LINEAR CODES OVER FINITE COMMUTATIVE RINGS

2022
MASTER THESIS
MATHEMATICS

MIDYA JASIM ISMAEL HESEEN

Thesis Advisor
Assist. Prof. Dr. TÜLAY YILDIRIM TURAN

LINEAR CODES OVER FINITE COMMUTATIVE RINGS

MIDYA JASIM ISMAEL HESEEN

T.C.
Karabük University
Institute of Graduate Programs
Department of Mathematics
Prepared as
Master Thesis

Thesis Advisor
Assist. Prof. Dr. TÜLAY YILDRIM TURAN

KARABÜK
March 2022

I certify that in my opinion the thesis submitted by Midya Jasim Ismael HESEEN titled “LINEAR CODES OVER FINITE COMMUTATIVE RINGS” is fully adequate in scope and in quality as a thesis for the degree of Master of Science.

Assist. Prof. Dr. Tülay YILDRIM TURAN ....
Thesis Advisor, Department of Mathematics

This thesis is accepted by the examining committee with a unanimous vote in the Department of Mathematics as a Master of Science thesis. March 10, 2022

Examining Committee Members (Institutions) Signature

Chairman : Assist. Prof. Dr. Eda TEKİN (KBU) ....

Member : Assist. Prof. Dr. Tülay YILDIRIM TURAN (KBU) ....

Member : Assist. Prof. Dr. Rabia Nagehan ÜREGEN (EBYU) ....

The degree of Master of Science by the thesis submitted is approved by the Administrative Board of the Institute of Graduate Programs, Karabük University.

Prof. Dr. Hasan SOLMAZ ....
Director of the Institute of Graduate Programs

“I declare that all the information within this thesis has been gathered and presented in accordance with academic regulations and ethical principles and I have according to the requirements of these regulations and principles cited all those which do not originate in this work as well.”

Midya Jasim Ismael HESEEN

ABSTRACT

M. Sc. Thesis

LINEAR CODES OVER FINITE COMMUTATIVE RINGS

Midya Jasim Ismael HESEEN

Karabük University
Institute of Graduate Programs
The Department of Mathematics

Thesis Advisor:
Assist. Prof. Dr. Tülay YILDIRIM TURAN

March 2022, 76 pages

In this thesis, we consider linear codes over finite commutative rings. In especially, we give our attention to fourth order commutative rings and their algebraic structures. The first aim of this paper is to get knowledge on linear codes and literature review in detail, then study algebraic structure of linear codes over the fourth order commutative rings. In the beginning of this thesis, theoretical background on ring and field theory are discussed and then it continues with important theories and definitions on linear codes. Furthermore, all the theories are supported with good examples.

Key Words : Linear codes, Rings of order four, Generators, Gray maps.
Science Code : 20401

ÖZET

Yüksek Lisans Tezi

SONLU DEĞİŞİMLİ HALKALAR ÜZERİNDEKİ LİNEER KODLAR

Midya Jasim Ismael HESEEN

Karabük Üniversitesi
Lisansüstü Eğitim Enstitüsü
Matematik Anabilim Dalı

Tez Danışmanı:
Dr. Öğr. Üyesi Tülay YILDIRIM TURAN

Mart 2022, 76 sayfa

Bu tezde, sonlu değişmeli halkalar üzerinde lineer kodları ele alıyoruz. Özellikle, dördüncü dereceden değişmeli halkalar ve onların cebirsel yapıları üzerine dikkatimizi veriyoruz. Bu makalenin ilk amacı, lineer kodlar hakkında bilgi sahibi olmak ve detaylı literatür taraması yapmak, ardından lineer kodların cebirsel yapısını dördüncü mertebeden değişmeli halkalar üzerinden incelemektir. Bu tezin başlangıcında, halka ve cisim teorisinin teorik arka planı tartışılmakta ve daha sonra lineer kodlar üzerine önemli teoriler ve tanımlarla devam edilmektedir. Ayrıca, tüm teoriler iyi örneklerle desteklenmektedir.

Anahtar Kelimeler : Doğrusal kodlar, Dördüncü mertebeden halkalar, Üreteçler, Gray görüntüler.

Bilim Kodu **:** 20401

ACKNOWLEDGMENT

In the Name of Allah, the most Beneficent, the most Merciful

First of all, I express my highest gratitude to Allah for the blessing and compassion through all the day that I went and to complete my Master degree in Karabük University.

Secondly, I would like to deepest gratitude for my loyalist supervisor Dr. Tülay Turan, for her valuable supervision, supporting, confidence, encourage to me and for her advice and correcting in selecting my thesis during my Master degree. It is an honor for my to study with Dr. Tülay Turan for her kindness and helping me how to develop myself and initiative in my thesis.

I would like to express my thanks for my beloved family, especially my late father, and my mother for her supporting me to motivate me to become a successful induvial.

CONTENTS

Page

SYMBOLS

SYMBOLS

$\mathbb{R}$	: Ring
$\mathbb{Z}$	: The set of all integer numbers
$\mathbb{Z}_n$	: The set of integer numbers with modulo n
I	: Ideal
M	: Maximal ideal
C	: Code
$C^{\perp}$	: Dual-code
φ	: Phi function
χ	: A generating character
α	: Alpha
β	: Beta
CRT	: Chinese Remainder Theorem
F	: Field
F_q	: Field of order q
$GF(q)$	: Galois field of the order q
$V(n,q)$	: The set of vectors
$d(x,y)$	: Distance between
$\|C\|$	: Order of code C
$\binom{n}{m}$	: Binomial coefficient
$C^{\perp}$	: Dual code of C
G	: Generator matrix
G^T	: Transpose of G
H	: Parity-check matrix
$\mathbb{R}^n$	: Submodule of R
w_H	: Hamming weight
w_E	: Euclidean weight

w_L	: Lee weight
w_B	: Bachoc weight
$\varphi_{\mathbb{Z}_4}$	: Gray map of $\mathbb{Z}_4$
φ_u	: Gray map of $F_2 + uF_2$ with $u^2 = 0$
φ	: Gray map of $F_2 + vF_2$ with $v^2 = 1$
$\|x\|$	: Norm of x
$w_c(z)$	: Weight enumerators
swe	: The symmetrized weight enumerator

PART 1

INTRODUCTION

Linear codes are an important class of codes. They have been studied over a wide variety of rings, including rings theory, fields theory [11-14]. A ring has an important part in the pure and applied algebra. Family of the rings were always chosen for a particular application, with understanding that all the finite commutative rings was being direct products of the local rings by the Chinese Remainder Theorem. Thus, we are studying codes over rings, and using the assumption that all the rings work as the alphabets to the codes in a finite Frobenius ring. On the other hands, fields are very important class for the rings, because in linear algebra we always take scalars form the field, and we have vector spaces over the finite fields**.**

In this thesis, we give our consideration to coding theory especial codes over the rings of order four. That is related to the codes over the commutative rings of order four and we will generalize these codes over finite commutative Frobenius rings and give evidence that this is the most broadly defined class of codes for which the generalization is natural. Finite Frobenius rings have arisen as a large class of rings and it is most important class of the rings that could be using as the alphabets see in [2], [7].

This thesis is organized as follows:

In part 2, we considered history of coding theory and linear codes with some way and technical of the solving problems, with using some references to be sure about the history of our subjects.

In part 3, ring theory has an importance part in the applied and pure algebra, So, we explained finite commutative rings with its important definitions, examples, and theories. One of the importance of this section is Frobenius rings because by the

Frobenius rings it was easy to study on linear codes. In the fallowing of the section, we explained the Chinese Remainder Theorem. Then we studied filed theory especially finite filed. Fields are very important class for the rings with definition of filed and properties, we also supported this section with some definitions, theorems, lemmas and examples.

In part 4, we gave some basic definitions and preliminary about linear codes and also with some examples we clarified it. In continues, one of the main Theorem 4.1.2.14 is studied and we deduced that perfect codes can be found by this theorem. In the following of the section, linear codes and one of essential Definition 4.3.3.7 is about dual code and self-dual code with examples are studied in detail. By the end of this part, generators for the linear codes, with its important definitions, examples are explained and also, we mentioned about the parity-check matrix and standard form of generator matrix.

In part 5, linear codes of order four, $\mathbb{Z}_4, F_2 + uF_2$ with $u^2 = 0,\ F_2 + vF_2$ with $v^2 = v,$ and $F_2 + wF_2$ with $w^2 = w + 1,$ are consider. The codes over rings have become an increasingly important area in coding theory. Especially, linear codes over rings have been shown to have many interesting connections to Gleason-Pierce theory, see [20]. Beginning with the realization that several important rings of order four to the linear codes are studied (see [9]). The classical Chinese Remainder Theorem is more powerful method for coding over the commutative rings. By the knowledge of the Chinese Remainder Theory into local rings, we identified Gray maps for each of the rings. Then for further develop our subjects, we considered rings with order 9 such as $F_3 + vF_3$ with $v^2 = v,\ F_3 + vF_3$ with $v^2 = 1,$ and defined their Gray maps. Many of the results of coding theory have been extended to $\mathbb{R}^n$. In the following of the chapter, we also explained the different weights over these rings namely, the Lee weight, Hamming weight, Bachoc weight and Euclidean weight. Then we consider to the inner products which are basically representing a relationship between two vectors one of the highly used inner products is the Hermitian inner product and Euclidean inner products for the ring of order four

Applying both MacWilliams theorems have been shown that for the binary linear codes and for general linear codes, that is for the larger classes of rings, afterwards both MacWilliams theorems are holding over any finite ring of $\mathbb{R}$ in [11]. The second MacWilliams Theorem generalizes that the complete weight enumerator of ring of order four, The MacWilliams identity we can use to find the weight enumerate of C and relationship with the rings of order four and its important way to using MacWilliams identity is an inefficient way of determining the weight enumerators.

In the coding theory, to find the generator matrix for code is one of the more important ways. Generally, we do not need a matrix whose rows generate code, we also need a matrix whose rows generate code with the minimum number of rows. We can easily determine a minimal generating set to codes over rings and codes over fields.

Generators for the rings are very important and widely studied in linear coding theory [7-9]. We talked about generator matrices for the codes over $\mathbb{Z}_4, F_2 + uF_2,$ with $u^2 = 0,$ $F_2 + vF_2$ with $v^2 = v,$ especially. With using residue code and the torsion in the generators.

In part 6, we are just talk about the summary in details, important references and resume with some information.

PART 2

LITERATURE REVIEW

The birth of coding theory was inspired by a classic paper of Shannon in 1948 [18]. In 1949, the American Scientist, Physicist and Mathematician Warren Weaver (1894-1978) established, “The Mathematics of Communication” appeared in the Scientific American [17]. Coding theory studies started in 1998 by the paper “A Mathematical Theory of Communication” [18].

Moreover, other roots of the later so-called “Information Theory” could be found in the Cybernetics of the Norbert Wiener (1894-1964) in [17]. In the 20th century Coding theory arose as a problem in engineering concerning the efficient transmission of information. Hence, coding theory, in this perspective, using the binary field as the alphabet was largely done. Although, the alphabets were quickly generalized to finite fields, at least for mathematicians, because a lots of the techniques and proofs were identical to the binary case seen as the field with two elements [7].

In the very beginning of it is study, coding theory was viewed by mathematicians not only as an application to electrical engineering and computer science, but also as a part of pure mathematics [7]. They were interested not only in the fundamental questions of coding theory, but also into its connections by other areas of discrete mathematics. The early results of the connected codes to lattices, combinatorics, and designs. While the alphabets were a finite field these connections were generally made by codes [7].

Some papers were written when the alphabets were a ring, such as Blake’s early papers [2] and [3]. It was not until, coding theorists in 1990s stared to study codes over finite rings in earnest [7]. This study stared by the understanding that certain non-linear binary codes, which had a few properties of linear codes, in general, the images of codes over $\mathbb{Z}_4$ under a non-linear map [9]. Families of rings presented themselves for studying and a great literature emerged studying codes over rings, for some specific application were always chosen by the families of rings [7].

The interested reader could consult Sloane's seminal text and MacWilliams "The Theory of Error-Correcting Codes", for the description of classical coding theory [24]. For more description, see Pless's and Huffman, "Fundamentals of Error Correcting Codes" [12]. For the description of the connection between codes and designs see Key's and Assmus "Designs and their Codes" [25]. Codes are generally defined over finite fields, in these all three classic texts.

A great deal of research has been devoted to finding efficient schemes by which digital information can be coded for reliable transmission through a noise channel [11]. Error-correcting codes are now widely used in applications such as returning pictures from deep space, design of registration numbers, and storage of date on magnetic tape [12]. Coding theory is also of great mathematical interest, relying on ideas from pure mathematics and, in particular, illustrating the power and the beauty of algebra [11].

The rings of order four are especial interest in terms of algebraic coding theory. Because they have natural Gray maps to the binary field which makes them of especial interest in terms of constructing interesting binary codes [7]. The four rings of order four are the finite field of order four denoted $\mathbb{Z}_4, F_2 + uF_2$ with $u^2 = 0$, $F_2 + vF_2$ with $v^2 = v$, and $F_2 + wF_2$ with $w^2 = w + 1$. Codes over $\mathbb{Z}_4$ have been widely studied, in reality it was the realization that codes over $\mathbb{Z}_4$, together with their Gray map, could be used to understand certain binary codes that began the study of codes over rings [8],[10] and [22].

PART 3

BASIC NOTIONS

3.1. RING THEORY

Starting from number theory to the modern algebraic geometry, ring has an importance part in the pure algebra and applied algebra. It is important in the number theory, cryptology, and many types of another a mathematical sections. A multiplication ring has a multiplication identity, and it is also commutative. Family of the rings were always chosen for a particular application, with understanding that all the finite commutative rings was being direct products of the local ring by Chinese Remainder Theorem. Thus, in this study we are studying codes over rings, and using the assumption that all the rings work like the alphabets to the codes in a finite Frobenius ring. There is now a rapidly expanding literature on codes over various ring families [6], [7] and [9].The binary field was largely used as the alphabet in coding theory. The alphabet, on the other hand, was applied to finite fields quickly and effectively. Rings and codes could be communicate through two an important ways. In the first way, a ring structure can have the alphabet to the any codes, including finite field. In second way, some rings could become an ideal or even a module over through the code.

3.1.1. Finite Commutative Rings

Definition 3.1.1.1. Assume $\mathbb{R}$ be a ring and a non-empty set with two binary operations, multiplication, and addition. Furthermore, $(\mathbb{R},.)$ is a semigroup and $(\mathbb{R},+)$ is an abelian group, so satisfies in the following axioms.

(i) Commutativity: $a+b=b+a$ and $a.b=b.a$ for all $a,b\ \in \mathbb{R}$;

(ii) Associativity: $(a+b)+c=a+(b+c)$; $(ab).c=a.(bc)$
for all a,b and $c\ \in \mathbb{R}$.

(iii) There is an additive identity element 0 in $\mathbb{R}$ in such a way $a+0=a$ and $a.1=a$ under multiplication for all $a \in \mathbb{R}$;

(iv) The $-a$ is an inverse additive element in $\mathbb{R}$ in such a way $a.a^{-1}=a^{-1}.a=1$ under multiplication, and $a+(-a)=(-a)+a=0$ addition for every element $a\ \in \mathbb{R}$;

(v) Distributive:$a(b+c)=ab+ac$ or $(a+b)c=ac+bc$ for all a,b and $c \in \mathbb{R}$;

Note 3.1.1.2. The first four axioms require that a ring be abelian group under addition $(\mathbb{R},+)$.

Definition 3.1.1.3. Let $(\mathbb{R},+,.)$ be a ring. Then $\mathbb{R}$ is a commutative ring if $a.b=b.a,$ for all $a,b \in R$.

Definition 3.1.1.4. If the element a in $\mathbb{R}$ has a multiplicative inverse b in $\mathbb{R}$ in such a way, $a.b=b.a=1$, then a is called unit element in $\mathbb{R}$ with identity, and it is inverse is denoted by a^{-1}. Therefore, all non-zero element of the $\mathbb{C}, \mathbb{Q}$ and $\mathbb{R}$ has always a unit but the unit in $\mathbb{Z}$ is only ∓ 1.

Definition 3.1.1.5. An element a of a ring $\mathbb{R}$ is called a right (left) zero-divisor if there exists a non-zero b in $\mathbb{R}$ such that $a.b=0$ $(b.a=0)$.

Definition 3.1.1.6. The commutative ring $\mathbb{R}$ with an identity is called integral domain, if it has no zero-divisor element.

