{aligned}$$

Let $h(x) = h_0 + h_1x + \cdots + h_tx^t \in R\,[x]$ and let $(f(x), g(x)) \in \mathbb{Z}_q[x]/\langle x^{\alpha} - 1\rangle \times \Re[x]/\langle x^{\beta} - \lambda\rangle$. The multiplication is defined by the basic rule

$$h(x)(f(x), g(x)) = (\eta(h(x))f(x), h(x)g(x)),$$

where $\eta(h(x)) = \eta(h_0) + \eta(h_1)x + \cdots + \eta(h_t)x^t$.

Theorem 5.2. *Let C be a linear code over $\mathbb{Z}_q\Re$ of length (α, β), and let $C = C_{\alpha} \times C_{\beta}$, where C_{α} is linear code over $\mathbb{Z}_q$ of length α and C_{β} is linear code over $\Re$ of length β. Then C is a $\lambda-$ constcyclic code if and only if C_{α} is a cyclic code over $\mathbb{Z}_q$ and C_{β} is a $\lambda-$constcyclic code over $\Re$.*

Proof. Let $(e_0, e_1, \ldots, e_{\alpha-1}) \in C_{\alpha}$ and let $(r_0, r_1, \ldots, r_{\beta-1}) \in C_{\beta}$. If $C = C_{\alpha} \times C_{\beta}$ is a $\lambda-$ constcyclic code, then

$$(e_{\alpha-1}, e_0, \ldots, e_{\alpha-1}, \lambda r_{\beta-1}, r_0, \ldots, r_{\beta-1}) \in C,$$

then

$$(e_{\alpha-1}, e_0, \ldots, e_{\alpha-1}) \in C_\alpha$$

and

$$(\lambda r_{\beta-1}, r_0, \ldots, r_{\beta-1}) \in C_\beta.$$

Hence, C_α is a cyclic code over $\mathbb{Z}_q$ and C_β is a $\lambda-$constcyclic code over $\Re$.

On the other hand, suppose that C_α is a cyclic code over $\mathbb{Z}_q$ and C_β is a $\lambda-$ constcyclic code over $\Re$. Note that

$$(e_{\alpha-1}, e_0, \ldots, e_{\alpha-1}) \in C_\alpha$$

and

$$(\lambda r_{\beta-1}, r_0, \ldots, r_{\beta-1}) \in C_\beta.$$

Since $C = C_\alpha \times C_\beta$, then

$$(e_{\alpha-1}, e_0, \ldots, e_{\alpha-1}, \lambda r_{\beta-1}, r_0, \ldots, r_{\beta-1}) \in C,$$

so C is a $\lambda-$constcyclic code over $\mathbb{Z}_q\Re$. □

Corollary 5.2. *Let $C = C_\alpha \times C_\beta$ be a $\lambda-$constacyclic code over $\mathbb{Z}_q\Re$. Then the dual code $C^\perp = C_\alpha^\perp \times C_\beta^\perp$ of C is a λ^{-1}-constacyclic code over $\mathbb{Z}_q\Re$.*

Proof. From Equation (**??**), we have $C^\perp = C_\alpha^\perp \times C_\beta^\perp$. Clearly, if C_α is a constacyclic code over $\mathbb{Z}_q$ then $C_\alpha^\perp$ is also a constacyclic code over $\mathbb{Z}_q$. Moreover, from Lemma(**??**), we have $C_\beta^\perp$ is a $\lambda-$constacyclic code over R. Hence the dual code $C^\perp$ is $\lambda^{-1}-$constacyclic over $\mathbb{Z}_q\Re$. □

Conclusion and perspectives

In this thesis we were able solve certain problems in the theory of correcting codes, especially the construction of certain type of codes over some finite rings.

In the first part of this thesis we present several kinds of construction of formally self-dual codes over $A_k = \mathbb{F}_2 [v_1, \ldots, v_k] / \langle v_i^2 = v_i, v_i v_j = v_j v_i \rangle$.

