ON LINEAR CODES OVER $F_2 \times F_2$

August 13, 2007

THE ISLAMIC UNIVERSITY OF GAZA
DEANERY OF HIGHER STUDIES
FACULTY OF SCIENCE
DEPARTMENT OF MATHEMATICS

ON LINEAR CODES OVER $F_2 \times F_2$

PRESENTED BY
IBTISAM MOHAMMED ISLEEM

SUPERVISED BY
Dr. MOHAMMED MAHMOUD AL-ASHKER

A THESIS SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENT
FOR THE DEGREE OF MASTER OF MATHEMATICS

1428-2007

To spirit of my parents...

To my sons Mohammed Tareq, Khaled and Ali ...

To my dear niece Manar Mohamed Abou-Rass...

And to all knowledge seekers...

Contents

Acknowledgments

Praise be to Almighty ALLAH who always help and guide me to bring forth to light this work. I am also grateful to my assistant professor Mohammed M. Al-Ashker for suggesting the topic of the thesis, tremendous support and healthy ideas. It has been a privilege to work with. My sincere thanks to Dr. Ahmed El-Mabhouh and Dr. Fayeq El-Naook for their critical comments enlightening discussion and all constructive suggestions. My special thanks to all members of the Math department at the Islamic University of Gaza for their help and teaching. I would like to thank prof. Dr. Masaaki Harada for providing me with copies of his papers from Yamagata University. This also a unique occasion for expressing the blessings of my dear niece Manar Mohamed Abou-Rass, who has shared time to cooperate with and help me. Also thanks to my sons (specially khaled Ibrahem Abou -Elshiekh) and family members ,who have always shadowed me with love and fortitude.

Abstract

A code of length n and size M consist of a set of M vectors of n components. The components being taken from some alphabet set S. So a code C is a set of n-tuples subset of S^n. If S has a ring structure then C is called a linear code over S if it is an S-module. To every linear code C there corresponds its dual $C^\perp$, if $C \subset C^\perp$, then C is called self-orthogonal . If $C = C^\perp$ then C is called self-dual. In this thesis we will study linear and self-dual codes over the rings of four alphabets and in more details over the ring $F_2 \times F_2$, this ring is isomorphic to the ring $F_2 + vF_2$ where $v^2 = v$ and $F_2 = \{0, 1\}$. We would also study linear and self-dual codes for other rings in the form $F_p + vF_p$ for different primes p.Also we will construct simplex code over the ring $F_2 + vF_2 \simeq F_2 \times F_2$.

Introduction

Coding theory originated with the 1948 publicated of Landmark paper “A mathematical theory of communication” by Claud Shannon. For the past half century, coding theory has grown into a discipline interesting mathematics and engineering with applications to almost every area of communication such as satellite and cellular telephone transmission, compact disc recording ,and data storage. Coding theory is the study of methods for efficient and accurate transfer of information from one place to another. The fundamental problem in coding theory is to determine what message are sent on the basis of what received. Coding theory deals with the problem of detecting and correcting transmission errors caused by noise in the channel. The following diagram shows the system communication system for transmitting information from a source to a destination through a channel.

$$\boxed{\text{Message source}} \rightarrow \boxed{\text{Encoder}} \rightarrow \boxed{\text{Channel}} \rightarrow \boxed{\text{Decoder}} \rightarrow \boxed{\text{Receiver}}$$

$$\uparrow$$

$$\boxed{\text{noise}}$$

The most important part of the diagram, as far as we are concerned is the noise, for without it there would be no need for the theory. The communication can be either in the space domain (i.e from one location to the other)or in the time domain (i.e by storing data at one point in time and retrieving it some time later).

Let q be a positive integer and let F_q be a set of q-alphabets.

A code C of length n and size M is a subset of F_q^n having M elements. The elements of C are called codewords. In order to be able to correct errors we associate some algebraic structure with F_q. If q is a prime power one usually takes $F_q = GF(q)$, otherwise $F_q = Z_q$. Let $F_q = GF(q)(Z_q)$. A linear code of length n over $GF(q)(Z_q)$ is a subspace (submodule) of F_q^n.

A linear code C can be specified by a generator matrix G over a set F_q such that C is the row space of G.

To every linear code C there corresponds its dual code $C^{\perp}$, if $C \subseteq C^{\perp}$ then C is called self-orthogonal, If $C = C^{\perp}$ then C is called -self-dual.