Definition 3.1.1.7. If every non-zero elements in a ring $\mathbb{R}$ is a unit so it is called division ring. Commutative division ring is also a filed.

Example 3.1.1.8. Let $(\mathbb{R},+,.)$ be a division ring with identity, for all $a \neq 0 \in \mathbb{R}$, $\exists\ a^{-1} \in \mathbb{R}$, such that $a.a^{-1}=a^{-1}.a=1$.

Definition 3.1.1.9. Let $(\mathbb{R}, +, .)$ be a ring and I be the non-empty subset of the $\mathbb{R}$. Then $(I, +, .)$ be an ideal of $\mathbb{R}$ if and only if it is satisfying the followings:

(i) $a - b\ ,\ a + b \in I,$ for all a and $b\ in\ I.$

(ii) $r.a \in I,$for all $r \in \mathbb{R}$ and $a \in I.$

Definition 3.1.1.10. An ideal $(I, +, .)$ in the ring $(\mathbb{R}, +, .)$ is called prime ideal if $a.b \in I$ implies that either $a \in I$ or $b \in I$ for all $a, b \in \mathbb{R}$.

Example 3.1.1.11. Let $(\mathbb{Z}_6, +_6, ._6)$ be a ring and $(I = \langle\bar{2}\rangle, +_6, ._6)$ a prime ideal of $\mathbb{Z}_6$, where $I = \langle\bar{2}\rangle = \{\bar{0}, \bar{2}, \bar{4}\}$ and $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$. So we have the followings:

(i) $\bar{2}, \bar{3} \in \mathbb{Z}_6$ such that $\bar{2}.\bar{3} = \bar{0} \in I \Longrightarrow \bar{2}. \in I\ , \bar{3} \notin I$

(ii) $\bar{1}, \bar{4} \in \mathbb{Z}_6$ such that $\bar{1}.\bar{4} = \bar{4} \in I \Longrightarrow \bar{1} \notin I, \bar{4} \in I$

(iii) $\bar{1}, \bar{2} \in \mathbb{Z}_6$ such that $\bar{1}.\bar{2} = \bar{2} \in I \Longrightarrow \bar{1} \notin I\ , \bar{2} \in I$

Therefore, for all $\bar{\mathrm{a}}\ , \bar{\mathrm{b}} \in \mathbb{Z}_6$, if $\bar{\mathrm{a}}.\bar{\mathrm{b}} \in I$, then either $\bar{\mathrm{a}} \in I$ or $\bar{\mathrm{b}} \in I$.

Definition 3.1.1.12. A principal ideal of the ring $(\mathbb{R}, +, .)$ is generated by a single element $a \in \mathbb{R}$, and it is denoted by $\langle a\rangle$ such that

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

Definition 3.1.1.13. Suppose $(\mathbb{R}, +, .)$ is ring, then $\mathbb{R}$ is called principal ideal ring if and only if every ideal of $\mathbb{R}$ is a principal ideal.

Remark 3.1.1.14.

(i) The principal ideal generated by zero is a ring of zero is $(0, +)$. Since

$$I = \langle 0\rangle = \{r.0 : \forall r \in \mathbb{R}\} = 0$$

(ii) The principal ideal generated by one be a ring of $(R, +)$. Since

$$I = \langle 1\rangle = \{r.1 : \forall r \in \mathbb{R}\} = \mathbb{R}$$

Example 3.1.1.15. Find the principal ideal of the ring $(\mathbb{Z}_{18}, +_{18}, \cdot_{18})$ is:

$$I_1 = \langle\bar{1}\rangle = (\mathbb{Z}_{18}, +_{18}, \cdot_{18})$$
$$I_2 = \langle\bar{0}\rangle = (\{\bar{0}\}, +_{18}, \cdot_{18})$$
$$I_3 = \langle\bar{2}\rangle = (\{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \overline{10}, \overline{12}, \overline{14}, \overline{16}\}, +_{18}, \cdot_{18})$$
$$I_4 = \langle\bar{3}\rangle = \left(\{\bar{0}, \bar{3}, \bar{6}, \bar{9}, \overline{12}, \overline{15}\}, +_{18}, \cdot_{18}\right)$$
$$I_5 = \langle\bar{6}\rangle = (\{\bar{0}, \bar{6}, \overline{12}\}, +_{18}, \cdot_{18})$$
$$I_6 = \langle\bar{9}\rangle = (\{\bar{0}, \bar{9}\}, +_{18}, \cdot_{18})$$

Definition 3.1.1.16. Let M be an ideal of the ring $\mathbb{R}$. If $M \neq \mathbb{R}$ and there is no-proper ideal I of ring the $\mathbb{R}$ that containing M, then M is called maximal ideal of $\mathbb{R}$.

Example 3.1.1.17. Determine the ideal and maximal ideal in the ring $(\mathbb{Z}_8, +_8, \cdot_8)$. The proper ideals of the ring $(\mathbb{Z}_8, +_8, \cdot_8)$ are;

$$I_1 = \langle\bar{1}\rangle = \left(\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\}, +_8, \cdot_8\right)$$
$$I_2 = \langle\bar{2}\rangle = (\{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}, +_8, \cdot_8)$$
$$I_3 = \langle\bar{4}\rangle = (\{\bar{0}, \bar{4}\}, +_8, \cdot_8)$$

$I_2 = \langle\bar{2}\rangle$ is ta maximal ideal in $\mathbb{Z}_8$, since there is no-proper ideal of the ring $(\mathbb{Z}_8, +_8, \cdot_8)$ containing $I_2 = \langle\bar{2}\rangle$, but $I_3 = \langle\bar{4}\rangle$ is not a maximal ideal, since $\langle\bar{4}\rangle \subseteq \langle\bar{2}\rangle$.

Definition 3.1.1.18. Assume $\mathbb{R}$ be a ring if it has a unique maximal ideal M, then $\mathbb{R}$ is called local ring. In this occasion the filed $\mathbb{R}/M$ is said to be the residue field of $\mathbb{R}$.

Definition 3.1.1.19. If M is a maximal ideal of $\mathbb{R}$, then $\mathbb{R}/M$ be a field.

Definition 3.1.1.20. $\mathbb{R}$ is called semi-local ring if it has finitely many maximal ideals. Semi-local rings are commutative with unity.

Definition 3.1.1.21. If $\mathbb{R}$ is a commutative ring, then it is two ideals I_1 and I_2 are called coprime ideals if $I_1 + I_2 = \mathbb{R}$.

3.1.2. Frobenius Rings

In coding theory, finite Frobenius rings have arisen like a large class of rings that could be using as the alphabets. In algebraic coding theory, the Frobenius rings have been the most important class of the rings. Maybe it is one of the most important implications of the code C with the length n over the Frobenius ring $\mathbb{R}$, it has the $|C|.|C^{\perp}| = |\mathbb{R}_n|$ where $C^{\perp}$ is a dual of C. When the ring is not a Frobenius, this is not always fact.

Theorem 3.1.2.1. We assume that $\mathbb{R}$ be the finite commutative ring, then the following conditions are equivalent:

(i) $\mathbb{R}$ is a Frobenius ring.
(ii) $\mathbb{R}$ is an injective by $\mathbb{R}$- module.
(iii) Assuming that $\mathbb{R}$ be the finite local ring with a maximal ideal M and residue field k, then those conditions must be equal with the $dim_k Ann(M) = 1$.

Proof. See the Theorem 2.1 in [7].

Example 3.1.2.2. Let $\mathbb{R}_1 = F_2 + vF_2$ be a ring of order four where $F_2 + vF_2 = \{v, 1 + v, 0, 1\}$ with $v^2 = v$. Also, $\mathbb{R}_2 = F_2 + uF_2$ be a ring of order four where $F_2 + uF_2 = \{0,1, u, 1 + u\}$ with $u^2 = 0$.

Consider the ring $\mathbb{R} = F_2[x, y]/\langle x^2, y^2, xy\rangle = \{x, y, x + y, 1 + x, 1 + y, x + y + 1, 0, 1\}$ such that $x^2 = y^2 = xy = 0$, so we have $\mathbb{R}_1[v]/\langle v^2 = v\rangle$ and $\mathbb{R}_2[u]/\langle u^2 = 0\rangle$. The maximal ideal of the $M = \{0, x, y, x + y\}$, and its dual could be defined as $M^{\perp} = \{x \in \mathbb{R}: \langle x, y\rangle = 0 , \forall\, y \in M\} = \{x, y, x + y, 0\}$. So

$$dim_k Ann(M) = dimAnn(M^{\perp}) = 2 \text{ , i.e. } M = \langle x, y\rangle$$

By the Theorem 3.1.2.1, we can see that $dim_k Ann(M) \neq 1$ and so the ring $\mathbb{R}$ is not a Frobenius ring. So, we have $|M|.|M^{\perp}| \neq |\mathbb{R}|$.

Theorem 3.1.2.3. Let $\mathbb{R}$ be a finite rings. Then the following conditions are equivalent:

(i) $\mathbb{R}$ is a Frobenius ring.
(ii) $\widehat{\mathbb{R}} \cong \mathbb{R}^{\mathbb{R}}$ like the left module.
(iii) $\widehat{\mathbb{R}} \cong \mathbb{R}_{\mathbb{R}}$ like the right module.

It's important to mention that a few of the conclusions are more complex of the non-commutative rings while we should determine if the module is on the left or right side. We assume $\mathbb{R}$ be the Frobenius ring and module isomorphism is : $\mathbb{R} \rightarrow \widehat{\mathbb{R}}$. Then the set $\chi = \varphi(1)$, and so $\varphi(r) = \chi^{r}$for some $r \in \mathbb{R}$. Thus, we can conclude that χ is a character and generating character of $\widehat{\mathbb{R}}$. For more details, one can follow the Theorem 2.2 in [7].

3.1.3. Chinese Remainder Theorem for Ring Theory

The classical Chinese Remainder Theorem is more powerful method for coding over the commutative rings.

Definition 3.1.3.1. Let we have two ideals a, b in the ring $\mathbb{R}$ is called relatively prime (coprime), if a$+b = \mathbb{R}$.

Lemma 3.1.3.2. Since a, b be a relative prime ideal of the commutative ring $\mathbb{R}$, so $a.b = a \cap \mathrm{b}$.
Proof. We can proof that directly, let $a.b \subseteq a \cap \mathrm{b}$ and as we said in the definition above if $a + b = \mathbb{R}$, then $a \cap \mathrm{b} = (a \cap \mathrm{b})\mathbb{R} = (a \cap \mathrm{b})(a + b) \subseteq ab$. As a result, $a.b = a \cap \mathrm{b}$.

Lemma 3.1.3.3. Assume that a, b and c are ideals of a commutative ring $\mathbb{R}$, by many of pairs that seem to be relatively prime. Then a be a relatively prime for bc.

Proof. It has a $\mathbb{R} = (a + \mathrm{b}).(a + \mathrm{c}) \subseteq a + bc$. Consequently $a + bc = \mathbb{R}$ so a and bc be the relatively prime.

Lemma 3.1.3.4. Assume that $a_1, a_2, a_3, \dots, a_s$ be ideals of a commutative ring $\mathbb{R}$ in that pairs seem to be relatively prime. Then $a_1 . a_2 . a_3 \dots a_s = a_1 \cap a_2 \cap a_3 \dots \cap a_s$.

Lemma 3.1.3.5. Assume that a and b are relatively prime ideals of a commutative ring $\mathbb{R}$. Then $R/a.b \cong \mathbb{R}/a \times \mathbb{R}/b$.

Proof. Let $\psi\colon \mathbb{R} \rightarrow (\mathbb{R}/a \times \mathbb{R}/b)$ be a map and defined by $\psi(\mathrm{x}) = \big(x.(mod\ a), x.(mod\ b)\big)$. It has $\ker(\psi) = a \cap \mathrm{b} = \mathrm{a.b}$, which gives us $\mathbb{R}/a.b \cong \mathbb{R}/a \times \mathbb{R}/b$.

Lemma 3.1.3.6. Let $a_1, a_2, a_3 \dots, a_s$ be ideals of commutative ring $\mathbb{R}$ such that they are relatively prime in the pairs. Then $\mathbb{R}/a_1, a_2, a_3 \dots, a_s \cong \mathbb{R}/a_1 \times \mathbb{R}/a_2 \times \mathbb{R}/a_3 \dots \times \mathbb{R}/a_s$. Assume that $\mathbb{R}$ is a finite commutative ring, with the ideal of the $\mathbb{R}$. Assume ψ_a is a canonical homomorphism $\psi_a\colon \mathbb{R} \rightarrow \mathbb{R}/a$, giving by $\psi_a(x) = x + a$. Assume that $M_1, \dots, M_s$ are maximal ideals of a finite commutative ring $\mathbb{R}$, and assume $e_1, \dots, e_s$ are individual indices of the stability. The ideals $M_1^{e1}, \dots, M_s^{es}$ are relatively prime in pair and $\prod_{i=1}^{s} M_i^{ei} = \bigcap_{i=1}^{k} M_i^{ei} = \{0\}$.

Theorem 3.1.3.7. (Chinese Remainder Theorem) Assume that $\mathbb{R}$ is a finite commutative ring, with maximal ideals $M_1, M_2, M_3, \dots, M_s$ where the index of stability of M_i is e_i. Then the map $\psi\colon \mathbb{R} \rightarrow \prod_{i=1}^{s} \mathbb{R}/M_i^{ei}$ is defined by $\psi(\mathrm{x}) = \big(x + M_1^{e1},\ x + M_2^{e2}, \dots, x + M_k^{ek}\big)$ is a ring isomorphism.

Proof. See the Theorem 2.6 in [7].

Note 3.1.3.8. Let $\mathbb{R}_i$ denote the local ring $\mathbb{R}/M_i^{ei}$. According to the Theorem 3.1.3.7, one gets $\mathbb{R} \cong \mathbb{R}_1 \times \mathbb{R}_2 \times \mathbb{R}_3 \times \dots \times \mathbb{R}_s$. Thus, $\mathbb{R}$ is Frobenius ring if and only if each $\mathbb{R}_i$ is Frobenius. For more information one can easily see the Remark 1.3 in [7]. The inverse of the isomorphism of ψ, given by Chinese Remainder Theorem, is $\mathbb{R}_1 \times \mathbb{R}_2 \times \mathbb{R}_3 \times \dots \times \mathbb{R}_s \rightarrow \mathbb{R}$.

Example 3.1.3.9. Let $\prod_{i=1}^{s} P_i^{ei}$ be a prime factorization. By the Theorem 3.1.3.7 we get $\mathbb{Z}_n \cong \mathbb{Z}_{p1^{e1}} \times \mathbb{Z}_{p2^{e2}} \times \ldots \times \mathbb{Z}_{ps^{es}}$. This is a classical application for the Chinese Remainder Theorem. Especially, it permits to the unique solution modulo $\prod n_i$ to the system of the equations $x \equiv a_i (mod\ n_i)$ while n_i be a relatively prime in the pairs. For more details, reader can follow [7].

Corollary 3.1.3.10. Let $\mathbb{R}_i$ be the finite commutative rings, $\mathbb{R} = CRT(\mathbb{R}_1, \mathbb{R}_2, \mathbb{R}_3, \ldots, \mathbb{R}_s)$ and C_i be the codes over $\mathbb{R}_i$ with $C = CRT(C_1, C_2, C_3, \ldots, C_s)$. Then

(i) $|C| = \prod_{i=1}^{s} |C_i|$;
(ii) $rank(C) = max\{rank(C_i), i = 1, \ldots, s\}$;
(iii) C is free if and only if C_i are free to every i each the same rank

Proof. For more details see the Corollary 2.1 in [7].

Theorem 3.1.3.11. Assume $\mathbb{R} = CRT(\mathbb{R}_1, \mathbb{R}_2, \mathbb{R}_3, \ldots, \mathbb{R}_s)$ is a finite commutative rings. Let $C = CRT(C_1, C_2, C_3, \ldots, C_s)$ is a code over $\mathbb{R}$. Next

$$C^{\perp} = CRT(C_1^{\perp}, C_2^{\perp}, C_3^{\perp}, \ldots, C_s^{\perp})$$

Proof. Consider vectors $v, w \in \mathbb{R}$. Then

$$\psi_a\left(\sum v_i w_i\right) = \sum \sum \psi_a(v_i) \sum \psi_a(w_i)$$

Hence, while $[v, w] = 0$, we have that

$$\left[\sum \psi_a(v), \sum \psi_a(w)\right] = 0$$

Then the standard cardinality argument gives equivalent.