In the second part, LCD codes and formally self-dual codes were considered over the ring $R = \mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$, where $v^3 = v$, for q odd. Conditions were given on the existence of LCD codes and constructions presented for LCD and formally self-dual codes over R. Some of the results presented can easily be generalized to codes over some Frobenius rings such as those in [**?**]. As an extension of the results in [**?**], we gave bounds on LCD codes over $\mathbb{F}_q$, and these used to obtain bound on LCD codes over R. Thus lower bounds on LCD codes over $\mathbb{F}_q$ are also lower bounds on LCD codes over R. LCD codes were presented which were constructed from weighing matrices. It will be interesting to construct LCD codes from other combinatorial objects. Further, it should be possible to obtain a linear programming bound for codes over R.

In the third part, skew constacyclic codes are considered over the ring $\mathbb{Z}_q R$, where $R = \mathbb{Z}_q + u\mathbb{Z}_q$, q is a prime power and $u^2 = 0$ and their algebraic and structural properties are studied. Considering their Gray images, we obtained some new linear codes over $\mathbb{Z}_4$ from skew cyclic codes over $\mathbb{Z}_q R$. Moreover, we generalized these codes to double skew constacyclic codes.

In the fourth part, cyclic and constacyclic codes are considered over the ring $\mathbb{Z}_q(\mathbb{Z}_q + u\mathbb{Z}_q + \ldots + u^{m-1}\mathbb{Z}_q)$, where q is a prime power and $u^m = 0$ and their algebraic and structural properties are studied.

Further research objective will include:

▷ Finding other applications of codes over rings such as code for DNA computing with good combinatorial and thermodynamical properties.

▷ Exploring other kind of Frobenuis ring to construct optimal codes.

▷ Another approach is to use codes over rings for secret sharing or cryptographical purpose. For example new kind of secret sharing different from the one given in [**?**].

Appendix A

Appendix

A.1 Coding theory

A.1.1 Linear codes over finite fields

Let $\mathbb{F}_q$ be the finite field of q elements. A linear codes C over $\mathbb{F}_q$, is defined as a $k-$dimensional vector subspace of $\mathbb{F}_q^n$, and C called an $[n, k]$ linear code over $\mathbb{F}_q$, with length n and dimension k. An element of C is called a word of C. Any matrix whose rows form a basis for C is called a generator matrix for C. Since C is of dimension k and length n, then a generator matrix is of type $k \times n$, and then $|C| = q^k$.

We can define over $\mathbb{F}_q^n$ a metric $d(.,.)$ called Hamming distance, defined by

$$d(x, y) = |\{i \ x_i \neq y_i\}|,$$

where $x = (x_0, x_1, \ldots, x_{n-1})$ and $y = (y_0, y_1, \ldots, y_{n-1})$ are vectors of $\mathbb{F}_q^n$. The Hamming weight $w(x)$ of a codeword x is the number of nonzero coordinates x

$$w(x) = d(x, 0).$$

The minimum distance of a $C \subset \mathbb{F}_q^n$ code is given by

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

The minimum weight of a C code is

$$w(C) = min\{w(x) \mid x \in C, x \neq 0\}.$$

A $[n, k]$ linear code C of minimal distance d is called a $[n, k, d]-$code.

Remark A.1. *In a linear code the minimum distance is equal to then minimal weight.*

A.1.2 The duality of linear codes

We will use the following definition of the inner product in $\mathbb{F}_q^n \times \mathbb{F}_q^n$.

Definition A.1. *Let C be a $[n, k]$ linear code in $\mathbb{F}_q^n$. The dual code of C is the orthogonal of the usual e inner product defined over $\mathbb{F}_q^n \times \mathbb{F}_q^n$ by*

$$\langle x, y\rangle = x_0y_0 + x_1y_1 + \ldots + x_{n-1}y_{n-1},$$

where $x = (x_0, x_1, \ldots, x_{n-1})$ and $y = (y_0, y_1, \ldots, y_{n-1})$ in $\mathbb{F}_q^n$. This code is noted $C^\perp$ and is defined by

$$C^\perp = \{x \in \mathbb{F}_q^n;\ \langle x, y\rangle = 0 \text{ for all } y \in C\}.$$

Example A.1. *On $\mathbb{F}_2$ if $C = \{000, 111\}$, then $C^\perp = \{000, 011, 110, 101\}$.*

If C is an $[n, k]$ code in $\mathbb{F}_q^n$, then the dual code $C^\perp$ of C is a linear $[n, n-k]$ code.