Linear and self dual codes over the rings Z_4, $F_2 + uF_2$, and over $R = F_2 + vF_2$ with $v^2 = v$ and their classification are studied by different authors for more details see [10], [13], [23] and [24].

In [6]Rain and Sloane gave examples of self-dual codes and their weight enumerators. They studied some families of self-dual codes in [9] it was shown that extremal (Hermitian) self-dual codes over $F_2 \times F_2$ exist only for lengths 1, 2, 3, 4, 5, 8 and 10. In particular it was shown that there is a unique extremal self-dual code up to equivalence for lengths 8 and 10 in [10] Koichi Betsumiya studied optimal self-dual codes and Type IV self-dual codes over the ring $F_2 \times F_2$ of order 4, he gave improved upper bounds on minimum Hamming and Lee weights for such codes, he also constructed optimal self-dual codes and Type IV self-dual codes.

Also there are various binary linear codes studied so far by several researchers. Some important class of binary codes are Hamming code and its dual which is called simplex code.Any nonzero codeword of the simplex code has many of the properties that we would expect from a sequence obtained by tossing a fair coin $2^m - 1$ times.

This randomness makes these codewords very useful in a number of applications such as range-finding, synchronizing, modulation and scrambling etc.

In [11] Gupta constructed simplex code of type α and β over Z_4 *and* Z_{2^s} some fundamental properties like 2-dimension, Hamming, Lee and Generalized Lee weight distribution , weight hierarchy etc. are determined for these codes . In [13] Al-Ashker obtained simplex code over the ring $F_2 + uF_2$ by generalization of simplex codes over the ring Z_4.

Also in [14] Al-Ashker constructed the generalized Gray map between the ring $F_2 + uF_2 + u^2F_2$ and F_2^n and introduced simplex linear codes over $\sum_{n=0}^{s} u^n F_2$ of types α and β where $u^{s+1} = 0$ and determined their properties

In this thesis, we will study linear and self-dual codes over the ring $F_2 \times F_2$ where this ring is isomorphic to the ring $F_2 + vF_2$ such that $v^2 = v$ and $F_2 = \{0, 1\}$.

We would also study linear and self-dual codes for other rings in the form $F_p + vF_p$ for different primes p and we will construct simplex codes over the ring $F_2 + vF_2$.

Finally we study Bachoc, Hamming and Lee weight of simplex codes. This thesis is organized into four chapters.

In chapter one, we give basic definitions and elementary results that we need throughout this thesis. In chapter two, we give the basic definitions of self orthogonal and self dual codes over some rings, this chapter covers the main last studies about self-dual code and their types. Chapter three, is devoted for the study of self-dual codes over the ring F_2+vF_2, Also we will generalize some results over the rings F_p+vF_p isomorphic to $F_p\times F_p$ where p is prime integer. In chapter four, first we define simplex codes over binary fields and over some commutative rings, also we construct simplex codes of types α and β (denoted by S_k^{α} and S_k^{β} resp.) over the commutative ring F_2+vF_2, and we extend our results by studying the Hamming weight (wt_H), the Lee weight (wt_L) and Bachoc weight (wt_B) for these codes.

Chapter 1

Preliminaries

This chapter is divided into four sections. In section one, we set some fundamental terminology and definitions which will be applied throughout the thesis. In section two, we study generating and parity check matrices.In section three , we look more closely at the most important types of codes, and study some properties which they posses with some examples. Section four covers terminology of encoding and decoding methods . Most definitions, facts and results in this chapter can be found in [1], [4], [6], [11], [21] and [29].

1.1 General definitions on codes

In this section, we define alphabet, codes, codewords, or strings, codes over fields, Hamming weights and Hamming distances.

Definition 1.1.1. (**Strings and codes**) Let $A = \{a_1, a_2......a_q\}$ be a finite set called alphabet. A **string** or a **word** over the alphabet A is any sequence of elements of A, we will usually (but not always)write words in the form $\mathbf{a} = a_{i_1}a_{i_2}......a_{i_k}$
using juxtaposition of symbols. The empty word 0 is the unique word with no symbols. The **length** of a word **a** denoted by **len(a)** is the number of the alphabet symbols appearing in the word. The set of all words (strings) over A will denoted by A^*.