Theorem 3.1.3.12. Assume that $\mathbb{R} = CRT(\mathbb{R}_1, \mathbb{R}_2, \mathbb{R}_3, \dots, \mathbb{R}_s)$ be a finite commutative ring. Let $C = CRT(C_1, C_2, \dots, C_s))$ be a code over $\mathbb{R}$. Then $d(C) = min\{d(C_i)\}$.

Proof. Let d_1 be the minimum of $\{d(C_i)\}$. Then, there exists j with $d(C_j) = d_1$. Let v_j is a minimum weight of vectors in C_j , later $CRT(0,0, \dots ,0, v_j, 0, \dots ,0)$ has been Hamming weight d_1 whichever giving $d(C) \leq d_1$. Then we assume that v is a minimum weight of vector in C. The projection $\psi_a(v)$ the weight less than or equal to $d(C)$ that giving $d(C) \leq d_1$. Therefore, $d_1 = d(C)$ and we have the result.

Theorem 3.1.3.13. Assuming that $\mathbb{R}$ be a finite commutative ring. Then $\mathbb{R}$ is isomorphic, by the Chinese Remainder Theorem ways, to direct product of the local rings.

Proof. For more information one can see the Theorem 2.10 in [7].

Theorem 3.1.3.14. Let $\mathbb{R}$ be a finite commutative ring. $\mathbb{R}$ is a principal ideal ring if and only if $R = CRT(R_1, R_2, \dots, R_t)$ where R_i is a chain ring for $i = 1, \dots, t$.

Proof. For more information one can see the Theorem 2.11 in [7].

Note 3.1.3.15. The standard examples of the Theorem 3.1.3.14 can be the example give in the Example 3.1.3.9. Namely, $\mathbb{Z}_n \cong \mathbb{Z}_{p1^{e1}} \times \mathbb{Z}_{p2^{e2}} \times \dots \times \mathbb{Z}_{ps^{es}}$. Here, $\mathbb{Z}_n$ be a principal ideal ring also all, $\mathbb{Z}_{pi^{ei}}$ be a chains ring.

Example 3.1.3.16. For the integers $k \geq 1$, we defined the family of the rings A_k to be $A_k = F_2[v_1, v_2, \dots, v_k]/\langle v_i^2 - v_i, v_i v_j - v_j v_i \rangle$. The ideal $\langle w_1, w_2, \dots, w_k \rangle$, where $w_i \in \{v_i, 1 + v_i\}$, be a maximal ideal of cardinality $2^{2^k} - 1$ and denoted those maximal ideals by M_i. We noted in here 2^k is any ideal and $M_i^{ei} = M_i$ for every i and $e \geq 1$. It can be elementary for seen that a direct sum of each two of those ideals be A_k. After, by the Chinese Remainder Theorem, one gets that A_k is isomorphic to $F_2^{2^k}$. Such that, A_k is the principal ideal ring and which is also isomorphic to the direct product of the chain rings.

3.2. FIELD THEORY

Fields, we are realized from the linear algebra, are very important class for the rings, because in linear algebra we always take scalars form the field. Even if a ring with the any single element can be technically qualified like a field under the definition, we always try to rule it out for this case. One more way in the field is that we must have $1 \neq 0$. (When their any element $1 \neq 0$ in a ring with identity, then $1.x = x \neq 0 = 0.x$ and so $1 \neq 0$).

3.2.1. Finite Fields

Definition 3.2.1.1. A filed F be a set of elements with both operations additions and multiplications. Let F_q is a finite field of order q where q is a prime number. A non-empty set V, together with the some (vector) scalar multiplication (.) and addition $(+)$ by the elements of F_q, be a (linear space or) vector space over F_q if it satisfies all the following axioms for all a, b and $c \in F_q$;

(i) Closure: $a + b$ and $a.b$ in F_q are closed under addition and multiplication respectively;

(ii) Commutativity: $a + b = b + a$ and $a.b = b.a$;

(iii) Associativity: $(a + b) + c = a + (b + c)$; $a.(bc) = (ab).c$;

(iv) Distributive: $a.(b + c) = ab + ac$; $(a + b).c = ac + bc$;

(v) There exists an identity element 0 and 1 in F like that $a + 0 = a$ and $a.1 = a$;

(vi) $-a$ additive inverse element be exists in F_q such that $a + (-a) = 0$;

(vii) a^{-1} multiplicative inverse element be exists in F_q such that $a.a^{-1} = 1$;

Definition 3.2.1.2. The axioms of filed from (i –vii), whole the set of elements with both multiplication (.) and addition $(+)$ is called a ring.

Definition 3.2.1.3. The finite filed be a filed, if we have finite numbers of any elements, those numbers are called order of the field and denoted by q.

Lemma 3.2.1.4. For a field $F,$ we have the following axioms:

(i) $a.0 = 0$ for all a in F.

(ii) $a.b = 0 \Rightarrow a = 0$ or $b = 0$. (So the product of any two non-zero elements of the filed be also non-zero).

Proof. For more information see Lemma 3.1 in [11].

Theorem 3.2.1.5. The order of field q exists if and only if q is a prime power such that $(q = p^h$ where p is a prime number and also h is positive integer). In the addition, when q is a prime power, so there is up to the relabeling, at most one filed of that order q. A Galois field of the order q is denoted by $GF(q)$.

Proof. For more information see Theorem 3.2 in [11].

Definition 3.2.1.6. Let m be a fixed positive integer. Two integers a and b are called congruent $(modul\ m),$ if $a - b$ be a divisible by m.

$$a \equiv b(mod\ m)$$

In another words, if $a = km + b$ to some k integer, then $a \not\equiv b(mod\ m)$ where a and b are not congruent $(modul\ m)$.

Theorem 3.2.1.7. $\mathbb{Z}_m$ is a field if and only if m is a prime number.

Proof. For more information see the Theorem 3.5 in [11].

Example 3.2.1.8. Find $GF(3)$ such that $\mathbb{Z}_3 = \{0, 1, 2\}$ with tables.

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

.	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\mathbb{Z}_4$ is not a field by Theorem 3.2.1.7 (examination of the multiplication table of $\mathbb{Z}_4$ shows that 2 dose not have an inverse and so we cannot divide by 2 in $\mathbb{Z}_4$). However, while $4 = 2^2$ is not prime, it is a prime power, and so the field $GF(4)$ dose exist, by the Theorem 3.2.1.5.

3.2.2. Vector Space over the Finite Fields

It is also very useful be able to perform certain operations with a codewords themselves, in carrying out of the arithmetic operations within the alphabet of the codes. Now, we assume that q is a prime power and also, $GF(q)$ denotes the finite field with q elements. The element of $GF(q)$ is called scalars. The set $GF(q)^n$of all ordered n-tuples over $GF(q)$ is denoted that by $V(n, q)$ where n is be length and also it is element will be called vectors. We define two operations within $V(n, q)$:

(i) Addition of vectors: if $x = (x_1, x_2, \dots, x_n)$ and $y = (y_1, y_2, \dots, y_n) \in V(n, q)$, then $x + y = (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n)$.

(ii) A scalar multiplication of a vector: if $x = (x_1, x_2, \dots, x_n) \in V(n, q)$ and $a \in GF(q)$.Next $ax = (ax_1, ax_2, \dots, ax_n)$.

For all $u, v,$ and $w \in V(n, q)$ and for all a and $b \in GF(q)$, we have the following axioms:

(i) $u + v \in V(n, q)$;

(ii) $(u + v) + w = u + (v + w)$;

(iii) The all-zero vector $0 = (0,0,\dots,0) \in V(n,q)$ and satisfying $u + 0 = 0 + u = u$;

(iv) The vector of $u = \{u_1, u_2, \dots, u_r\} \in V(n,q)$, and the element of the $-u = \{-u_1, -u_2, \dots, -u_r\} \in V(n,q)$ and satisfies $u + (-u) = 0$;

(v) $u + v = v + u$ from axioms (i)-(iv) mean that $V(n,q)$ is abelian group under addition;

(vi) $a.v \in V(n,q)$ it is closure under scalar multiplication;

(vii) Distributive : $a(u + v) = au + av, (a + b)u = au + bu$;

(viii) $(ab).u = a.(bu)$;

(ix) $1.u = u$, where 1 is the multiplicative identity of $GF(q)$;

Definition 3.2.2.1. Let V a vector space is a non-empty subset of C and also its be a subspace of V, if it is a vector space by the same scalar multiplication and vector addition as V, then it is a vector space.

Theorem 3.2.2.2. A non-empty subset C of $V(n,q)$ is a subspace if and only if C is closed under scalar multiplication and addition, if and only if C satisfy the followings:

(i) If $x, y \in C,$ then $x + y \in C$;

(ii) If $a \in GF(q)$ and $x \in C,$ then $a.x \in C$;

Proof. For more information see Theorem 4.1 in [11].

Definition 3.2.2.3. Assume V be a vector space over F_q. A linear combination of r vectors $\{v_1, v_2, v_3 \dots, v_r\}$ in $V(n,q)$ is a vector of the form $a_1v_1 + a_2v_2 + a_3v_3 \dots + a_rv_r$ where a_i's are scalar numbers for $i = 1, \dots, r$.

Definition 3.2.2.4. Assume that V be a vector space over F_q**.** The set of the vectors $\{v_1, v_2, v_3 \dots, v_r\}$ is called a linearly dependent if there are scalar $a_1, a_2, a_3 \dots, a_r$ not all zero, so that $a_1v_1 + a_2v_2 + a_3v_3 \dots + a_rv_r = 0$.

A set of vectors $\{v_1, v_2, v_3 \dots, v_r\}$ is called linearly independent if it is not linearly dependent such that, if $a_1v_1 + a_2v_2 + a_3v_3 \dots + a_rv_r = 0 \Longrightarrow a_1 = a_2 = \cdots = a_r = 0$.

Definition 3.2.2.5. Let C be a subspace of $V(n, q)$, then a subset $\{v_1, v_2, v_3 \dots, v_r\}$ is a non-empty subset of C is called generating set or (spanning set) of C, providing that every single vector in C could be expressed as a linear combination of $v_1, v_2, v_3 \dots, v_r$.

Moreover, if $\{v_1, v_2, v_3 \dots, v_r\}$ is a generating set and linearly independent, so it is called basis of the C.

Theorem 3.2.2.6. Let C be a non-trivial and subspace of $V(n, q)$. Then, $\{v_1, v_2, v_3 \dots, v_r\}$ is any generating set that containing bases of C.

Proof. For more information see the Theorem 4.2 in [11].

Theorem 3.2.2.7. Suppose $\{v_1, v_2, v_3 \dots, v_r\}$ be a basis of subspace C of $V(n, q)$. Then

(i) All vector of C may be expressed uniquely like a linear combination of the basis vectors.

(ii) C exactly includes q^k vectors.

Proof. For more information see Theorem 4.3 in [11].

Note 3.2.2.8. It follows from Theorem 3.2.2.7 that any two bases of a subspace C contains the same number k of vectors, where $|C| = q^k$, and also the number of k is said to be dimension of the subspace C and it is denoted by $\dim(C)$. We have already exhibited a basis of $V(n, q)$ having n vectors and so $\dim\big(V(n, q)\big) = n$.

Definition 3.2.2.9. Let $w = \{w_1, w_2, w_3 \dots w_n\}$ and $v = \{v_1, v_2, v_3 \dots v_n\} \in \left(F_q\right)^n$.

(i) The scalar product (also known as the Euclidean inner product or dot product) of v and also w are defined as $v.w = v_1w_1 + v_2w_2 + v_3w_3 \dots + v_nw_n \in F_q$.

(ii) v and w are are called orthogonal if $v.w = 0$.

(iii) Assume S be a non-empty subset of $\left(F_q\right)^n$. The complement of orthogonal $S^\perp$ of S be a definite as $S^\perp = \left\{v \in \left(F_q\right)^n | v.s = 0\,, \forall s \in S\right\}$. If $S = \emptyset$, then we define $S^\perp = \left(F_q\right)^n$.

Definition 3.2.2.10. $F_{q^2}^n \times F_{q^2}^n \to F_{q^2}^n$ be defined as $\langle u, v\rangle_H = \sum_{i=1}^n u_i v_i$, where $u, v \in F_{q^2}^n$**.** This inner product is said to be the Hermitian inner product. To the linear code C over $F_{q^2}^n$**.** Its be a Hermitian dual be definite as $C^{\perp H} = \left\{v \in F_{q^2}^n : \langle u.c\rangle_H = 0, \forall\, c \in C\right\}$. If $C = C^{\perp H}$, after that we can say that C be a self-dual with respect for the Hermitian inner product.

PART 4

INTRODUCTION TO LINEAR CODES

4.1 LINEAR CODES

4.1.1. Introduction

In the coding theory, linear codes be an error-correcting codes in some linear combination of the codewords. We are also worried about sending a message via the channel that may be affect by the "noise." Linear code is introduced in forwards the error-correction and are apply in the ways for sending signal as a (bits). In the communications channel thus, we hope to obtain the decode and encode if occur the errors in a communication, a few errors may be detected up or corrected by the receiver a block message. That information about the manner that will be allowed to detect up, and also possible the correction, of the errors caused by the noise. This circumstance rises in several areas of the communications, consists computer communications, television, telephone and radio and also even compact disc player technologies. In coding theory, probability, polynomial rings, linear algebra and group theory over finite field every play a very valuable role. Also, in this part, let the alphabet F_q be a Galois field $GF(q)$, where q be a prime power, and regarded $\left(F_q\right)^n$even as a vector space $V(n,q)$. A vector $(x_1, x_2, \dots, x_n)$ is usually written as $x_1 x_2 \dots x_n$. For some positive integer n, a linear code over $GF(q)$ be just a subspace of $V(n,q)$.

Definition 4.1.1.1. A binary code be a linear if and only if the sum of any two codewords are a codeword. A binary code be just given a set of sequence of {0s and 1s} whichever is called codewords. If we have 2-ary code is always said binary codes, and 3-ary code sometimes refer to like the ternary codes.

Definition 4.1.1.2. The massage symbol is encoded by repeating the symbol five times, then the code called is binary repetition code of length n and also, we have binary date is $\{0,1\}$. We used binary code in the digital computers, based on a binary number system there are only 0 and 1 possible.

Example 4.1.1.3. 2-ary repetition code of length 3 and 3-ary repetition code of length 4 can be shown by followings:

(i) $(F_2)^3 = \{000, 111\}$ so $(n, q, d) = (3, 2, 3)$.
(ii) $(F_3)^4 = \{0000, 1111, 2222\}$ so $(n, q, d) = (4, 3, 4)$.

Definition 4.1.1.4. A code in any codeword be a sequence including of a fixed number n of symbol is said to be a block code with length n.

Definition 4.1.1.5. A code C with codewords M of the length n be frequently written just as an $M \times n$ array whose rows are the codewords of C. Such that, the binary repetition code of length 5 be $\{00000, 11111\}$. Let $(F_q)^n$denote $a = a_1 a_2 \dots a_n$ be a set of ordered n-tuples where any $a_i \in F_q$. The elements of $(F_q)^n$ are said to be words or vector.

Definition 4.1.1.6. The Hamming distance between two vectors x and y of distance function $(F_q)^n$is the number of places in which they differ and denote by $d(x, y)$. The Hamming distance be a legitimate distance matric or function, since it is satisfying the following axioms:

(i) $d(x, y) = 0$, if and only if $x = y$
(ii) $d(x, y) = d(y, x)$ for all $x, y \in (F_q)^n$.
(iii) $d(x, y) \leq d(x, z) + d(y, z)$ for all x, y and $z \in (F_q)^n$.

Definition 4.1.1.7. The decoded likelihood of correcting-errors provided the following assumptions are made about the channel.

(i) Any symbol transmitted has been the same probability $p < \left(\frac{1}{2}\right)$ from to being received in errors.

(ii) Supposing that each symbol being received in the error, after that any of $(q-1)$ be possible errors are the equally likely.

Definition 4.1.1.8. A minimum distance is an important parameter of a code C, giving a measure of how good it is at the error correcting, and the minimum distance denote by $d(C)$. To be smallest of the distance between codewords,

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

Example 4.1.1.9. Let $C = \{000, 001, 010, 100, 011, 101, 110, 111\}$ being a linear code, the minimum distance of C can be calculate as follows:

$d(000, 001) = 1;\ d(000, 111) = 3;\ d(110, 111) = 1;\ d(100, 111) = 2$

and if we continue with the process of finding the distance between the codewords, one can obtain that $d(C) = min\{d(x,y)|x$ and $y \in C, x \neq y\} = 1$.