A.1.3 Self-dual codes

If $C \subseteq C^\perp$ then C is called self-orthogonal and if $C = C^\perp$, then C is called self-dual code. In this case must be a $[n, n/2]$ code with n even; it is reach for a linear code C we have

$$\dim C + \dim C^\perp = n.$$

Then a $[n, k]$ linear code is self-dual if and only if it is self-orthogonal with $k = n/2$.

A.2 Cyclic codes over finite fields

Cyclic codes play a very important role in the coding theory. We give in this section some useful results on cyclic codes over finite field.

Definition A.2. *A linear code C of length n over $\mathbb{F}_q$ is cyclic code if C satisfies the property that:*

$$(c_0, c_1, \ldots, c_{n-1}) \in C \Rightarrow (c_{n-1}, c_0, \ldots, c_{n-2}) \in C.$$

It is well known that cyclic codes of length n over $\mathbb{F}_q$ can be considered ideals in the quotient ring $R_n = \frac{\mathbb{F}_q[x]}{\langle x^n-1\rangle}$ via the following $\mathbb{F}_q$-module isomorphism

$$\begin{array}{ccc} \mathbb{F}_q^n & \rightarrow & \mathbb{F}_q[x]/\langle x^n-1\rangle \\ (c_0, c_1, \ldots, c_{n-1}) & \mapsto & c_0 + c_1 x + \ldots + c_{n-1}x^{n-1} \end{array}$$

The shift to the right is nothing more than the multiplication by x and then a cyclic code C is an ideal of R_n. Since R_n is a principal ideal ring and then is an ideal of R_n generated by a polynomial $g(x)$. We summarize the properties of cyclic codes in the following lemma

Lemma A.1. *For a cyclic linear code C over the finite field $\mathbb{F}_q$ there exists a unique monic polynomial g of minimal degree such that the following hold:*

1. *C is generated by g in $\mathbb{F}_q[x]/\langle x^n-1\rangle$*
2. *g is a divisor of x^n-1 in $\mathbb{F}_q[x]$.*
3. *If the dimension of the code C is K, the generator polynomial has degree $n-k$.*

Using the coefficients of the generator polynomial, the generator matrix can given by

$$G = \begin{bmatrix} g \\ xg \\ \vdots \\ x^k g \end{bmatrix} = \begin{bmatrix} g_0 & g_1 & \ldots & g_{n-1} & 0 & \ldots & 0 \\ 0 & g_0 & \ldots & g_{n-k-1} & g_{n-k} & 0 & \ldots \\ \vdots & \ddots & & \vdots & & \ddots & \vdots \\ 0 & \ldots & 0 & g_0 & g_1 & \ldots & g_{n-k} \end{bmatrix}, \tag{A.1}$$

Let C be an $[n,k]$ cyclic code with a generator $g(x) = \sum_{i=0}^{n-k} g_i x^i$. Since $g(x)$ is a divisor of $x^n - 1$. Hence

$$x^n - 1 = g(x)h(x)$$

for some h(x) of degree k. Where h(x) is called the check polynomial of C.

Proposition A.1. *[?, Proposition 3] Let $h(x)$, $g(x)$ be, respectively, the parity-check and the generator polynomial of the cyclic code C. The dual code $C^\perp$ is cyclic with generator polynomial*

$$g^\perp = x^{\deg(h)} h(x^{-1}).$$

A.3 Skew cyclic codes over finite fields

In this section we want to generalize the notion of cyclic codes over $\mathbb{F}_q$ to the notion of $\theta-$cyclic codes. The following results are analogous to the ones obtained in [?].