Definition 1.1.2. Let $A = \{a_1, a_2......a_q\}$ be a finite set which we call a code alphabet. An **q-ary** is a nonempty subset C of the set A^* of all words over A. The size q of the code alphabet is called the **radix** of the code and the element of the code are called **codewords**.

The field $F_2 = \{0, 1\}$ has had a very special place in history of coding theory, and codes over F_2 are called binary codes. Similarly, codes over $F_3 = \{0, 1, 2\}$ are termed ternary codes , while codes over $F_4 = \{0, 1, w, \overline{w}\}$ are called quaternary codes.The term "quaternary" has also been used to refer to codes over the ring $Z_4 = \{0, 1, 2, 3\}$ of integers modulo 4.

Definition 1.1.3. Fixed and variable length codes If all codewords in a code C have the same length we say that C is a **fixed length code**, or **block code**. If C contains codes of different lengths, we say that C is a **variable length code**. We will consider only **block** codes. We shall denote the number of codewords in a code C by $|C|$.
Let A^n be the set of all strings of length n. Any nonempty subset C of A^n is called a q-ary block code , each string in C is called codeword. If $C \subset A^n$ contains M codewords, it is customary to say that C has length n and size M, we denote this by (n, M)-code.

Example 1.1.1. *The binary code* $C = \{000, 100, 010, 001, 110, 101, 011, 111\}$ *contains* $M = |C| = 2^3 = 8$ *words.*
Fact:*For any binary code* C *of length* n, $1 \leq |C| \leq 2^n$.

For the purpose of this thesis, codes will have alphabet as a field or a ring under addition and multiplication. In fact, almost our codes' alphabet will be defined on $\mathbf{GF(q)}$, a Galois field of q-element and on commutative finite rings.

Definition 1.1.4. Hamming weight Let $\mathbf{x}$ be a q-ary word of length n. The Hamming weight is the number of nonzero components in x. We denote the Hamming weight of x by $wt_H(x)$. The minimum Hamming weight of a code C is the minimum Hamming weight of all nonzero codewords in C and is denoted by $wt_H(C)$.

Example 1.1.2. *If* $x = 110203$ *then* $wt_H(x) = 4$ *and* $wt_H(0000) = 0$.

Definition 1.1.5. Hamming distance

Let $\mathbf{x} = (x_1, x_2, ..., x_n)$ and
$\mathbf{y} = (y_1, y_2, ..., y_n) \in C$. The Hamming distance between x and y is the $d_H(x, y) =$ the number of $i^{'s}$ such that $x_i \neq y_i$.
A code C is said to have (minimum) distance d if d =minimum $\{d_H(x, y)|x, y \in C, x \neq y\}$ and it is denoted by $d(C)$.

Notation: An (n, M, d) code is a code of length n size M and minimum distance d.

Example 1.1.3. *If* $x = 20221$ *and* $y = 10220$ *then* $d_H(x, y) = 2$ *and if* $x = 1011$ *and* $y = 1011$ *then* $d_H(x, y) = 0$.

Note that for binary codes the Hamming distance between x and y is the same as the Hamming weight of z such that $z = x + y$.

$$d(x, y) = wt_H(x + y).$$

Example 1.1.4. *If* $x = 10110$ *and* $y = 01101$ *we have*
$d(x, y) = d(10110, 01101) = 4,$
$wt_H(x + y) = wt_H(10110 + 01101) = wt_H(11011) = 4.$

Proposition 1.1.1. *We now list a number of facts concerning weight and distance, Let* x, y *and* z *be words of the same length* n *and* a *be a scalar then,*