Theorem 4.1.1.10.

(i) C is a code may be detect up to s errors in each codeword if $d(C) \geq s+1$.

(ii) C is a code may be correct up to t errors in each codeword if $d(C) \geq 2t+1$.

Proof. For more details see the Theorem 1.9 in [11].

Corollary 4.1.1.11. If C has a minimum distance d, then C may be used either;

(i) $d-1$ errors for detect up, or

(ii) $\left\lfloor \frac{(d-1)}{2} \right\rfloor$ errors for correct up in each codeword.

Proof.

(i) $d \geq s + 1$ if and only if $s \leq d - 1$.
(ii) $d(C) \geq 2t + 1$ if and only if $t \leq \frac{(d-1)}{2}$.

4.1.2. The Aim of the Coding Theory

Definition 4.1.2.1. An (n, M, d)-code be a code of length n. Including codewords M and d has the minimum distance.

Note 4.1.2.2. A good (n, M, d)-code have small n (for quickly transference of massages), large M (to enable transference of wide variety of the massage) and d is large (many errors be correct). This is a conflicted goals and also be frequently mentions to the coding theory main problem to find a way to optimize one of the parameters (n, M, d) to given values of the others two. The normal version of the problems is to find the hugest code of given minimum distance. We denoted by $A_q(n, d)$ the largest value of the M such that there exist a $q -$ ary (n, M, d)- code.

Theorem 4.1.2.3.

(i) $A_q(n, 1) = q^n$;
(ii) $A_q(n, n) = q$;

Proof.

(i) To the minimum distance of a code to be at least 1 we require that codewords are distinct, and the largest $q -$ ary (n, M, d)- code be the whole of $(F_q)^n$ $w$ith $M = q^n$.

(ii) Suppose C is a $q -$ ary (n, M, n)- code. Then any two distinct codewords of C are different in all n positions. Thus symbol appearing in any fixed position. e.g., The first, in the M codewords must be the distinct. Giving $M \leq q$. Thus $A_q(n, n) \leq q$. On the other side, the $q -$ ary repetition code of length n. Is an (n, q, n)- code and so $A_q(n, n) = q$.

Definition 4.1.2.4. A permutation of a set $S = (x_1, x_2, \dots, x_n)$ is one-to-one mapping from S to itself. We denoted by a permutation f by;

$$\begin{pmatrix} x_1 & x_2 & & x_n \\ \downarrow & \downarrow & \dots & \downarrow \\ f(x_1) & f(x_2) & & f(x_n) \end{pmatrix}.$$

If one of the two q-ary codes is obtained from the other by using combination of operation of the following operations, then they are said to be equivalent.

(i) Permutation of the positions of the code.
(ii) A non-zero scalar multiplies symbols appearing at a fixed position.

Clearly the distances between any codewords are not changed by such operations and so equivalent codes have the same parameters (n, M, d) will be correct the same number of the errors.

Example 4.1.2.5. Apply the permutation to the code $C = \{00100, 00011, 11111, 11000\}$;

(i) Apply the permutation $\begin{pmatrix} 0 \to 1 \\ 1 \to 0 \end{pmatrix}$to the symbol in third position.
(ii) Interchange position two and four.
(iii) Multiply by 1 in one and five position.

We can obtain equivalent code $C = \{00000, 01101, 11011, 10110\}$.

Lemma 4.1.2.6. Each q-ary (n, M, d)-code over the alphabets $\{0, 1, \dots, q-1\}$ be equal to an (n, M, d)-code which includes all zero vectors $0 = 00 \dots 0$.

Proof. Choose any codewords $x_1 x_2 \dots x_n$ and for each $x_i \neq 0$, apply the permutation $\begin{pmatrix} 0 & x_i & & \\ \downarrow & \downarrow & \dots & for\ all\ j \neq 0, x_i \\ x_i & 0 & & \end{pmatrix}$ to the symbols in position i.

Note 4.1.2.7. We take the set $\{0,1\}$ for F_2, and define two operations in $(F_2)^n$. Assume that $x = x_1x_2 \dots x_n$ and $y = y_1y_2 \dots y_n$ are two vectors in $(F_2)^n$. Then, $x + y$ is in $(F_2)^n$ and defined by $x + y = (x_1 + y_1, x_2 + y_2\ , \dots, x_n + y_n)$, while the intersection $x \cap y$ is in $(F_2)^n$ defined by $x \cap y = (x_1y_1, x_2y_2\ , \dots, x_ny_n)$. The terms $x_i + y_i$ and x_iy_i are calculated modulo of 2 (without carrying); that are, according to multiplication and addition table

.	0	1
0	0	0
1	0	1

+	0	1
0	0	1
1	1	0

For example, $1011 + 1111 = 0100$ and $1011 \cap 1111 = 1011$. The weight of the vector $x\ in\ (F_2)^n$, denoted $w(x)$, be define to be a number of 1s appeared in x.

Lemma 4.1.2.8. If x and $y \in (F_2)^n$, then $d(x,y) = w(x) + w(y) - 2w(x \cap y)$.

Proof. $d(x,y) = w(x +\ y) =$ (number of $1s\ in\ x$) + (number of $1s\ in\ y$) $-$ 2(number of positions where both x and y have 1) $= w(x) + w(y) - 2w(x \cap y)$.

Theorem 4.1.2.9. Suppose d be odd. Next the binary (n, M, d)-code exists if and only if a binary $(n + 1, M, d + 1)$-code exist.

Proof. For more information see the Theorem 2.7 in [11].

Corollary 4.1.2.10. If d is odd, then $A_2\ (n + 1, d + 1) = A_2\ \ (n, d)$, equivalently, if d is even, then $A_2\ \ (n, d) = A_2\ (n - 1, d - 1)$.

Example 4.1.2.11. We will determine the value $A_2\ (5,3)$. The code C is a binary $(5,4,3)$-code and so $A_2\ (5,3) \geq 4$. By the Corollary 4.1.2.10**,** $A_2\ (6,4) = 4$. To illustrate the 'only if' part of Theorem 4.1.2.9 we construct below a $(6,4,4)$-code from the $(5,4,3)$-code of C. $(5,4,3)$-code adds overall parity-check $(6,4,4)$-code are;

$$00000 \rightarrow 000000$$

$$01101 \rightarrow 011011$$

$$10110 \to 101101$$
$$11011 \to 110110$$

The trial-and error method of C, which proved that a binary $(5,4,3)$-code must have $M \leq 4$, would not be practical for sets of larger parameters.

Definitions 4.1.2.12. If n and m are integers with $0 \leq m \leq n$. Then the binomial coefficient $\binom{n}{m}$. Pronounced 'n choose m', is defined by

$$\binom{n}{m} = \frac{n!}{m!\,(n-m)!}$$

Where $m! = m(m-1)\dots 3.2.1$ for $m > 0$.

Lemma 4.1.2.13. The number of unordered selections of m distinct objects from the set of n distinct objects be $\binom{n}{m}$.

Proof. An ordered selection of m distinct objects from the set of n distinct objects may be made in $n(n-1)\dots(n-m+1) = \frac{n!}{(n-m)!}$. Ways, for the first object can be chosen in any of n ways, then the second in any of $n-1$ ways, and so on. Since there are $m(m-1)\dots 3.2.1 = m!$ Ways of ordering the m objects chosen, the number of unordered selections is

$$\frac{n!}{m!\,(n-m)!}$$

Definition 4.1.2.14. For any vector v in $\left(F_q\right)^n$and each integer $r \geq 0$, the sphere of radius r and center u denoted by $S(u,r)$ is the set $\left\{v \in \left(F_q\right)^n \mid d(u,v) \leq r\right\}$.

Lemma 4.1.2.15. A sphere of radius r in $\left(F_q\right)^n$ $(0 \leq r \leq n)$ includes exactly $\binom{n}{0} + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \cdots + \binom{n}{r}(q-1)^r$ vectors.

Proof. For more information look at Lemma 2.15 in [11].

Theorem 4.1.2.16. (Hamming bound or the sphere-packing) A q-ary $(n, M, 2t + 1)$-code satisfying

$$M\left\{\binom{n}{0} + \binom{n}{1}(q-1) + \cdots + \binom{n}{t}(q-1)^t\right\} \leq q^n.$$

Proof. For more information look at the Theorem 2.16 in [11].

Definitions 4.1.2.17. A code which achieves the sphere-packing bound, such that equality occurs in Theorem 4.1.2.16, is called a perfect code. As a result, the M spheres of t radius centered on the codewords 'fill' the all of space $\left(F_q\right)^n$without overlapping for perfect t-error-correcting codes. In other words, every vector in $\left(F_q\right)^n$ be at distance $\leq t$ from exactly one codeword. The binary repetition code

$$\begin{cases} 0\ 0 \ldots 0 \\ 1\ 1 \ldots 1 \end{cases}$$

of length n, where n is odd, is a perfect code $(n, 2, n)$-code. As a result, codes contain only one codeword or are the whole of $\left(F_q\right)^n$are referred to as trivial perfect codes. The problem of finding all perfect codes, has provide mathematicians with one of the greatest challenges in coding theory.

4.1.3. Introduction to the Linear Codes

Definitions 4.1.3.1. A code is called a linear code or a group code. For some positive integer, a linear code over $GF(q)$ is just a subspace of $V(n, q)$. A ternary code or binary code is used to explain the code, especially. The vectors in C are said to be codewords. So a subset C of $V(n, q)$ be a linear code if and only if,

(i) $u + v \in C,$ for all u and $v\ in\ C$.
(ii) $a.u \in C,$ for all $u \in C, a \in GF(q)$.

A binary code is said to be linear if and only if the sum of any two codewords are also a codeword. For example, the binary repetition of code C of length 3. We assume that n is length = 3, q is distinct elements or [number of digit] = 2 and M is the elements of C [number of codewords] = 4.

$$(n, M, d) - \text{code} = (3, 4, 1)$$

In normal case, we have $\left(F_q\right)^n = (F_2)^3, i.e\ \ q^n = 2^3 = 8$ codewords, and we have

$$C = \{000, 001, 010, 100, 011, 101, 110, 111\}.$$

If linear subspace C is a K-dimensional subspace of (n, q) where be the finite field with the q elements as a code be called a q-ary code, then the linear code C is called $[n, k]$-code and also the minimum distance d of C is an $[n, k, d]$-code.

Note 4.1.3.2.

(i) A q-ary $[n, k, d]$-code is also a q-ary (n, q^k, d)-code by (Theorem 4.3 in [11]). However, not every (n, q^k, d)-code is an $[n, k, d]$-code.

(ii) The all-zero vector 0 automatically belong to a linear code.

Definition 4.1.3.3. The weight of a vector x in $\left(F_q\right)^n$denoted $w(x)$ be defined as the number of 1s appeared in x, $w_t H(x) = \{x_i \neq 0\}$. The minimum Hamming weight of a code C be $min\{w_t H(x) |\ x \in C, x \neq 0\}$.

Example 4.1.3.4. Let $C = \{000, 100, 011, 101\}$ be a code and its weights of codewords are calculated as follows:

$$w(000) = 0;\ w(100) = 1;\ w(011) = 2;\ w(101) = 2$$

Lemma 4.1.3.5. Even if x and $y \in V(n,q)$. Then $d(x,y) = w(x-y)$.

Proof. The vector $x-y$ have a non-zero entries in precisely those places where x and y different.

Theorem 4.1.3.6. Suppose C is a linear code and $w(C)$ is a smallest of the weights of a non-zero codewords of C.Then, $d(C) = w(C)$.

Proof. For more details see the Theorem 5.2 in [11].

Definition 4.1.3.7. A linear $[n,k]$-code C, and C be dual code, denote by $C^{\perp}$, is defined to be the set of these vectors of $V(n,q)$, which is orthogonal for all codeword of C. i.e

$$C^{\perp} = \{v \in V(n,q) |\, v.u = 0, \text{for all } u \in C\}$$

$C^{\perp}$ is a linear code of dimension $n-k$, so $|C^{\perp}| = |n-k|$. C is self-orthogonal if $C \subseteq C^{\perp}$, self-dual if $C = C^{\perp}$. Self-dual codes exist whenever the length n is even.

Definition 4.1.3.8. Let C be a linear code, then C is said to be self-dual if $C = C^{\perp}$.

Note 4.1.3.9. Self-dual is self-orthogonal code, but self-orthogonal is not self-dual code.

Lemma 4.1.3.10. Suppose C is an $[n,k]$-code have G is a generator matrix. Then v is a vector of $V(n,q)$ belongs to $C^{\perp}$ if and only if v is orthogonal to every rows of G; i.e.

$$v \in C^{\perp} \Leftrightarrow vG^{T} = 0,$$

where G^{T} denoted the transpose of G.

Proof. For more details see the Lemma 7.2 in [11].

Theorem 4.1.3.11. Suppose C is an $[n,k]$-code over $GF(q)$. Then $C^{\perp}$dual code of C be a linear $[n,n-k]$-code.

Proof. Firstly we want to show that $C^{\perp}$ be a linear code. Let $v_1, v_2 \in C^{\perp}$ and $\lambda, \mu \in GF(q)$. Then, for all $u \in C$. For more information can one see the Theorem 7.3 in [11].

Example 4.1.3.12. Let C be a linear binary code, if $C = \{000, 110, 011, 101\}$, then the dual of C be, $C^{\perp} = \{v \in V(n,q) | \ v.u = 0, \forall u \in C\}$. Let $v = a_1a_2a_3$, then

(i) $(a_1a_2a_3).(000) = (000)$ so $a_1 = a_2 = a_3 = 0$;
(ii) $(a_1a_2a_3).(110) = (000$ or $110)$ so $a_1 + a_2 = 0$ and $a_3 = 0$ or $a_3 = 1$;
(iii) $(a_1a_2a_3).(011) = (000$ or $011)$ so $a_3 + a_2 = 0$ and $a_1 = 0$ or $a_1 = 1$;
(iv) $(a_1a_2a_3).(101) = (000$ or $111)$ so $a_1 + a_3 = 0$ and $a_2 = 0$ or $a_2 = 1$;

So dual code of C is $C^{\perp} = \{000, 111\}$.

(2) If $C = \{0000, 1100, 0011, 1111\}$, let $v = a_1a_2a_3a_4$

(i) $(a_1a_2a_3a_4).(0000) = (0000)$ so $a_1 = a_2 = a_3 = a_4 = 0$;
(ii) $(a_1a_2a_3a_4).(1100) = (0000\ )$ so $a_1 + a_2 = 0$ and $a_3 = a_4 = 0$;
(iii) $(a_1a_2a_3a_4).(0011) = (0000)$ so $a_1 = a_2 = 0$ and $a_3 + a_4 = 0$;
(iv) $(a_1a_2a_3a_4).(1111) = (0000)$ so $a_1 + a_2 + \ a_3 + a_4 = 0$;

So dual code of C are equal to self-dual code, such that $C = C^{\perp}$.

4.2. GENERATORS

4.2.1. Introduction

In the coding theory, to find the generator matrix for code is one of the more important methods. In general, we don't need a matrix whose rows generate code, we also need a matrix whose rows generate code with the minimum number of rows. We can easily determine a minimal generating set to codes over fields and codes over rings.

Definition 4.2.1.1. A matrix $k \times n$ whose rows from a basis of a linear $[n, k]$-code is said to be a generator matrix of the code.

Note 4.2.1.2. The q-ary repetition code with length n over $GF(q)$ be an $[n, 1, n]$-code with generator matrix of $[11 \dots 1]$.

Theorem 4.2.1.3. Let $k \times n$ two matrices which generate equivalent linear $[n, k]$-code over $GF(q)$ if one of the matrix can be obtain by other matrix by a sequence of following operations:

(R1) Permutation of rows;
(R2) Multiplying of any row by a non-zero scalar number;
(R3) Additive of a scalar multiple of one row to another;
(C1) Permutation of columns;
(C2) Multiplying of any column by a non-zero scalar number;

Proof. For more details see the Theorem 5.4 in [11].

Theorem 4.2.1.4. Suppose G is a generator matrix of an $[n, k]$-code. Then by performing operations of type (R1 to C2), G can be transformed for the standard form $[I_k|A]$, where I_k be $k \times k$ identity matrix, and A be a $k \times (n-k)$ matrix.

Proof. For more details see the Theorem 5.5 in [11].