Definition A.3. *Let $\mathbb{F}_q$ be a finite field and θ an automorphism of $\mathbb{F}_q$. A skew cyclic code is a linear code satisfies the property that*

$$c = (c_0, c_1, \ldots, c_{n-1}) \in C \Rightarrow \sigma(c) = (\theta(c_{n-1}), \theta(c_0), \ldots, \theta(c_{n-2})) \in C,$$

Where $\sigma(c)$ is the skew cyclic shift of C.

Let θ an automorphism of $\mathbb{F}_q$ and let m be its order. Define the skew polynomial ring $\mathbb{F}_q[x;\theta]$ on the set

$$\mathbb{F}_q[x;\theta] = \{c_{n-1}x^{n-1} + \ldots + c_1 x + c_0; c_i \in \mathbb{F}_q\}.$$

The skew polynomial ring $\mathbb{F}_q[x,\theta]$ is defined as the usual addition of polynomials and the multiplication is defined by the rule

$$xa = \theta(a)x.$$

The multiplication is extended to all elements in $\mathbb{F}_q[x,\theta]$ by associativity and distributivity. Further, an element $g(x) \in \mathbb{F}_q[x,\theta]$ is said to be a right divisor (resp. left divisor) of $f(x)$ if there exists $q(x) \in \mathbb{F}_q[x,\theta]$ such that

$$f(x) = q(x)g(x) \quad (\text{ resp. } f(x) = g(x)q(x)).$$

In this case, $f(x)$ is called a left multiple (resp. right multiple) of $g(x)$.

A.4 Constacyclic codes over finite fields

The class of constacyclic codes plays a significant role in the theory of error correcting codes. These include cyclic and negacyclic codes, which have been well studied since 1950's [?]. Throughout this section $\mathbb{F}_q$ denotes a finite field with q elements. The following results are analogous to the ones obtained in [?] and [?].

Definition A.4. *Let λ be a unit in $\mathbb{F}_q$, a linear code C is called $\lambda-$constacyclic if*

$$(c_0, c_1, \ldots, c_{n-1}) \in C \Rightarrow (\lambda c_{n-1}, c_0, \ldots, c_{n-2}).$$

code of length n over $\mathbb{F}_q$ can be identified as an ideal in the quotient ring $\mathbb{F}_q[x]/\langle x^n - \lambda\rangle$ via the following $\mathbb{F}_q$-module isomorphism

$$\begin{array}{ccc} \mathbb{F}_q^n & \to & \mathbb{F}_q\left[x\right]/\langle x^n - \lambda\rangle \\ (c_0, c_1, \ldots, c_{n-1}) & \mapsto & c_0 + c_1 x + \ldots + c_{n-1}x^{n-1} \end{array}$$

If $\lambda = 1$, $\lambda-$constacyclic codes are just cyclic codes.
Define the Euclidean inner product of $u, v \in \mathbb{F}_q^n$ in the usual way: if $u = (u_1, u_2, \ldots, u_n)$ and $v = (v_1, v_2, \ldots, v_n)$. We say u and v are orthogonal if

$$\langle u, v\rangle = 0.$$

The dual of a linear code C in $\mathbb{F}_q^n$ is

$$C^{\perp} = \{u \in \mathbb{F}_q^n;\, \langle u, v\rangle = 0 \text{ for all } y \in C\}.$$

Theorem A.2. *[?, Theorem 1] If C is a $\lambda-$constcyclic code over $\mathbb{F}_q$, then $C^{\perp}$ is a $\lambda^{-1}-$constacyclic code over $\mathbb{F}_q$.*

Corollary A.1. *[?, Corollary 2] The only self-dual constacyclic codes over finite fields are cyclic or negacyclic codes.*