1) $0 \leq wt_H(x) \leq n.$

2) $wt_H(x) = 0 \ iff \ x = 0.$

3) $0 \leq d_H(x, y) \leq n.$

4) $d_H(x, x) = 0.$

5) *If* $d_H(x, y) = 0$ *then* $x = y.$

6) $d_H(x, y) = d_H(y, x).$

7) $wt_H(x + y) \leq wt_H(x) + wt_H(y).$

8) $d_H(x, z) \leq d_H(x, y) + d_H(y, z).$

9) $wt_H(ax) = a.wt_H(x),$ *where* $a \neq 0$ *and* $a \in F_q.$

10) $d_H(ax, az) = a.d_H(x, z),$ *where* $a \neq 0$ *and* $a \in F_q.$

Definition 1.1.6. [21] Equivalent codes Two q-ary (n, M)-codes C_1 and C_2 are **equivalent** if there exist a permutation σ of the n coordinate positions and permutations $\pi_1, \pi_2, ..., \pi_n$, of the code alphabet for which $c_1, c_2......, c_n \in C_1$ if and only if $\pi_1(c_{\sigma(1)})\pi_2(c_{\sigma(2)})......\pi_n(c_{\sigma(n)}) \in C_2$ In words, two codes are equivalent if one can be turned into the other by permutation the coordinate position of each codeword ($via \ \ \sigma$) and by permutating the code symbols in each codeword ($via \ \pi_1, ...\pi_n$). Of course σ or any π_i may be the identity permutation.

Example 1.1.5. *If* $n = 5$ *and we choose rearrange the digits in the order 2, 1, 4, 5, 3 then the code*
$C_1 = \{33333, 12013, 23110\}$ *is equivalent to the code*
$C_2 = \{33333, 21130, 32101\}$

Theorem 1.1.2. *[21] If* C_1 *and* C_2 *are equivalent codes then* $d(C_1) = d(C_2)$*.*

The following definition of equivalence is useful for special types of codes.

Definition 1.1.7. **[21] Monomial transformation** Let σ be a permutation of size n, for $i = 1, ..., n$, let $\pi_i : F_q \longrightarrow F_q$ be a multiplication by a nonzero scalar α_i in F_q that is,

$$\pi_i s = \alpha_i s$$

Then the map $\mu : F_q^n \longrightarrow F_q^n$ defined by

$$\mu(c_1, c_2, ..., c_n) = \pi_1(c_{\sigma(1)})\pi_2(c_{\sigma(2)})......\pi_n c_{\sigma(n)})$$

is called a monomial transformation of degree n.

In words a monomial transformation acting on n coordinates is a permutation of those coordinates, followed by multiplication of each coordinate by a nonzero scalar. Among all types of codes, linear codes are mostly studied because of their algebraic structure. They are easier to describe, encode, and decode than nonlinear codes. The code alphabet for linear codes is a finite field, although sometimes other algebraic structure (such as the integers modulo 4 and other commutative rings) can be used to define codes that are also called **linear** . One of the great advantages of using a finite field F_q as code alphabet is that we can perform vector space operations on the codewords. However, unless the code is a subspace of the vector space F_q^n, we cannot be certain that the sum of two codewords (or scalar multiple of a codeword) is another codeword

Definition 1.1.8. (**Linear codes**) A code C is a linear code if it is a subspace of the vector space F_q^n of dimension n over the field $GF(q)$. If C has dimension k over $GF(q)$, we say that C is an $[n, k]$-code, and if C has the minimum distance d we say C is an $[n, k, d]$-code

Note that all linear codes contain the **zero codewords**, denoted by $\mathbf{0} = 00......0$. **Note** also that the dimension of a q-ary $[n, k]$ code is defined by $k = \log_{|F|} M$ where the size $M = q^k$ and the rate of C is $R = k/n$.

Example 1.1.6. *The binary code is the code* $\{000, 011, 101, 110\}$ *over* $F_2 = \{0, 1\}$ *is a linear code where* $M = 4$. *The dimension of the code is* $\log_2 4 = 2$ *and its rate is* $2/3$

Theorem 1.1.3. *[29] If* $x, y \in F_q^n$ *then* $d(x, y) = wt(x - y)$. *If* C *is a linear code , the minimum distance* d *is the same as the minimum weight of the nonzero codewords of* C *i.e* $d(C) = wt(C)$. *For proof see [21]*

Example 1.1.7. *For the binary code* $C = \{0000, 1010, 1101, 0111\}$ *clearly* C *is linear code.* $d(1010, 1101) = 3$

$wt(1010 - 1101) = wt(0111) = 3$
$d(C) = wt(C) = 2$

Example 1.1.8. *The code* $C = \{0000, 1101, 0111, 1110\}$ *is not linear code since* $1101 + 0111 = 1010 \notin C$.
$d(1101, 0111) = 2.$
$wt(1101 - 0111) = wt(1010) = 2.$

Definition 1.1.9. The information rate or just rate Of an q-ary is a number that is designed to measure the proportion of each codeword that is carrying the message, the information rate of a code C of length n is defined to be $(1/n)\log_q |C|$. Notice that the information rate of an $[n, k, d]$ binary code is $(1/n)\log_2(2^k) = k/n$.