Example 4.2.1.5. Let C be linear code is a $[7,4,3]$-code, then by the Theorem 4.2.1.3 to transform the generator matrix to the standard form.

$$(1) \qquad \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}_{4\times 7} \quad \begin{matrix} r_2 \to r_2 - r_1 \\ r_3 \to r_3 - r_1 \end{matrix} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\begin{matrix} \\ r_1 \to r_1 - r_2 \\ r_4 \to r_4 - r_2 \\ \\ \end{matrix}\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} r_2 \to r_2 - r_3 \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

$$r_2 \to r_2 - r_3 \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} r_3 \to r_3 - r_4 \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

$$= \ [I_{4\times4}|A]$$

(2) Consider the code [6,3]-code over $GF(3)$ having generator matrix.

$$\begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 2 \\ 1 & 0 & 2 & 0 & 1 & 1 \end{bmatrix}_{3\times6}$$

Interchanging column 1 and column 4

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 2 \\ 0 & 0 & 2 & 1 & 1 & 1 \end{bmatrix}$$

Interchanging column 3 and column 4

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 2 \\ 0 & 0 & 1 & 2 & 1 & 1 \end{bmatrix} = [I_{3\times3}|A_{3\times3}]$$

It is a generator matrix for an equivalent code, where I_k be the $k \times k$ identity matrix, and A is a $k \times (n-k)$ matrix.

Theorem 4.2.1.6. For any $[n,k]$-code C. $(C^{\perp})^{\perp} = C$.

Proof. Clearly $C \subseteq (C^{\perp})^{\perp}$since every vector in C is orthogonal to every vector in $C^{\perp}$. But $\dim((C^{\perp})^{\perp}) = n - (n-k) = k = \dim C$, and so $(C^{\perp})^{\perp} = C$.

Definition 4.2.1.7. A parity-check matrix H for an $[n,k]$-code C be a generate matrix of $C^{\perp}$. so H is an $(n-k)\times n$ matrix satisfying $GH^T=0$ where H^T denotes the transpose of H and 0, is an all-zero matrix. It follows from the Lemma 4.1.3.10 and Theorem 4.2.1.6 that if H is a parity – check matrix of C, then

$$C=\{x\in V(n,q)|x.H^T=0\}$$

Theorem 4.2.1.8. If $G=[I_k|A]$ be a standard form of generator matrix for $[n,k]$-code C, then a parity-check matrix of C be $H=[-A^T|I_{n-k}]$.

Proof. For more details see the Theorem 7.6 in [11].

Definition 4.2.1.9. A parity-check matrix H is called standard form if $H=[B|I_{n-k}]$.

Example 4.2.1.10. The code $[7,4,3]$-code, has standard form of generating matrix as we founded in Example 4.2.1.5 in (1) so,

$$G=\begin{bmatrix}1&0&0&0&1&0&1\\0&1&0&0&1&1&1\\0&0&1&0&1&1&0\\0&0&0&1&0&1&1\end{bmatrix}=\ [I_k|A_{n-k}]$$

$$A^T=\begin{bmatrix}1&1&1&0\\0&1&1&1\\1&1&0&1\end{bmatrix},-A^T=\begin{bmatrix}-1&-1&-1&-0\\-0&-1&-1&-1\\-1&-1&-0&-1\end{bmatrix},-A^T=\begin{bmatrix}1&1&1&0\\0&1&1&1\\1&1&0&1\end{bmatrix}$$

$$H=[-A^T|I_{n-k}]=\begin{bmatrix}1&1&1&0&1&0&0\\0&1&1&1&0&1&0\\1&1&0&1&0&0&1\end{bmatrix}$$

Note 4.2.1.11. If the minus signs are unnecessary in the binary case, if $q=2$ then $-1\equiv 1\ mod\ (2)$ $w$here a parity-check matrix of C is $H=[-A^T|I_{n-k}]$.

PART 5

LINEAR CODES OF ORDER FOUR

5.1. INTRODUCTION

In this chapter, we are studying coding theory. Especial, codes over the rings of order four. Specifically, we consider the linear codes of order four such as the rings of $\mathbb{Z}_4, F_2 + uF_2,$ with $u^2 = 0,$ $F_2 + vF_2$ with $v^2 = v,$ and $F_2 + wF_2$ with $w^2 = w + 1$. The maps of these rings are isometric form Hamming distance to the Lee distance and are said to be Gray map. To further develop the subject, we also study on the Gray maps for the rings of order nine such that $F_3 + vF_3$ with $v^2 = v$ and $F_3 + vF_3$ with $v^2 = 1.$ In the continuity, we observed that there are different weights over these rings namely, Lee weight, the Hamming weight, Bachoc weight and the Euclidean weight. We also give our consideration to the inner products which are basically representing a relationship between two vectors. The highly used inner products are Euclidean inner product and Hermitian inner products for the ring of order four. In [9], authors studied on symmetrized weight enumerators for the ring $F_2 + vF_2$ with $v^2 = v$. However, in this chapter we also generalized symmetrized weight enumerators for the ring $\mathbb{Z}_4, F_2 + uF_2,$ with $u^2 = 0$. Generators for the rings are widely studied in linear coding theory, for more details we recommend [8], [9] and [10]. Therefore, in this study generators for the rings of order four are also considered and some important theories are denoted.

Theorem 5.1.1. (Gleason-Pierce) Let C be a formally self-dual divisible code of length n over F_q, also suppose δ is the largest positive integer divide every non-zero weights of C. Next we have following conditions:

Type (I) $q = 2$ and $\delta = 2$;

Type (II) $q = 2$ and $\delta = 4$;

Type (III) $q = 3$ and $\delta = 3$;

Type (IV) $q = 4$ and $\delta = 2$ or

Type (V) q be arbitrary, $\delta = 2$, and $w_C(x, y) = (x^2 + (q-1)y^2)^{n/2}$.

Proof. For more details see [20].

5.2. CODES OVER RINGS OF ORDER FOUR

This section is related to the codes over the commutative rings of order four. There are four commutative rings with order four. So, we give their properties and examples with related to the coding theory.

5.2.1. The Element of Rings of Order Four

(i) $\mathbb{Z}_4$, it is elements are $\{0, 1, 2, 3\}$. We can give some examples of codewords over the ring $\mathbb{Z}_4$ with the lengths 4 or 5 such that $\{0221, 1102\}$ or $\{20201, 11022\}$.

(ii) $F_2[u]/< u^2 >$. It is also written as $F_2 + uF_2 = \{0, 1, u, 1+u\}$ with $u^2 = 0$, we can give some examples of codewords over the ring $F_2 + uF_2$ with the lengths 4 or 5 such that $\{u110, 11u1\}$ or $\{uu001, 110u(1+u)\}$.

(iii) $F_2[v]/< v^2 + v >$. It is also written as $F_2 + vF_2 = \{0,1, v, 1+v\}$ with $v^2 = v$, we can give some examples of codewords over the ring $F_2 + vF_2$ with the lengths 4 or 5 such that $\{1v10, (1+v)100\}$ or $\{11vv0, 11vvv\}$.

(iv) $F_4 = F_2[\omega]/< \omega^2 + \omega + 1 >= \{0, 1, \omega, 1+\omega\}$. We can give some examples of codewords over the ring F_4 with the lengths 3 or 6 such that $\{11w, 1w1\}$ or $\{ww0111, (1+w)11w01\}$.

Definition 5.2.2. A linear code of C of length n over $\mathbb{R}$ is defined to be an $\mathbb{R}$-submodule of $\mathbb{R}^n$, and the elements of C are said to be a codewords. A matrix whose rows generate C is described as a C generator matrix.

Definition 5.2.3. Suppose $\mathbb{R}$ is a finite ring and linear code over the alphabets of $\mathbb{R}$ with length n is a submodule of $\mathbb{R}^n$.

5.3. WEIGHTS OF CODES

In this section, we considered different weights of the codewords over the rings $\mathbb{Z}_4$, $F_2 + uF_2, F_2 + vF_2\ or\ F_4$. Also, we considered Hamming distance and Lee distances and between two codewords. In the following of the section, the minimum Lee, Bachoc, Hamming and Euclidean weights, d_L, d_B, d_H and d_E of C are considered as the smallest Lee, Bachoc, Hamming and Euclidean weights among all non-zero codewords of C.

5.3.1. Hamming Weights

The number of non-zero components in a codeword defines a Hamming weight. Let $\{00000,\ 01101, 10110,\ 11011\}$ be codewords over $\mathbb{Z}_4$. Then Hamming weights of each codewords are $w_H(00000) = 0,\ w_H(01101) = 3,\ w_H(10110) = 3,$ $w_H(11011) = 4.$

Let $(01u(1+u)0)$ and $(110\,uu)$ be two codewords over the ring $F_2 + uF_2$ with $u^2 = 0.$ Then the Hamming weights are $w_H(01u(1+u)0\ ) = 3$ and $w_H(110uu\ ) = 4.$

Let $(101vv)$ and $(11v00)$ be two codewords over the ring $F_2 + vF_2$ with $v^2 = v.$ Then the Hamming weights are $w_H(101vv) = 4$ and $w_H(11v00) = 3.$

5.3.2. Euclidean Weights

The elements of the Euclidean weights for the ring $\mathbb{Z}_4$ are $w_E(0) = 0$, $w_E(1) = 1$, $w_E(2) = 4$ and $w_E(3) = 1$. The Euclidean weights of a codewords are the rational sum of the Euclidean weights. For example, Euclidean weights of (2130011) and (1023012) codewords are

$$\begin{aligned} w_E(2130011) &= w_E(2) + w_E(1) + w_E(3) + w_E(0) + w_E(0) + w_E(1) + w_E(1) \\ &= 4 + 1 + 1 + 0 + 0 + 1 + 1 = 8. \end{aligned}$$

$$\begin{aligned} w_E(\ 1023012) &= w_E(1) + w_E(0) + w_E(2) + w_E(3) + w_E(0) + w_E(1) + w_E(2) \\ &= 1 + 0 + 4 + 1 + 0 + 1 + 4 = 11. \end{aligned}$$

The elements of the Euclidean weights for the ring $F_2 + uF_2 = \{0,1,u,1+u\}$ with $u^2 = 0$ are $w_E(0) = 0,\ w_E(1) = 1, w_E(u) = 4$ and $w_E(1+u) = 1$. The Euclidean weight of a codeword is a rational sum of the Euclidean weights of it is component. For example, Euclidean weights of $(u1u(1+u)110)$ and $(011(1+u)0u1)$ codewords are

$$\begin{gathered} w_E(u1u(1+u)110) = w_E(u) + w_E(1) + w_E(u) + w_E(1+u) + w_E(1) + w_E(1) \\ +w_E(0) = 4 + 1 + 4 + 1 + 1 + 1 + 0 = 12 \end{gathered}$$

$$\begin{gathered} w_E(011(1+u)0u1) = w_E(0) + w_E(1) + w_E(1) + w_E(1+u) + w_E(0) + w_E(u) \\ + w_E(1) = 0 + 1 + 1 + 1 + 0 + 4 + 1 = 8 \end{gathered}$$

5.3.3. Lee Weights

The elements of the Lee weights for the ring $\mathbb{Z}_4$ are $w_L(0) = 0, w_L(1) = 1, w_L(2) = 2$ and $w_L(3) = 1$. The Lee weight of a codeword is a rational sum of the Lee weights. For example, Lee weights of (0113122) and (3310200) codewords are

$$\begin{aligned} w_L(0113122) &= w_L(0) + w_L(1) + w_L(1) + w_L(3) + w_L(1) + w_L(2) + w_L(2) \\ &= 0 + 1 + 1 + 1 + 1 + 2 + 2 = 8 \end{aligned}$$

$$w_L(3310200\ ) = w_L(3) + w_L(3) + w_L(1) + w_L(0) + w_L(2) + w_L(0) + w_L(0)$$
$$= 1 + 1 + 1 + 0 + 2 + 0 + 0 = 5$$

The elements of the Lee weights for the ring $F_2 + uF_2 = \{0,1,u,1+u\}$ with $u^2 = 0$ are $w_L(0) = 0$, $w_L(1) = 1$, $w_L(u) = 2$ and $w_L(1+u) = 1$. Respectively, such that Lee weight of $(uu1101(1+u))$ and $(00u1110)$ codewords are

$$w_L\big(uu1101(1+u)\big) = w_L(u) + w_L(u) + w_L(1) + w_L(1) + +w_L(0) + w_L(1) + w_L(1+u) = 2 + 2 + 1 + 1 + 0 + 1 + 1 = 8$$

$$w_L(00u1110) = w_L(0) + w_L(0) + w_L(u) + w_L(1) + w_L(1) + w_L(1) + w_L(0)$$
$$= 0 + 0 + 2 + 1 + 1 + 1 + 0 = 5$$

The elements of the Lee weights for the ring $F_2 + vF_2 = \{0,1,v,1+v\}$ with $v^2 = v$ are $w_L(0) = 0$, $w_L(1) = 2$, $w_L(v) = 1$ and $w_L(1+v) = 1$. Respectively, such that Lee weight of $(001(1+v)v1v)$ and $(1vv0010\ )$ codewords are

$$w_L(001(1+v)v1v) = w_L(0) + w_L(0) + w_L(1) + w_L(1+v) + w_L(v) + w_L(1) + w_L(v) = 0 + 0 + 2 + 1 + 1 + 2 + 1 = 7$$

$$w_L(1vv0010\ ) = w_L(1) + w_L(v) + w_L(v) + w_L(0) + w_L(0) + w_L(1) + w_L(0)$$
$$= 2 + 1 + 1 + 0 + 0 + 2 + 0 = 6$$

5.3.4. Bachoc Weights

The elements of the Bachoc weights for the ring $F_2 + vF_2 = \{0,1,v,1+v\}$ with $v^2 = v$ are $w_B(0) = 0$, $w_B(1) = 1$, $w_B(v) = 2$ and $w_B(1+v) = 2$. Bachoc weights of the following codewords are calculated as

$$w_B\big(1v1v01(1+v)\big) = w_B(1) + w_B(v) + w_B(1) + w_B(v) + w_B(0) + w_B(1) + w_B(1+v) = 1 + 2 + 1 + 2 + 0 + 1 + 2 = 9$$

$$w_B(vv1001v) = w_B(v) + w_B(v) + w_B(1) + w_B(0) + w_B(0) + w_B(1) + w_B(v)$$
$$= 2 + 2 + 1 + 0 + 0 + 1 + 2 = 8$$

Note 4.3.4.1. The Lee and the Hamming distance between two codewords x and y are the Lee and Hamming weights of $x - y$. For example, let $x = 01123$ and $y = 11200$ be two codewords over $\mathbb{Z}_4$. The Hamming distance and Lee distance of x and y are

$$d_H(x,y) = w_H(x-y) = w_H(01123\ - 11200) = \ w_H(30323) = 4$$
$$d_L(x,y) = w_L(x-y) = w_L(01123\ - 11200) = \ w_L(30323) =$$
$$w_L(3) + w_L(0)\ + w_L(3) + w_L(2) + w_L(3) = 1 + 0 + 1 + 2 + 1 = 5$$

The minimum Lee, Bachoc, Hamming and Euclidean weights, d_L, d_B, d_H and d_E of C are the smallest Lee, Bachoc, Hamming and Euclidean weights.

5.4. CHINESE REMAINDER THEOREM FOR RINGS

Definition 5.4.1. In a commutative ring $\mathbb{R}$, two ideals I_1 and I_2 are said coprime ideal if, $I_1 + I_2 = \mathbb{R}$.

Proposition 5.4.2. Suppose $\mathbb{R}$ is a commutative ring with unity I and J are two ideals of $\mathbb{R}$. Afterwards,

(i) If summations of two ideals $I + J = \mathbb{R}$, then $IJ = I \cap J$.

(ii) If $I_1, I_2, \dots, I_n$ are coprime in pairs, then the multiplication are

$$I_1.I_2\ \dots\ I_n = \bigcap_{i=1}^{n} I_i$$

Proof. (i) $IJ \subseteq I \cap J$ is straight forward. Let $x \in I \cap J$, since $I + J = \mathbb{R}$, there exists $a \in I$ and $b \in J$ such that $a + b = 1$. So we have $x = x.1 = x(a+b) = xa + xb$ and $xa, xb \in I \cap J$. Hence $x \in IJ$.

(ii) Prove is extended version of (i).

Theorem 5.4.3. (Chinese Remainder Theorem) If $\mathbb{R}$ is a commutative ring and $I,\ J$ are proper ideals with $I + J = \mathbb{R}$, then $\mathbb{R}/I \cap J \cong \mathbb{R}/I \oplus \mathbb{R}/J$.