A.5 Skew constacyclic codes over finite fields

Given an automorphism θ of $\mathbb{F}_q$ and a unit λ in $\mathbb{F}_q$, a linear code C of length n over $\mathbb{F}_q$ is said to be skew $\lambda-$constacyclic code if C is invariant under the skew $\lambda-$constacyclic

$$(c_0, c_1, \ldots, c_{n-1}) \in C \Rightarrow (\lambda\theta(c_{n-1}), \theta(c_0), \ldots, \theta(c_{n-2})) \in C,$$

code of length n over $\mathbb{F}_q$ can be identified as an ideal in the quotient ring $\mathbb{F}_q[x;\theta]/\langle x^n - \lambda\rangle$ via the following $\mathbb{F}_q$-module isomorphism

$$\begin{array}{ccc} \mathbb{F}_q^n & \to & \mathbb{F}_q[x;\theta]/\langle x^n - \lambda\rangle \\ (c_0, c_1, \ldots, c_{n-1}) & \mapsto & c_0 + c_1 x + \ldots + c_{n-1}x^{n-1} \end{array}$$

In particular, such codes are called skew cyclic when $\lambda = 1$. When θ is the identity automorphism, they become classical constacyclic.

Theorem A.3. *[?, Lemma 2] A code C in $\mathbb{F}_q[x;\theta]/\langle x^n - \lambda\rangle$ is a skew $\lambda-$ constacyclic code if and only if C is a left $\mathbb{F}_q[x;\theta]-$ submodule of $\mathbb{F}_q[x;\theta]/\langle x^n - \lambda\rangle$.*

Lemma A.2. *[?, Lemma 3] Let C be a lef $\mathbb{F}_q[x;\theta]-$ submodule of $\mathbb{F}_q[x;\theta]/\langle x^n - \lambda\rangle$. Then C is a skew $\lambda-$constacyclic code generated by a monic polynomial with minimal degree in C.*

Bibliography

[1] T. Abualrub, I. Siap, *Cyclic codes over the rings* $\mathbb{Z}_2 + u\mathbb{Z}_2$ *and* $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2$, Designs Codes and Cryptography, 42 (3), pp. 273–287, 2007.

[2] T. Abualrub, I. Siap and I. Aydogdu, $\mathbb{Z}_2(\mathbb{Z}_2 + u\mathbb{Z}_2)$-*Linear cyclic codes*, Proceedings of the IMECS 2014, 2, Hong Kong, 2014.

[3] T. Abualrub, I. Siap, and N. Aydin, $\mathbb{Z}_2\mathbb{Z}_4-$*additive cyclic codes*, IEEE. Trans. Inf. Theory, vol. 60, no. 3, pp. 1508–514, 2014.

[4] R. Ackerman, N. Aydin, New quinary linear codes from quasi-twisted codes and their duals, Appl. Math. Lett., 24(4), pp. 512–515, 2011.

[5] A.A. de Andrade, R. Palazzo Jr. *Linear codes over finite rings*, TEMA Tend. Mat. Apl. Comput., 6(2), pp. 207–217, 2005.

[6] K. T. Arasu, T. A. Gulliver, Self-dual codes over $\mathbb{F}_p$ and weighing matrices, IEEE Trans. Inform. Theory, 47(5), pp. 2051–2056, 2001.

[7] D. Augot, E. Betti and E. Orsini, *An Introduction to Linear and Cyclic Codes* , Springer-Verlag Berlin Heidelberg, pp. 47-68 , 2009.

[8] J. B. Ayats, C. F. Córdoba and R. T. Valls, $\mathbb{Z}_2\mathbb{Z}_4$-*additive cyclic codes, generator polynomials and dual codes*, IEEE Transactions on Information Theory, 62, pp. 6348–6354, 2016.

[9] N. Aydin, T. Asamov, *A Database of* $\mathbb{Z}_4$ *Codes*, Journal of Combinatorics, Information & System Sciences, 34 (1-4), pp. 1–12, 2009.

[10] N. Aydin, Y. Cengellenmis and A. Dertli, *On some constacyclic codes over* $\mathbb{Z}_4[u]/\langle u^2-1\rangle$, *their* $\mathbb{Z}_4$ *images, and new codes*, Designs, Codes and Cryptography, 86 (6), pp. 1249–1255, 2018.

[11] N. Aydin, N. Connolly and M. Grassl, *Some results on the structure of constacyclic codes and new linear codes over* $GF(7)$ *from quasi-twisted codes*, Adv. Math. of Commun., 11 (1), pp. 245–258, 2017.