Example 1.1.9. *For the binary code* $C = \{000, 001, 101, 110\}$, *the information rate of* C *is 2/3 since* $|C|$*=4 and* $n = 3$ *so* $(1/3)\log_2 4 = 2/3$.

1.2 Generator and Parity Check Matrices

If C is a $k-$dimensional subspace of F_q^n then C will be called an $[n, k]$ linear code over F_q. The linear code C has q^k codewords. The two most common ways to present a linear code is a generator matrix. Since a linear code is a vector subspace we can describe it by giving a basis. It is customary to arrange the basis vectors rows of a matrix.

Definition 1.2.1. A generator matrix A generator matrix for an $[n, k]$ code C is any $k \times n$ matrix G whose rows form a basis for C. Note that a generator matrix for C must have k rows and n columns and it must have rank k. If C is an $[n, k]$-code, with generator matrix G, then the codewords in C are precisely the linear combinations of the rows of G and we can write

$$C = \{xG | x \in F_q^n\}.$$

This provides a very simple method for encoding source data.

Theorem 1.2.1. *[4] A matrix* G *is a generator matrix for some linear code* C *if and only if the rows of* G *are linearly independent; that is, if and only if the rank of* G *is equal to the number of rows of* G.

In general there are many generator matrices for a code because row equivalent matrices have the same rank and we have the following theorem.

Theorem 1.2.2. *[4] If G is a generator matrix for a linear code C, then any matrix row equivalent to G is also a generator matrix for C. In particular, any linear code has a generator matrix in **RREF**(Reduced Row Echelon Form).*

Example 1.2.1. *To find the generator matrix G for the code $C = \{0000, 1110, 0111, 1001\}$ By elementary row operations we write*

$$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix} \to \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \to \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \to \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

so $G_1 = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}$ *is a generator matrix for C, also* $G_2 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$,

is a generator matrix for C.
*Note that G_2 is in **RREF***

Definition 1.2.2. [29] Information set and redundancy set For any set of k independent columns of a generator matrix G , the corresponding set of coordinates form an information set for C. The remaining $r = n - k$ coordinates are termed a redundancy set and r is called redundancy of C.

Definition 1.2.3. [29] Standard form If the first k coordinates form an information set, the code has a unique generator matrix of the form $[I_k|A]$ where I_k is the $k \times k$ identity matrix. Such a generator matrix is in standard form. Because a linear code is a subspace of a vector space , it is the kernel of some linear transformation. In particular we have the following.

Definition 1.2.4. [29] Parity check matrix A parity check matrix for the $[n, k]$ code C, is an $(n - k) \times n$ matrix H such that

$$C = \{x \in F_q^n | Hx^T = 0\}.$$

Note that the rows of H will also be independent. In general, there are also several possible parity check matrices for C. The next theorem gives one of them when C has a generator matrix in standard form. In this theorem, A^T is the transpose of A.

Theorem 1.2.3. *[29] If $G = [I_k|A]$ is a generator matrix for the $[n, k]$code C in standard form, then $H = [-A^T|I_{n-k}]$ is a parity check matrix for C.*

Proof. we clearly have

$$HG^T = [-A^T|I_{n-k}] \begin{bmatrix} I_k \\ A^T \end{bmatrix} = -A^T + A^T = 0.$$

Thus, C is contained in the kernel of the linear transformation $x \to Hx^T$. As H has rank $n-k$, this linear transformation has kernel of dimension k, which is also the dimension of C. The result follows.

□

Notation: Since $GH^T = [I_k|A] \begin{bmatrix} -A \\ I_{n-k} \end{bmatrix}$ = -A+A $= 0$. Hence the rows of H are orthogonal to the rows of G and since $rank(H) = n-k = dim(C^{\perp})$. We deduce that H is a generator matrix for the dual code $C^{\perp}$

1.3 Important types of codes

Definition 1.3.1. [21] If $\mathbf{x} = x_1x_2, ..., x_n$ and $\mathbf{y} = y_1y_2, ..., y_n$ are binary words, we define the intersection of x and y by

$$x \cap y = (x_1y_1, x_2y_2, ...x_ny_n),$$

thus $x \cap y$ has a 1 in the ith position if and only of both x and y have 1 in the ith position.