Proof. Define a map between $\mathbb{R}/I \cap J$ and $\mathbb{R}/I \oplus \mathbb{R}/J$, such that $\varphi: \mathbb{R} \to \mathbb{R}/I \oplus \mathbb{R}/J$ for any $r \in R$, we have $\varphi(r) = (r + I, r + J)$.

(i) Let $r_1, r_2 \in \mathbb{R}$ such that $r_1 = r_2$, then $\varphi(r_1) = (r_1 + I, r_1 + J) = (r_2 + I, r_2 + J) = \varphi(r_2)$ so φ is a well-defined function.

(ii) Let $r_1, r_2 \in \mathbb{R}$, $\varphi(r_1 + r_2) = ((r_1 + r_2) + I, (r_1 + r_2) + J) = (r_1 + I, r_1 + J) + (r_2 + I, r_2 + J) = \varphi(r_1) + \varphi(r_2)$.

Suppose $r_1, r_2 \in \mathbb{R}$, $\varphi(r_1 . r_2) = (r_1 . r_2 + I, r_1 . r_2 + J) = (r_1 + I, r_1 + J).(r_2 + I, r_2 + J) = \varphi(r_1).\varphi(r_2)$.

(iii) Let $\overline{r_1}, \overline{r_2} \in \mathbb{R}/I \oplus \mathbb{R}/J$ here $(\overline{r_1}, \overline{r_2}) = (r_1 + I, r_2 + J)$ since $I + J = \mathbb{R}$, let $r_1 = a_1 + b_1$ and $r_2 = a_2 + b_2$, $a_1, a_2 \in I$ and $b_1, b_2 \in J$.
$\varphi(b_1 + a_2) = (b_1 + a_2 + I, b_1 + a_2 + J) = (b_1 + I, a_2 + J) = (\overline{r_1}, \overline{r_2})$.

(iv) Let $\varphi(r_1) = \varphi(r_2)$ such that $(r_1 + I, r_1 + J) = (r_2 + I, r_2 + J)$, so it is easy to see that $r_1 = r_2$. Hence φ be an isomorphism.

(v) Now we want to show that $\ker \varphi = I \cap J$.

(⊆) Let $r \in \ker \varphi$, then $\ker \varphi = \{r \in \mathbb{R}: \varphi(r) = (0 + I, 0 + J) = (I, J)\}$ so $r \in I$ and $r \in J$. If $r \in I$ and $r \in J$, then $r \in I \cap J$.

(⊇) Let $s \in I \cap J$, so $s \in I$ and $s \in J$. Then, $\varphi(s) = (s + I, s + J) = (I, J)$ and $s \in \ker \varphi$. So, by the first isomorphism theorem we can say that $\mathbb{R}/\ker \varphi \cong \mathbb{R}/I \oplus \mathbb{R}/J$ such that

$$\mathbb{R}/I \cap J \cong \mathbb{R}/I \oplus \mathbb{R}/J$$

5.5. GRAY MAPS

In this section, we want to know what is the difference between codes on finite field and codes on rings. At this point, we studied on the Gray maps to learn the relationship between codes over finite fields and codes over rings, and also we use Gray maps with knowledge of the Chinese Remainder Theory to easily identify the Gray maps. In the beginning, Gray maps are defined for the ring of order four and then continue with order nine to further enrich the topics.

5.5.1. Gray Map for the Ring $\mathbb{Z}_4$

Let $\mathbb{R} = \mathbb{Z}_4 = \{0, 1, 2, 3\}$, we now define a Gray map between ($\mathbb{R}$, Lee distance) and (F_2^2, Hamming distance). This map is a distance preserving for the binary Hamming spaces. To all element $a + 2b \in \mathbb{R}$ where $a, b \in F_2$, we have

$$\varphi_{\mathbb{Z}_4}: \mathbb{Z}_4 \to F_2 \times F_2$$
$$\varphi_{\mathbb{Z}_4}(a + 2b) = (b, a + b).$$

$\varphi_{\mathbb{Z}_4}$ is a non-linear map. In general, the Gray image of a $\mathbb{Z}_4$ linear code cannot be a binary linear code. However, it has a significant importance about the isometry from ($\mathbb{R}^n$, Lee distance) to (F_2^{2n}, Hamming distance). Moreover, the Gray image of linear codes over $\mathbb{Z}_4$ are distance-invariant binary codes, even if they are non-linear.

5.5.2. Gray Map for the Ring $F_2 + uF_2$ With $u^2 = 0$

Let $\mathbb{R} = F_2 + uF_2 = \{0, 1, u, 1 + u\}$ with $u^2 = 0$, we now define a Gray map between ($\mathbb{R}$, Lee distance) and (F_2^2, Hamming distance). Since only maximal ideal of $F_2 + uF_2$ with $u^2 = 0$ is $\langle u \rangle$, $\mathbb{R}$ is a local ring. The Gray map of $F_2 + uF_2$ can be define as follow:

$$\varphi_u: F_2 + uF_2 \to F_2 \times F_2,$$

$$\varphi_u(a + ub) = (b, a + b).$$

Theorem 5.5.2.1. φ_u is a F_2-linear map.

Proof. Let $x = a_1 + ub_1$ and $y = \ a_2 + ub_2$ be two elements of $\mathbb{R} = \mathrm{F}_2 + u\mathrm{F}_2$.

$$\begin{aligned}\varphi_u(x-y) &= \varphi_u\big((a_1+ub_1)-(a_2+ub_2)\big) = \varphi_u((a_1-a_2)+u(b_1-b_2)) \\ &= \big(\,(b_1-b_2),(a_1-a_2)+\ (b_1-b_2)\big) \\ &= \big((b_1-b_2),(a_1+b_1)-(a_2+b_2)\,\big) \\ &= (b_1,a_1+\ b_1)-(b_2,a_2+b_2) = \varphi_u(a_1+ub_1)-\varphi_u(a_2+ub_2) \\ &= \varphi_u(x)-\varphi_u(y)\end{aligned}$$

Theorem 5.5.2.2. φ_u is a distance preserving map from ($\mathbb{R}$, Lee distance) to (F_2^2, Hamming distance).

Proof. Let $x = a_1 + ub_1$ and $y = \ a_2 + ub_2$ be elements of $\mathbb{R} = \mathrm{F}_2 + u\mathrm{F}_2$. By the Theorem 5.5.2.1, we have φ_u is a linear map so

$$\begin{aligned}d_L(x,y) = w_L(x-y) = w_H(\varphi_u(x-y)) &= w_H\big(\varphi_u(x)-\varphi_u(y)\big) \\ &= d_H\big(\varphi_u(x),\varphi_u(y)\big).\end{aligned}$$

5.5.3. Gray Map for the Ring $F_2 + vF_2$ With $v^2 = v$

Let $\mathbb{R} = F_2 + vF_2 = \{0,1,v,1+v\}$ with $v^2 = v$, we now define a Gray map between ($\mathbb{R}$, Lee distance) and (F_2^2, Hamming distance) by using the Chinese remainder theorem,

$$\varphi : \mathbb{R} \to \mathbb{R}/I \ \oplus \ \mathbb{R}/J$$

and $I + J = \mathbb{R}$, maximal ideals of $\mathbb{R}$ are $\langle v \rangle = \{vk : k \in \mathbb{R}\} = \{0, v\}$ and $\langle 1+v \rangle = \{(1+v)l : l \in \mathbb{R}\} = \{0, 1+v\}$. So $\mathbb{R}$ is a semi-local ring.

By the Definition 3.1.1.21, we can show that $\mathbb{R}/\langle v\rangle \cong$ field and $\mathbb{R}/\langle 1+v\rangle \cong$ field

$$\mathbb{R}/\langle v\rangle = \{(a+vb)+\langle v\rangle : a,b \in F_2\} = \{(a+vb)+\{0,v\}: a,b \in F_2\} = \{0,1\} \cong F_2$$

$$\mathbb{R}/\langle 1+v\rangle = \{(a+vb)+\langle 1+v\rangle : a,b \in F_2\} = \{(a+vb)+\{0,1+v\}: a,b \in F_2\} = \{0,1\} \cong F_2$$

So, we have $\varphi: F_2+vF_2 \to F_2 \times F_2\ by\ \varphi(a+vb) \to (a+b,a)$.

Theorem 5.5.3.1. φ is a linear map.

Proof. We need to show that $\varphi(x-y)=\varphi(x)-\varphi(y)$. Let $x=a_1+vb_1$ and $y=a_2+vb_2$ be elements of $\mathbb{R}=\mathrm{F}_2+v\mathrm{F}_2$.

$$\begin{aligned}\varphi(x-y) = \varphi\big((a_1+vb_1)-(a_2+vb_2)\big) &= \varphi((a_1-a_2)+v(b_1-b_2))\\ &= \big((a_1-a_2)+(b_1-b_2),(a_1-a_2)\big)\\ &= \big((a_1+b_1)-(a_2+b_2),(a_1-a_2)\big)\\ &= (a_1+b_1,a_1)-(a_2+b_2,a_2) = \varphi(a_1+vb_1)-\varphi(a_2+vb_2)\end{aligned}$$

Theorem 5.5.3.2. φ is a distance preserving map from ($\mathbb{R}$, Lee distance) to (F_2^2, Hamming distance).

Proof. Let $x=a_1+vb_1$ and $y=a_2+vb_2$ be elements of $\mathbb{R}=\mathrm{F}_2+v\mathrm{F}_2$. By the Theorem 5.5.3.1, we have φ is a linear map so

$$d_L(x,y)=w_L(x-y)=w_H\big(\varphi(x-y)\big)=w_H\big(\varphi(x)-\varphi(y)\big)=d_H\big(\varphi(x),\varphi(y)\big).$$

In the following, we can mention some rings with order 9 and then define their Gray maps.

5.5.4. Gray Map for the Ring $F_3 + vF_3$ With $v^2 = v$

Let $\mathbb{R} = F_3 + vF_3 = \{0, 1, 2, v, 2v, 1 + v, 1 + 2v, 2 + v, 2 + 2v\}$ with $v^2 = v$, we now define a Gray map between ($\mathbb{R}$, Lee distance) and (F_3^n, Hamming distance) by using Chinese remainder theorem,

$$\varphi_{3,1}: \mathbb{R} \to \mathbb{R}/I \oplus \mathbb{R}/J$$

and $I + J = \mathbb{R}$, maximal ideals of $\mathbb{R}$ are $\langle v\rangle = \{vk: k \in \mathbb{R}\} = \{0, v, 2v\} \subset \mathbb{R}$ and $\langle v - 1\rangle = \{(v - 1)l: l \in \mathbb{R}\} = \{0, 1 + 2v, 2 + v\} \subset \mathbb{R}$. So $\mathbb{R}$ is a semi-local ring. By the Definition 3.1.1.21, we can show that $\mathbb{R}/\langle v\rangle \cong$ field and $\mathbb{R}/\langle v - 1\rangle \cong$ field

$$\mathbb{R}/\langle v\rangle = \{(a + vb) + \langle v\rangle: a, b \in F_3\} = \{(a + vb) + \{0, v, 2v\}: a, b \in F_3\} = \{0,1,2\} \cong F_3$$

$$\mathbb{R}/\langle v - 1\rangle = \{(a + vb) + \langle v - 1\rangle: a, b \in F_3\} = \{(a + vb) + \{0, 1 + 2v, 2 + v\}: a, b \in F_3\} = \{0,1, 2\} \cong F_3.$$

$$\varphi_{3,1}: \mathbb{R} \to \mathbb{R}/\langle v\rangle \oplus \mathbb{R}/\langle v - 1\rangle$$

Let $a + vb = x(v) + y(v - 1)$, so $x = a + b, y = -a$ for any $a, b \in F_3$. So, we have $\varphi_{3,1}: F_3 + vF_3 \to F_3 \times F_3$, the Gray map of $\varphi_{3,1}(a + vb) = (a + b, - a)$.

Theorem 5.5.4.1. $\varphi_{3,1}$ is a linear map.

Proof. We need to show that $\varphi_{3,1}(x - y) = \varphi_{3,1}(x) - \varphi_{3,1}(y)$. Let $x = a_1 + vb_1$ and $y = a_2 + vb_2$ are the elements of $\mathbb{R} = F_3 + vF_3$.

$$\begin{aligned}\varphi_{3,1}(x - y) &= \varphi_{3,1}\big((a_1 + vb_1) - (a_2 + vb_2)\big) = \varphi_{3,1}((a_1 - a_2) + v(b_1 - b_2)) \\ &= \big((a_1 - a_2) + (b_1 - b_2), -(a_1 - a_2)\big) = \big((a_1 + b_1) - (a_2 + b_2), -(a_1 - a_2)\big) \\ &= (a_1 + b_1, -a_1) - (a_2 + b_2, -a_2) \\ &= \varphi_{3,1}(a_1 + vb_1) - \varphi_{3,1}(a_2 + vb_2)\end{aligned}$$

Theorem 5.5.4.2. $\varphi_{3,1}$ is a distance preserving map from ($\mathbb{R}$, Lee distance) to (F_3^n, Hamming distance).

Proof. Let $x = a_1 + vb_1$ and $y = a_2 + vb_2$ be elements of $\mathbb{R} = F_3 + vF_3$. By the Theorem 5.5.4.1, we have $\varphi_{3,1}$ is a linear map so

$$d_L(x,y) = w_L(x-y) = w_H\left(\varphi_{3,1}(x-y)\right) = w_H\left(\varphi_{3,1}(x) - \varphi_{3,1}(y)\right)$$
$$= d_H\left(\varphi_{3,1}(x), \varphi_{3,1}(y)\right)$$

5.5.5. Gray Map For The Ring $F_3 + vF_3$ With $v^2 = 1$

Let $\mathbb{R} = F_3 + vF_3 = \{0, 1, 2, v, 2v, 1+v, 1+2v, 2+v, 2+2v\}$ with $v^2 = 1$, we now define a Gray map between ($\mathbb{R}$, Lee distance) and (F_3^n, Hamming distance) by using Chinese Remainder Theorem,

$$\varphi_{3,2}: \mathbb{R} \to \mathbb{R}/I \oplus \mathbb{R}/J$$

and $I + J = \mathbb{R}$, maximal ideals of $\mathbb{R}$ are $\langle 1+v \rangle = \{(1+v)(a+vb): a,b \in F_3\} = \{0, 1+v, 2+2v\} \subset \mathbb{R}$ and $\langle v-1 \rangle = \{(v-1)(a+vb): a,b \in F_3\} = \{0, 1+2v, 2+v\} \subset \mathbb{R}$. So $\mathbb{R}$ is a semi-local ring.
By the Definition 3.1.1.21, we can show that $\mathbb{R}/\langle v-1 \rangle \cong$ field and $\mathbb{R}/\langle 1+v \rangle \cong$ field

$\mathbb{R}/\langle v-1 \rangle = \{(a+vb) + \langle v-1 \rangle: a,b \in F_3\} = \{(a+vb) + \{0, 1+2v, 2+v\}: a,b \in F_3\} = \{0,1,2\} \cong F_3$.

$\mathbb{R}/\langle 1+v \rangle = \{(a+vb) + \langle 1+v \rangle: a,b \in F_3\} = \{(a+vb) + \{0,1+v, 2+2v\}: a,b \in F_3\} = \{0,1,2\} \cong F_3$.

$$\varphi_{3,2}: \mathbb{R} \to \mathbb{R}/\langle v-1 \rangle \oplus \mathbb{R}/\langle 1+v \rangle$$

So, $\varphi_{3,2}: F_3 + vF_3 \to F_3 \times F_3$. Also, for any $x, y \in F_3$, we have $a + vb = (a - b)(v - 1) - (a + b)(1 + v)$. Thus, the Gray map of $\varphi_{3,2}(a + vb) = (a - b, -(a + b))$.

Theorem 5.5.5.1. $\varphi_{3,2}$ be a linear map.

Proof. We need to show that $\varphi_{3,2}(x - y) = \varphi_{3,2}(x) - \varphi_{3,2}(y)$. Let $x = a_1 + vb_1$ and $y = a_2 + vb_2$ be elements of $\mathbb{R} = F_3 + vF_3$.

$$\begin{aligned}\varphi_{3,2}(x - y) = \varphi_{3,2}\big((a_1 + vb_1) - (a_2 + vb_2)\big) &= \varphi_{3,2}((a_1 - a_2) + v(b_1 - b_2)) \\ &= ((a_1 - a_2) - (b_1 - b_2), -((a_1 - a_2) + (b_1 - b_2))) \\ &= \big((a_1 - b_1) - (a_2 - b_2), -\big((a_1 + b_1) - (a_2 + b_2)\big) \big) \\ &= (a_1 - b_1, -(a_1 + b_1)) - (a_2 - b_2, -(a_2 + b_2)) \\ &= \varphi_{3,2}(a_1 + vb_1) - \varphi_{3,2}(a_2 + vb_2)\end{aligned}$$

Theorem 5.5.5.2. $\varphi_{3,2}$ is a distance preserving map from ($\mathbb{R}$, Lee distance) to (F_3^n, Hamming distance).