[12] N. Aydin, N. Connolly and J. Murphree, *New binary linear codes from QC codes and an augmentation algorithm*, Appl. Algebra Eng. Commun. Comput., 28(4), pp. 339–350, 2017.

[13] N. Aydin, A. Halilović, *A Generalization of Quasi-twisted Codes: Multi-twisted codes*, Finite Fields and Their Applications, 45, pp. 96–106, 2017.

[14] N. Aydin, I. Siap, *New quasi-cyclic codes over* $\mathbb{F}_5$, Appl. Math. Lett., 15 (7), pp. 833–836, 2002.

[15] N. Aydin, I. Siap and D. Ray-Chaudhuri, *The structure of 1-generator quasi-twisted codes and new linear codes*, Designs, Codes and Cryptography, 24 (3), pp. 313–326, 2001.

[16] I. Aydogdu, T. Abualrub and I. Siap, $\mathbb{Z}_2\mathbb{Z}_2[u]-$*cyclic and constacyclic codes*, IEEE Transactions on Information Theory, 63 (8), pp. 4883–4893, 2016.

[17] G. K. Bakshi, M. Raka, *A class of constacyclic codes over a finite field*, Finite Fields and Their Applications, 18 (2), pp. 362–377, 2012.

[18] R. K. Bandi, M. Bhaintwal, *A note on cyclic codes over* $\mathbb{Z}_4+u\mathbb{Z}_4$, Discrete Mathematics, Algorithms and Applications, 8 (1), pp. 1–17, 2016.

[19] A. Batoul, K. Guenda, A. Kaya, and B. Yildiz, Cyclic isodual and formally self-dual codes over $\mathbb{F}_q+v\mathbb{F}_q$, European Journal of Pure and Applied Mathematics, 8(1), pp. 64–80, 2015.

[20] N. Bennenni, K. Guenda and S. Mesnager, *DNA cyclic codes over rings*, Adv. in Math. of Comm., 11 (1), pp. 83–98, 2017.

[21] T. Blackford, *Isodual constacyclic codes*, Finite Fields and Their Applications, 24, pp. 29–44, 2013.

[22] D. Boucher, W. Geiselmann and F. Ulmer, *Skew-cyclic codes*, Appl. Algebra Engrg. Comm. Comput., 18(4), pp. 379–389, 2007.

[23] C. Carlet, S. Guilley, Complementary dual codes for counter-measures to Side-Channel Attacks, Coding Theory and Applications CIM Series in Mathematical Sciences, 3, pp. 97-105.

[24] Y. Cengellenmis, A. Dertli and S. T. Dougherty, *Codes over an infinite family of rings with a Gray map*, Des. Codes Cryptogr, 72, pp. 559–580, 2014.

[25] 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.

[26] C. J. Colbourn, J. H. Dinitz, *The Handbook of combinatorial theory*, CRC Press, Nov. 2006.

[27] R. Daskalov, P. Hristov, *New binary one-generator quasi-cyclic codes*, IEEE Trans. Inf. Theory, 49 (11), pp 3001–3005, 2003.

[28] R. Daskalov, P. Hristov and E. Metodieva, *New minimum distance bounds for linear codes over GF(5)*, Discrete Math., 275 (1–3), pp. 97–110, 2004.

[29] Database of $\mathbb{Z}_4$ Codes. [online] Z4Codes. info (Accessed March, 2018).

[30] H. Q. Dinh, A. K. Singh, S. Pattanayak and S. Sriboonchitta, *Cyclic DNA codes over the ring* $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2 + v^2\mathbb{F}_2 + uv^2\mathbb{F}_2$, Designs, Codes and Cryptography, 86 (7), pp. 1451–1467, 2018.

[31] S. T. Dougherty, *Formally self-dual codes and Gray mapes*, Proceesings of the International Workshop on Algebraic and Combinatorial Coding Theory, pp. 136–141, Jun. 2012, Pomorie, Bulgaria.

[32] S.T. Dougherty, J.-L. Kim, B. Ozkaya, L. Sok and P. Solé, *The combinatorics of LCD codes: Linear Programming bound and orthogonal matrices*, International Journal of Information and Coding Theory, 4(2–3), pp. 116–128, 2015.

[33] M. F. Ezerman, M. Grassl and P. Solé, *The weights in MDS codes*, IEEE Trans. Inform. Theory, 57(1), pp. 392–396, 2011.

[34] M.F. Ezerman, S. Ling, P. Solé and O. Yemen, *From skew-cyclic codes to asymmetric quantum code*, Adv. in Math. of Comm., 5 (1), pp. 41–57, 2011.

[35] J. Gao, *Some results on linear codes over* $\mathbb{F}_p+u\mathbb{F}_p+u^2\mathbb{F}_p$, Journal of Applied Mathematics and Computing, 47(1), pp. 473–485, 2015.

[36] J. Gao., *Skew cyclic codes over* $\mathbb{F}_p + v\mathbb{F}_p$, J. Appl. Math. Inform., 31 (3–4), pp. 337–342, 2013.

[37] J. Gao, F. W. Fu, L. Xiao and R. K. Bandi, *Some results on cyclic codes over* $\mathbb{Z}_q + u\mathbb{Z}_q$, Discrete Mathematics, Algorithms and Applications, 7 (4), pp. 1–9, 2015.

[38] J. Gao, F. Ma and F. Fu, *Skew constacyclic codes over the ring* $\mathbb{F}_q + v\mathbb{F}_q$, Appl.Comput. Math., 6 (3), pp. 286–295, 2017.

[39] J. Gao, F. W. Fu, L. Xiao, R. K. Bandi *On cyclic codes and quasi-cyclic codes over* $\mathbb{Z}_q+v\mathbb{Z}_q$, arXiv:1501.03924v2 [cs.IT] 24 Jan 2015.

[40] J. Gao, L. Shen and F-W. Fu, *Skew generalized quasi-cyclic codes over finite fields*, 2013.

[41] K. Guenda and T.A. Gulliver, Construction of cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$, for DNA computing. Appl. Algebra Eng. Commun. Comput. 24(6), pp. 445-459, 2013.

[42] K. Guenda and T. A. Gulliver, *Self-dual respeated root cyclic and negacyclic codes over finits fields*, in Proc. IEEE Int. Symp. Inform. Theory 2904–2908, Cambridge, MA, July. 2012.

[43] K. Guenda, K. Jitman and T. A. Gulliver, *Constructions of Good Entanglement-Assisted Quantum Error Correcting Codes*, Designs, Codes and Cryptography 86 (1), 121-136

[44] F. Gursoy, I. Siap and B. Yildiz, Construction of skew cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q$, Advances in Mathematics of Communications, 8 (3), pp. 313–322, 2014.

[45] M. Grassl, *Bounds on the minimum distance of linear codes and quantum codes*. Online available at http://www.codetables.de. Accessed on 19-08-2016.

[46] G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers*, 4th Ed. Oxford Univ. Pr, London, 1965.

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

[48] K. F. Ireland and M. Rosen, *A Classical Introduction to Modern number Theory*, Springer-Verlag, New York, 1982.

[49] Y. Jia, S. Ling. and C. Xing, *On self-dual cyclic codes over finite fields*, IEEE Transactions on Information Theory, 57(4), pp. 2243–2251, 2011.

[50] M. Jia, P.Solé, and B. Wu, *Cyclic codes and the weight enumerator of linear codes over* $\mathbb{F}_2 + v\mathbb{F}_2 + v^2\mathbb{F}_2$, Applied and Computational Mathematics, 12(2), pp. 247–255, 2013.

[51] S. Jitman, S. Ling and P. Udomkavanich, *Skew constacyclic over finite chain rings*, Adv. Math.Commun., 6 (1), pp. 39–63, 2012.

[52] S. Karadeniz, S. T. Dougherty, and B. Yiliz, *Constructing formally self-dual codes over* R_k, Discrete Applied Mathematics, 167(1), pp. 188–196, 2014.