Proof. Let $x = a_1 + vb_1$ and $y = a_2 + vb_2$ be elements of $\mathbb{R} = F_3 + vF_3$. By the Theorem 5.5.5.1, we have $\varphi_{3,2}$ is a linear map so

$$\begin{aligned}d_L(x, y) = w_L(x - y) = w_H\left(\varphi_{3,2}(x - y)\right) &= w_H\left(\varphi_{3,2}(x) - \varphi_{3,2}(y)\right) \\ &= d_H\left(\varphi_{3,2}(x), \varphi_{3,2}(y)\right).\end{aligned}$$

Note 5.5.5.3. Let $\varphi_{\mathbb{Z}_4}$, φ_u and φ be three Gray maps defined as above and they are also isometries from ($\mathbb{R}$, Lee distance) to (F_2^2, Hamming distance). So we have the followings:

(i) $\varphi_u(0) = 00,\ \varphi_u(1) = 11,\ \varphi_u(1 + u) = 10,\ \varphi_u(u) = 11,$

(ii) $\varphi_{\mathbb{Z}_4}(0) = 00,\ \varphi_{\mathbb{Z}_4}(1) = 11,\ \varphi_{\mathbb{Z}_4}(3) = 10,\ \varphi_{\mathbb{Z}_4}(2) = 11,$

(iii) $\varphi(0) = 00,\ \varphi(1) = 11,\ \varphi(1 + v) = 10,\ \varphi(v) = 11,$

These Gray maps can be extended to $\mathbb{R}^n$. The maps φ_u and φ are F_2-linear, but $\varphi_{\mathbb{Z}_4}$ is not.

5.6. INNER PRODUCT OF ELEMENTS OF $\mathbb{R}^n$

Geometric concepts like the length of a vector, the angle between two vectors, orthogonality, and so on are all expressed by the dot product. Now, we are going to apply geometric principles to abstract vector spaces, allowing us to abstract vectors using geometric concepts.

5.6.1. Basic Notions

Definition 5.6.1.1. For $x, y \in \mathbb{R}^n$, dot product of x and y is denoted by $x.y$, is defined as $x.y = x_1.y_1 + \cdots + x_n.y_n$ where $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$.

Example 5.6.1.2. Assume that $x = (u, 1, (1+u), 0)$ and $y = (0, u, 1, u)$ be two codewords over $F_2 + uF_2$ with $u^2 = 0$. The dot product of x and y is

$$\begin{aligned} x.y = (u, 1, (1+u), 0).(0, u, 1, u) &= u.0 + 1.u + (1+u).1 + 0.u \\ &= 0 + u + 1 + u + 0 = 1 \end{aligned}$$

Definition 5.6.1.3. The length of a vector x in $\mathbb{R}^n$ is called the norm of x, denoted $\|x\|$. The norm of x= $(x_1, \ldots, x_n) \in \mathbb{R}^n$ is $\|x\| = \sqrt{{x_1}^2 + \cdots + {x_n}^2}$. The norm is not linear on $\mathbb{R}^n$.

Note 5.6.1.4. The dot product of two vectors in $\mathbb{R}^n$ is a scalar number, not a vector. Obviously $x.x = \|x\|^2$ for all $x \in \mathbb{R}^n$. The properties of the dot product on $\mathbb{R}^n$ are as follows:

(i) $x.x \geq 0$ for all $x \in \mathbb{R}^n$;
(ii) $x.x = 0$ if and only if $x = 0$;
(iii) For $y \in \mathbb{R}^n$ fixed, the map from $\mathbb{R}^n$ to $\mathbb{R}$ that sends $x \in \mathbb{R}^n$ to xy is a linear;
(iv) $x.y = y.x$ For all $x, y \in \mathbb{R}^n$;

Definition 5.6.1.5. A generalization of the dot product is an inner product. It is a method for multiplying vectors together in a vector space, with the results being a scalar. An inner product $\langle .,. \rangle$ is more exact for a real vector space, satisfies the following axioms. Suppose u, v and $w \in V$ be vectors and α be a scalar in $\mathbb{R}$, then:

(i) $\langle u + v, w \rangle = \langle u, w \rangle + \langle v, w \rangle$;
(ii) $\langle \alpha v, w \rangle = \alpha \langle v, w \rangle$;
(iii) $\langle v, w \rangle = \langle w, v \rangle$;
(iv) $\langle v, v \rangle \geq 0$, if and only if $v = 0$;

An inner product space is a vector space and it has an inner product on it. This concept also stands true for an abstract vector space over any field.

5.6.2. Euclidean Inner Products

Definition 5.6.2.1. Let $v = \{v_1, v_2, v_3, \dots, v_n\}, w = \{w_1, w_2, w_3, \dots, w_n\} \in F_q^n$.

(i) The scalar product also known as the Euclidean inner product or the dot product of v and w is defined as $v.w = \{v_1w_1 + v_2w_2 + v_3w_3 + \cdots + v_nw_n\} \in F_q^n$

(ii) v and w are called orthogonal if $v.w = 0$.

(iii) Assume C be a non-empty subset of F_q^n. The orthogonal complement $C^\perp$of C is defined to be

$$C^\perp = \{v \in F_q^n | v.u = 0 , \forall\, u \in C\}$$

Example 5.6.2.2. Assume that $x = (v, (1 + v)1,1,0,)$ and $y = (1,0, v, v, (1 + v))$ be two codewords over $F_2 + vF_2$, with $v^2 = v$. Then their Euclidean inner product is

$$\begin{aligned} x.y &= (v, (1 + v)1,1,0).\big(1,0, v, v, (1 + v)\big) \\ &= v.1 + (1 + v).0 + 1.v + 1.v + 0.(1 + v) = v + 0 + v + v + 0 \\ &= v \end{aligned}$$

5.6.3. Hermitian Inner Products

Definition 5.6.3.1. Let $x = \{x_1, \dots, x_n\}$ and $y = \{y_1, \dots, y_n\}$ be two elements of $\mathbb{R}^n$ wherever the operations are performing to $\mathbb{R}$. To codes over $F_2 + vF_2$ with $v^2 = v$, we can defined the Hermitian inner product of x and y in $\mathbb{R}^n$such that $\sum x_i\overline{y_\imath}$ where $\overline{0} = 0, \overline{1} = 1, \overline{v} = v + 1$ and $\overline{v + 1} = v$.

Example 5.6.3.2. Assume that $x = (v, (1 + v), 0, 1)$ and $y = (1, (1 + v), v, 0)$ be two codewords over $F_2 + vF_2$. Then the Hermitian inner product is

$$\sum x_i\overline{y_\imath} = v.\overline{1} + (1 + v).\overline{(1 + v)} + 0.\overline{v} + 1.\overline{0} = v + 0 + 0 + 0 = v$$

5.7. WEIGHT ENUMERATORS

We start this section with basic notions about the weight enumerators and its relationship with Macwilliam identities. Then we continue with the description of the symmetrized weight enumarators and its relationship with the rings of order four.

Definition 5.7.1. If C is a linear $[n,k]$-code, its weight enumerators are define to be the polynomial.

$$w_c(z) = \sum_{i=0}^{n} A_i z^i = A_0 + A_1 z + A_2 z^2 \ldots + A_n z^n$$

where A_i defines the number of weights i codewords in C. Another way of writing $w_c(z)$ is

$$w_c(z) = \sum_{x \in C} z^{w(x)}$$

Example 5.7.2. (i) Let C be binary even weight code of length 5, for $C = \{00000, 01101, 10110, 11011\}$, one gets $w(00000) = 0$, $w(01101) = 3$, $w(10110) = 3$ and $w(11011) = 4$. Also, $C^{\perp}$=$\{00000, 11011\}$ and weight of each codewords is $w(00000) = 0$ and $w(11011) = 4$. The weight enumerators of C and $C^{\perp}$ are,

$$w_C(z) = \sum_{i=0}^{n} A_i z^i = A_0 + A_1 z + A_2 z^2 + A_3 z^3 + A_4 z^4 = 1 + 0 + 0 + 2z^3 + z^4$$

$$= 1 + 2z^3 + z^4$$

$$w_{C^{\perp}}(z) = \sum_{i=0}^{n} A_i z^i = A_0 + A_1 z + A_2 z^2 + A_3 z^3 + A_4 z^4 = 1 + 0 + 0 + 1z^4$$

$$= 1 + z^4$$

(ii) The code $C = \{00, 11\}$ is self-dual code and so $w(00) = 0$ and $(11) = 2$ $w_C(z) = w_{C^{\perp}}(z) = 1 + z^2$.

Lemma 5.7.3. Suppose x is a fixed vector in $V(n,2)$ and assume z is indeterminate. Then the following polynomial identity holds

$$\sum_{y\in V(n,2)} z^{w(y)}(-1)^{x.y} = (1-z)^{w(x)}(1+z)^{n-w(x)}$$

Proof. For more details see Lemma (13.4) in [11].

Theorem 5.7.4. (The MacWilliams identity for the binary linear codes) If C is a binary $[n,k]$-code with the dual code $C^{\perp}$, then

$$w_{C^{\perp}}(z) = \frac{1}{2^k}(1+z)^n w_C\left(\frac{1-z}{1+z}\right)$$

Proof. For more details see Theorem (13.5) in [11].

Theorem 5.7.5. (The MacWilliams identity for general linear codes) If C is a linear $[n,k]$-code over $GF(q)$ with the dual code $C^{\perp}$, then

$$w_{C^{\perp}}(z) = \frac{1}{q^k}[1+(q-1)z]^n\, w_C\left(\frac{1-z}{1+(q-1)z}\right)$$

Remark 5.7.6. If C is a binary $[n,k]$-code, then, since the dual code $C^{\perp}$is just C, we can write the MacWilliams identity is the (often more useful) from,

$$w_C(z) = \frac{1}{2^{n-k}}(1+z)^n w_{C^{\perp}}\left(\frac{1-z}{1+z}\right)$$

Example 5.7.7. For the code $C = \{000, 011, 101, 110\}$ and $k = 2$,

(i) We have $w_C(z) = 1 + 3z^2$ and by the Theorem 5.7.4,

$$w_{C^\perp}(z)\,\frac{1}{2^k}(1+z)^n w_C\left(\frac{1-z}{1+z}\right)=\frac{1}{4}(1+z)^3 w_C\left(\frac{1-z}{1+z}\right)$$

$$=\frac{1}{4}\left[(1+z)^3.1+3\left(\frac{1-z}{1+z}\right)^2\right]$$

$$=\frac{1}{4}\left[(1+z)^3.1+(1+z)^3.3\,\frac{(1-z)^2}{(1+z)^2}\right]$$

$$=\frac{1}{4}\left[(1+z)^3+(1+z)^3.3\,\frac{(1-z)^2}{(1+z)^2}\right]$$

$$=\frac{1}{4}[(1+z)^3+3(1-z)^2(1+z)]$$

$$=\frac{1}{4}[1+3z+3z^2+z^3+3-3z-3z^2+3z^3]$$

$$=\frac{1}{4}[4+4z^3]=1+z^3.$$

As already found directly from $C^\perp$. Let changing the formula by using Remark 5.7.6 to get C. We have $w_{C^\perp}(z)=1+z^3,$ and $C^\perp=\{000{,}111\},$ so $k=2.$

$$w_C(z)=\frac{1}{2^{n-k}}(1+z)^n w_{C^\perp}\left(\frac{1-z}{1+z}\right)=\frac{1}{2}(1+z)^3 w_{C^\perp}\left(\frac{1-z}{1+z}\right)^3$$

$$=\frac{1}{2}\left[(1+z)^3.1+\left(\frac{1-z}{1+z}\right)^3\right]=\frac{1}{2}\left[(1+z)^3.1+(1+z)^3.\frac{(1-z)^3}{(1+z)^3}\right]$$

$$=\frac{1}{2}\left[(1+z)^3+(1+z)^3.\frac{(1-z)^3}{(1+z)^3}\right]=\frac{1}{2}[(1+z)^3+(1-z)^3]$$

$$=\frac{1}{2}[1+3z+3z^2+z^3+1-3z+3z^2-z^3]=\frac{1}{2}[2+6z^2]$$

$$=1+3z^2$$

which is indeed $w_C(z)$.

(ii) We have $w_C(z)=1+z^2.$ In the example 5.7.2, Hence,

$$\begin{aligned} w_{C^{\perp}}(z) &= \frac{1}{2^k}(1+z)^n w_C\left(\frac{1-z}{1+z}\right) = \frac{1}{2}(1+z)^2 w_C\left(\frac{1-z}{1+z}\right)^2 \\ &= \frac{1}{2}\left[(1+z)^2.(1+\frac{(1-z)^2}{(1+z)^2})\right] \\ &= \frac{1}{2}\left[(1+z)^2.1+(1+z)^2.\frac{(1-z)^2}{(1+z)^2}\right] = \frac{1}{2}[(1+z)^2+(1-z)^2] \\ &= \frac{1}{2}[2+2z^2] = 1+z^2 \end{aligned}$$

Thus $w_{C^{\perp}}(z) = w_C(z)$, as we expect, since C is self-dual. For the very small codes just considered, the use of the MacWilliams identity is an inefficient method of determining the weight enumerators for the very small codes just considered, which can be written directly down from the lists of codewords. But suppose we are required to calculate the weight enumerate of an $[n,k]$-code C over $GF(q)$ where k is large. To enumerate all q^kcodewords by weight be a formidable task. However, if k is so large that $n-k$ is small, then the dual code $C^{\perp}$ maybe small enough to find its weight enumerate, and then the MacWilliams identity can be used to find the weight enumerate of C.

5.8. SYMMETRIZED WEIGHT ENUMERATORS

Some weight enumerators are associative with a code over $\mathbb{R}$. In this section, we deal by the symmetrized weight enumerators. The symmetrized weight enumerator (swe) of a code C over $\mathbb{R}$ is given by

$$swe_C(a,b,c) = \sum_{x\in C} a^{n_0(x)}\ b^{n_1(x)+n_3(x)} c^{n_2(x)}.$$

Where $n_i(x)$ is the number of components of $x \in C$ that are i in $\mathbb{Z}_4$, and $n_0(x), n_1(x), n_2(x)$ and $n_3(x)$ are the number of component of $x \in C$ that are $0, 1, u,$ and $1+u$, respectively, in $F_2 + uF_2$. For codes over $F_2 + vF_2$ we defined the symmetrized weight enumerator (swe) by

$$swe_C(a,b,c) = \sum_{x\in C} a^{n_0(x)}\ b^{n_1(x)} c^{n_2(x)}.$$

Where $n_i(x)$ is the number of components of x whose Lee weight is i. For codes over $F_2 + vF_2$ the MacWilliams relations to the swe are the same for both inner products [9]. Wood [21] established the MacWilliams identities for codes over any finite Frobenius ring. Klemm [13] established the MacWilliams identities for a code over $\mathbb{Z}_4$.

Example 5.8.1. (i) Let 0120111, 1130133 be codewords of length 7 over $\mathbb{Z}_4$.

For the codeword x_1 =0120111, we have $n_0(x_1)$=2, $n_1(x_1)$=4, $n_2(x_1)$=1, $n_3(x_1)$=0.

For the codeword $x_2 =$ 1130133, we have $n_0(x_2)$=1, $n_1(x_2)$=3, $n_2(x_2)$=0, $n_3(x_2)$=3.

$$swe_C(a,b,c)\sum_{x\in C} a^{n_0(x)}\ b^{n_1(x)+n_3(x)}c^{n_2(x)}$$

$$= a^{n_0(x_1)}\ b^{n_1(x_1)+n_3(x_1)}c^{n_2(x_1)} + a^{n_0(x_2)}\ b^{n_1(x_2)+n_3(x_2)}c^{n_2(x_2)}$$

$$= a^2\ b^{4+0}c^1 + a^1\ b^{3+3}c^0 = a^2\ b^4c^1 + a^1\ b^6$$

(ii) Let $01u0(1+u), (1+u)11uu$ be codewords of length 5 over $F_2 + uF_2$. For the codeword $x_1 = 01u0(1+u)$, we have $n_0(x_1)$=2, $n_1(x_1)$=1, $n_u(x_1)$=1, $n_{1+u}(x_1)$=1.