[53] A. Kaya, B, Yildiz, and I. Siap, *Quadratic residue codes over* $\mathbb{F}_p + v\mathbb{F}_p$ *and their Gray images*, Journal of Pure and Applied Algebra, 218(11), pp. 1999–2011, 2014.

[54] T. Y. Lam, *Lectures on modules and rings*, Graduate Texts in Math., 189, Springer-Verlag, 1999.

[55] P. Li, W. Dai and X. Kai, *On* $\mathbb{Z}_2\mathbb{Z}_2[u]-(1+u)$*-additive constacyclic*, arXiv:1611.03169v1 [cs.IT] 10 Nov 2016.

[56] R. Lidl, H. Niederretier, *Introduction to Finite Fields and their Applications*, Cambridge University Press, 1986.

[57] X. Liu and H. Liu, *LCD codes over finite chain rings*, Finite Fields and Their Applications, 34, pp. 1–19, 2015.

[58] Y. Liu, M. Shi, and P. Solé, *Quadratic residue codes over* $\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p$, Arithmetic of Finite Fields, WAIFI 2014, pp. 204–211, 2014.

[59] Magma computer algebra system, online, http://magma.maths.usyd.edu.au/

[60] J. L. Massey, *Linear Codes with Complementary Duals*, Discrete Mathematics, 106/107, pp. 337–342, 1992.

[61] A. Melakhessou, N. Aydin, Z. Hebbache, K. Guenda, $\mathbb{Z}_q(\mathbb{Z}_q + u\mathbb{Z}_q)-$*Linear skew constacyclic codes*, Journal oJ. Algebra Comb. Discrete Appl. 7(1), pp. 85–101, 2019.

[62] A. Melakhessou, K. Guenda, T. A. Gulliver, M. Shi, P. Solé, *On Codes over* $\mathbb{F}_q+v\mathbb{F}_q+v^2\mathbb{F}_q$, Journal of Applied Mathematics and Computing, 57(1-2), pp. 375–391, 2018.

[63] A. Melakhessou, K. Chatouh, K.Guenda, *Formally Self-dual Codes over* A_k, CMA-2014, Tlemcen.

[64] A. Melakhessou, K.Guenda, L. Noui, $\mathbb{Z}_q(\mathbb{Z}_q + v\mathbb{Z}_q + \ldots + v^{m-1}\mathbb{Z}_q)-$ *Linear Cyclic, Skew Cyclic and Constacyclic Codes*, ECMI-SciTech-2017, Constantine.

[65] A. A. Nechaev, *Finite Rings with Applications*, Handbook of Algebra, pp. 213–320, 2008.

[66] J. F. Qian, L. N. Zhang and S. X. Zhu, $(1+u)$*-Constacyclic and cyclic codes over* $\mathbb{F}_2+u\mathbb{F}_2$, Applied Mathematics Letters, 19 (8), pp. 820–823, 2006.

[67] A. Sharma and M. Bhaintwal, A class of skew-constacyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$, Int. J. Information and Coding Theory, 4 (4), pp. 289–303, 2017.

[68] I. Siap, T. Abualrub, N. Aydin and P. Seneviratne, *Skew cyclic codes of arbitrary length*, Int. J. Information and Coding Theory, 2 (1), pp. 10–20, 2011.

[69] M. Shi and P. Solé, *Skew cyclic codes over a non-chain ring*, Chinese Journal of Electronics, 26(3), 2017.

[70] M. Shi, T. Yao, A. Alahmadi, and P. Solé, *Skew cyclic codes over* $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$, IEICE Trans. Fundamentals, E98-A(8), pp. 1845–1848, 2015.

[71] J. J. Watkins, *Topics in commutative ring theory*, Princeton University press, 2007.

[72] B. Yildiz, N. Aydin, Cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$ and their $\mathbb{Z}_4$-images , Int. J. Information and coding Theory, 2 (4), pp. 226–237, 2014.

[73] S. Zhu and L. Wang, *A class of constracyclic codes over* $\mathbb{F}_p + v\mathbb{F}_p$ *and its Gray image*, Discrete Mathematics, 311(23-24), pp. 2677–2682, 2011.