For the codeword $x_2 = (1+u)11uu$, we have $n_0(x_2)$=0, $n_1(x_2)$=2, $n_u(x_2)$=2, $n_{1+u}(x_2)$=1.

$$swe_C(a,b,c)\sum_{x\in C} a^{n_0(x)}\ b^{n_1(x)+n_3(x)}c^{n_2(x)}$$

$$= a^{n_0(x_1)}\ b^{n_1(x_1)+n_{1+u}(x_1)}c^{n_u(x_1)} + a^{n_0(x_2)}\ b^{n_1(x_2)+n_{1+u}(x_2)}c^{n_u(x_2)}$$

$$= a^2\ b^{1+1}c^1 + a^0\ b^{2+1}c^2 = a^2\ b^2c^1 + b^3c^2$$

(iii) Let $(1+v)001vvv, 011v0(1+v)(1+v)$ be codewords of length 7 over $F_2 + vF_2$, we have $w_L(0) = 0, w_L(1) = 2, w_L(v) = 1, w_L(1+v) = 1$.

For the codeword $x_1 = (1+v)001vvv$, we have $n_0(x_1)$=2, $n_1(x_1)$=4, $n_2(x_1)$=1.

For the codeword $x_2 = 011v0(1+v)(1+v)$, we have $n_0(x_2)$=2, $n_1(x_2)$=3, $n_2(x_2)$=2,

$$swe_C(a,b,c) = \sum_{x \in C} a^{n_0(x)}\ b^{n_1(x)} c^{n_2(x)}$$
$$= a^{n_0(x_1)}\ b^{n_1(x_1)} c^{n_2(x_1)} + a^{n_0(x_2)}\ b^{n_1(x_2)} c^{n_2(x_2)} = a^2\ b^4 c^1 + a^2\ b^3 c^2$$

Theorem 5.8.2. Klemm [13], Wood [21]: For a code C over a commutative ring of order 4 we have,

$$swe_{C^\perp}(a,b,c) = \frac{1}{|C|} swe_C(a+2b+c, a-c, a-2b+c)$$

Definition 5.8.3. K_n is a Klemm codes of length $n = 4m$ are constructed with a bilevel construction in this repetition code R_n and its dual the parity-check code P_n, $K_n := R_n + 2P_n \cup (1 + 2P_n)$, where 1 is the every-one's vector. Their symmetrized weight enumerators are

$$swe_{K_n}(a,b,c) = \frac{1}{2}((a+c)^n + (a-c)^n) + 2^{n-1}b^n$$

Theorem 5.8.4. Let C be a linear code over $\mathbb{Z}_4$. Then $C^\perp$, $L_{C^\perp}(x,y) = \frac{1}{|C|} L_C(x+y, x-y)$. In other side, the Lee weight enumerator to linear codes over $\mathbb{Z}_4$ follows the several MacWilliams relations such as a binary linear code even though it is image cannot be a linear code. The same MacWilliams relations will hold to codes over $F_2 + uF_2$.

Proof. For more information one can see the Theorem 4.1 in [7].

5.9. GENERATORS

In this section we are talking about generator matrices for the codes over $\mathbb{Z}_4, F_2 + uF_2$ and $F_2 + vF_2$, respectively. With using residue code and the torsion in the generators.

5.9.1. Generator Matrix for the Code Over $\mathbb{Z}_4$

Every code over $\mathbb{Z}_4$ is permutation-equivalent for a code C with generator matrix of the form

$$\begin{pmatrix} I_{k_1} & A & B_1 + 2B_2 \\ 0 & 2I_{k_2} & 2D \end{pmatrix} \qquad (1)$$

where A, B_1, B_2 and D are $(1,0)$-matrices and I_{k_i} are identity matrices for $i = 1, 2$. We said that a code with generator matrix form (1) have type $4^{k_1}2^{k_2}$ [15]. The binary $[n, k_1]$-code $C^{(1)}$ with generator matrix

$$G_1 = (I_{k_1} \quad A \quad B_1) \qquad (2)$$

is said to be the residue code of $\mathbb{Z}_4$-code. The binary $[n, k_1 + k_2]$-code $C^{(2)}$ with generator matrix

$$G_2 = \begin{pmatrix} I_{k_1} & A & B_1 \\ 0 & 2I_{k_2} & D \end{pmatrix} \qquad (3)$$

is said to be torsion code of the $\mathbb{Z}_4$-code.

5.9.2. Generator Matrix for the Code Over $F_2 + uF_2$ With $u^2 = 0$

Any code over $F_2 + uF_2$, with $u^2 = 0$, is permutation-equivalent for a code C with generator matrix

$$G = \begin{pmatrix} I_{k_1} & A & B_1 + uB_2 \\ 0 & uI_{k_2} & uD \end{pmatrix} \qquad (1)$$

where A, B_1, B_2 and D are matrices over F_2 and I_{k_i} are identity matrices for $i = 1, 2$. We associate two binary codes: the residue code $C^{(1)}$ and the torsion code $C^{(2)}$ as follows:

$$C^{(1)} = \{x \in F_2^n |\, y \in F_2^n |\, x + uy \in C\} \text{ and } C^{(2)} = \{x \in F_2^n |\, ux \in C\}.$$

A generator matrix of $C^{(1)}$ is:

$$G_1 = (I_{k_1} \quad A \quad B_1) \qquad (2)$$

And generator matrix of $C^{(2)}$ is:

$$G_2 = \begin{pmatrix} I_{k_1} & A & B_1 \\ 0 & I_{k_2} & D \end{pmatrix} \qquad (3)$$

We have $|C| = \left|C^{(1)}\right|.\left|C^{(2)}\right| = 2^{k_1}2^{k_1+k_2} = 2^{2k_1+k_2}$.

5.9.3. Generator Matrix for the Code Over $F_2 + vF_2$ With $v^2 = 1$

If A and B are codes, we denote that $A \otimes B = \{(a,b)|a \in A, b \in B\}$, and $A \oplus B = \{(a+b)|a \in A, b \in B\}$. Let C be a linear code of length n over $\mathbb{R}$. Define $C^{(1)} = \{x \in F_2^n|\, x + vy \in C, \text{for some } y \in F_2^n\}$, and $C^{(2)} = \{x + y \in F_2^n|\, x + vy \in C\}$. Obviously, $C^{(1)}$ and $C^{(2)}$ are binary linear codes.

Theorem 5.9.3.1. Assume that C is a linear code of length n over $\mathbb{R}$**.** $\varphi(C) = C^{(1)} \otimes C^{(2)}$, and $|C| = \left|C^{(1)}\right|.\left|C^{(2)}\right|$. Moreover, $\varphi(C)$ is linear.

Proof. For more details see the Theorem 3.1 in [23].

Corollary 5.9.3.2. If G_1 and G_2 are the generator matrices of binary linear codes $C^{(1)}$ and $C^{(2)}$, especially, the generator matrix of C is

$$\begin{pmatrix} (1+v)G_1 \\ vG_2 \end{pmatrix} \qquad (1)$$

furthermore, if $G_1 = G_2$ then $G = G_1$.

Proof. For more information see Corollary (3.2) in [23].

Corollary 5.9.3.3. If $\varphi(C) = C^{(1)} \otimes C^{(2)}$, then C can be uniquely expressed as

$$C = (1+v)C^{(2)} \oplus vC^{(1)}$$

A non-zero linear code C over $\mathbb{R}$ has a generator matrix which after a suitable permutation of the coordinates may be written in the form

$$G = \begin{pmatrix} I_{k_1} & A & B & D_1 + vD_2 \\ 0 & vI_{k_2} & 0 & vC_1 \\ 0 & 0 & (1+v)I_{k_3} & (1+v)E \end{pmatrix} \qquad (2)$$

where A, B, C_1, D_1, D_2 and E are $(1,0)$-matrices and I_{k_i} are identity matrices for $i = 1, 2$ 3, and $|C| = 4^{k_1}2^{k_2}2^{k_3}$. Hence, the generator matrix of $\varphi(C) = C^{(1)} \otimes C^{(2)}$ is

$$\begin{pmatrix} G_1 & 0 \\ 0 & G_2 \end{pmatrix} \qquad (3)$$

where,

$$G_1 = \begin{pmatrix} I_{k_1} & A & B & D_1 \\ 0 & 0 & I_{k_3} & E \end{pmatrix} \qquad (4)$$

$$G_2 = \begin{pmatrix} I_{k_1} & A & B & D_1 + D_2 \\ 0 & I_{k_2} & 0 & C_1 \end{pmatrix} \qquad (5)$$

are the generator matrices of binary linear codes $C^{(1)}$ and $C^{(2)}$. Furthermore, $\left|C^{(1)}\right| = 2^{k_1}2^{k_3}$ and $\left|C^{(2)}\right| = 2^{k_1}2^{k_2}$.

PART 6

SUMMARY

In this thesis, our main subject is to study on coding theory. Especial, we consider linear codes over the commutative rings of order four such as the rings of $\mathbb{Z}_4, F_2 + uF_2,$ with $u^2 = 0,$ $F_2 + vF_2$ with $v^2 = v,$ and $F_2 + wF_2$ with $w^2 = w + 1.$ We used Gray maps with knowledge of Chinese Remainder Theory to easily identify linear codes over the rings. By the Gray maps, $\varphi_{\mathbb{Z}_4},$ φ_u and $\varphi,$ it is shown that isometries and a distance preserving properties between $(\mathbb{R}, \text{Lee distance})$ and (F_2^2, Hamming distance). However, it is explained that the Gray map of $\varphi_{\mathbb{Z}_4}$ is a non-linear map, as we prove it the Gray image of $\mathbb{Z}_4$ linear code cannot be a binary linear code. Also, the Gray image of linear codes over $\mathbb{Z}_4$ are distance-invariant binary codes, even if they are non-linear. Gray map for the ring $F_2 + uF_2,$ with $u^2 = 0$ is $\varphi_u(a + ub) = (\,b, a + b)$ since only have a maximal ideal is $\langle u \rangle$, so $\mathbb{R}$ is a local ring. φ_u is a F_2-linear map. Gray map for the ring $F_2 + vF_2$ with $v^2 = v$ is $\varphi(a + vb) \to (a + b, a)$, since maximal ideals of $\mathbb{R}$ are $\langle v \rangle$ and $\langle 1 + v \rangle$ So $\mathbb{R}$ is a semi-local ring. φ is a linear map. These Gray maps are extended to $\mathbb{R}$. To further develop the subject, we also talked about some rings with order 9 such that $F_3 + vF_3,$ with $v^2 = v,$ $F_3 + vF_3$ with $v^2 = 1$, and defined their Gray maps and both rings are linear map and a distance preserving properties between $(\mathbb{R}, \text{Lee distance})$ and (F_2^2, Hamming distance). In the following of the study, we observed that there are different weights over these rings namely, Lee weight, Hamming weight, Bachoc weight and the Euclidean weight. By the examples of these weights, we ensure our theories. Moreover, we considered inner products which are basically representing a relationship between two vectors. The highly used inner products are known as Euclidean inner product and Hermitian inner products for the ring of order four.

We continue our study with some basic notions about the weight enumerators and it is relationship with Macwilliam identities for the binary linear codes and for general linear codes. Using MacWilliams identity is an inefficient method of determining the weight enumerators for the very small codes just considered, which can be written directly down from the lists of codewords and the MacWilliams identity can be used to find the weight enumerate of C and relationship with the rings of order four.

Furthermore, generators for the rings are very important and widely studied in linear coding theory [7-9]. Thus, we introduced generator matrices for the codes over $\mathbb{Z}_4$, $F_2 + uF_2$ with $u^2 = 0$ and $F_2 + uF_2$ with $v^2 = v$, respectively.

REFRENCES

1. Artin, M., “Algebra”, ***Prentice-Hall***, (1991).

2. Blake, I.F., “Codes over certain rings”, ***Information and Control,*** 20: 396–404 (1972).

3. Blake, I.F., “Codes over integer residue rings”, ***Information and Control,*** 29(4): 295–300 (1975).

4. [16] Chapman, R., Dougherty, S.T., Gaborit, P., and Sole, P., “2-Modular Lattices From Ternary Codes”, ***Journal de Théorie des Nombres de Bordeaux***, 14(1):73–85 (2002).

5. Conway, J.H., and Sloane, N.J.A., “Self-dual codes over the integers modulo 4”, ***Journal of Combinatorial Theory,*** 62, 30-45 (1993).

6. Dougherty, S.T., and Liu, H., “Independence of vectors in codes over rings”, ***Designs, Codes and Cryptography***, 51:55-68 (2009).

7. Dougherty, S.T., “Algebraic Coding Theory over Finite Commutative Rings”, ***Springer International Publishing,*** Scraton, PA, USA, (2017).

8. Dougherty, S.T., Kim, J.L., Kulosman, H., and Liu, H., “Self-Dual Codes Over Commutative Frobenius Rings,” ***Finite Fields and Their Application,*** 16(1):14-26 (2010).

9. Dougherty, S.T., Gaborit, P., Harada, M., Munemasa, A., and Sole, P., “Type IV Self-Dual Codes over Rings”, ***in IEEE Transactions on Information Theory***, 45 (7): 2345–2360 (1999).

10. Dougherty, S.T., Gaborit, P., Harada, M., and Sole, P., “Type II Codes over $F_2 + uF_2$”, ***in Transactions on Information Theory***, 45(1):32-45 (1999).

11. Hill, R., “A First Course in Coding Theory”, ***Oxford university press***, US, (1986).

12. Huffman, W.C., and Pless, V., “Fundamentals of Error Correcting Codes”, ***Cambridge University Press,*** New York, US (2010).

13. Klemm, M., “Selbstduale Codes uber dem Ring der ganzen Zahlen modulo 4”, ***Archiv der Mathematik,*** 53:201-207 (1989).

14. Ling, S., and Xing, C., “Coding Theory A First Course”, ***Cambridge University Press,*** New York, US (2004).

15. Nebe, G., Rains, E. M., and Sloane, N. J.A., “Self-Dual Codes and Invariant Theory”, ***Springer,*** Berlin, volume 17 (2006).

16. Priestley, H. A., “Introduction to Groups, Rings and Fields”, H.T and T.T, *https://people.maths.ox.ac.uk/flynn/genus2/sheets0405/grfnotes1011.pdf,* (2011).

17. Rudolf, S., 60 years, “A Mathematical Theory of Communication”, Towards “a Fuzzy Information Theory”, ***In IFSA/EUSFLAT Conf***, 1332–1337 (2009).

18. Shannon, C.E., “A Mathematical Theory of Communication”, ***The Bell System Technical Journal,*** 27(3): 279-423 (1948).

19. Shi, M., Alahmadi, A., and Sole, P., “Codes and Rings: theory and practice”, first edition , ***Academic Press,*** London, UK (2017).

20. Sloane, N. J. A., “Self-dual codes and lattices”, in Proc. Symp. Pure Mathematics, American. Mathematical. Society, vol.34:273-308 (1979).

21. Wood, J.A., “Duality for Modules Over Finite Rings and Applications to Coding Theory,” ***American Journal of Mathematics***, 555-575 (1999).

22. Yasemin, C., Dertli, A., and Dougherty, S.T., “Codes over an infinite family of rings with a Gray map”, ***Journal Designs, codes and cryptography,*** Springer, US, 72(3): 559-580 (2014).

23. Zhu, S., Wang, Y., and Shi, S., “Some Results on Cyclic codes over $F_2 + vF_2$”, ***in IEEE Transactions on Information Theory***, 56(4):1680-1684 (2010).

24. MacWilliams, F.J., and Sloane N.J.A., “The Theory of Error-Correcting Codes”, volume 16, ***North Holland***, New York, US (1977).

25. Assmus, E. F., and Key, J. D., “Designs and codes: an update” ***Springer, Boston, MA*** (1996).

RESUME

Midya Jasim Ismael HESEEN was born in Duhok in 1996 and she was graduated first, elementary and high school education in this city. Then she started study at the Duhok University- College of Basic education-Department of Mathematics. He wrote a B.Sc. thesis entitled Some Theorems in the Existence and Uniqueness Solution of Integro Differential Equation which was part of the requirements to obtain a B.Sc. in Mathematics in 2017. she has taught mathematics as a teacher in Duhok first and high school for two years. Midya speaks four languages, including Kurdish, Arabic, Turkish, and English. In 2019, he started his post-graduate studies at Karabük University in Turkey.