We define the dot product x and y by :

$$x.y = x_1y_1 + x_2y_2 + ... + x_ny_n.$$

Theorem 1.3.1. *[29] The following hold*

1) *If* $x, y \in F_2^n$, *then*
$wt(x+y) = wt(x) + wt(y) - 2wt(x \cap y)$.

2) *If* $x, y \in F_2^n$, *then* $wt(x \cap y) \equiv x.y (mod 2)$.

3) *If* $x \in F_2^n$, *then* $wt(x) \equiv x.x (mod 2)$.

4) *If* $x \in F_3^n$, *then* $wt(x) \equiv x.x (mod 3)$.

5) *If* $x \in F_4^n$, *then* $wt(x) \equiv \langle x.x \rangle (mod 2)$, *where* F_4 *is the Galois field of 4 elements.*

We can now define the most important subclass of linear codes.

Definition 1.3.2. Dual code Let C be a linear $[n, k]$-code. The set

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

is called the dual code for C, where $x.c$ is the usual scalar product $x_1c_1 + x_2c_2 + ... + x_nc_n$ of the vectors x and c. **Note** that $C^{\perp}$ is an $[n, n-k]$ code.

Theorem 1.3.2. *[20] Let C be a linear code of length n over F_q. Then,*

1) $|C| = q^{\dim(C)}, i.e., \dim(C) = \log_q |C|$;

2) $C^{\perp}$ *is a linear code and* $\dim(C) + \dim(C^{\perp}) = n$;

3) $(C^{\perp})^{\perp} = C$.

Definition 1.3.3. Repetition codes The q-ary any Repetition code $Rep(n)$ of length n is

C={00......00, 11......11,......, (q-1)(q-1)......(q-1)}.

These very simple codes are q-ary linear $[n, 1, n]$-codes, with $R = 1/n$.

Example 1.3.1. *For* $C = \{0000000, 1111111\}, R = 1/7$.

Definition 1.3.4. Extended code $\hat{C}$ The process of adding one or more additional coordinate positions to the code is referred to as extending code. The most common way to extend a code is by adding an overall parity check, which is done as follows. If C is a q-ary $[n, k, d]$-code , we define the extended code $\hat{C}$ by

$$\hat{C} = \{c_1c_2, ..., c_n | c_1c_2......, c_{n+1} \in C \text{ and } \sum_{i=1}^{n+1} C_i = 0\}.$$

If $\hat{C}$ be an $[\hat{n}, \hat{k}, \hat{d}]$ binary-code, then $\hat{n} = n + 1, \hat{k} = k, \hat{d} = d$ or $d + 1$ for $[n, k, d]$ code. Directly from definition, it is easy to prove that an extended linear code is also linear. **Note** that an overall parity check is the sum of all entries mod q.

Example 1.3.2. *Let* $C = \{00, 01, 10, 11\}$ *is an* $[2, 2, 1]$*-code,*
then $\hat{C} = \{000, 011, 101, 110\}$ *is an* $[3, 2, 2]$*-code.*

Definition 1.3.5. Puncturing a code The opposite process to extending a code is puncturing a code in which one or more coordinate positions are removed from the codewords (and omitting a zero or duplicate row that may occur). If C is a q-ary $[n, M, d]$-code, and if $d \geq 2$ then the code C^* obtained by puncturing C once has parameters

$$n^* = n - 1, M^* = M, d^* = d \text{ or } d - 1.$$

For $[n,k,d]$ code C over F_q, C^* or (C^T) is $[n-1,k,d^*]$ linear code.

Note that when $d=1, C^*$ is an $[n-1,k,1]$ code if C has no codeword of weight 1 whose nonzero entry is in coordinate i.

Example 1.3.3.

a) *Let* $C=\{000,011,101,110\}$ *is* $[3,2,2]$*-code,*
then $C_3^*=\{00,01,10,11\}$ *is* $[2,2,1]$*-code,*
$C_1^*=\{00,11,01,10\}$ *is* $[2,2,1]$*-code.*

b) *Let* $C=\{00,01,10,11\}$ *is* $[2,2,1]$*-code,*
$C_1^*=C_2^*=\{0,1,0,1\}=\{0,1\}$ *is* $[1,1,1]$*-code.*

Definition 1.3.6. Shortening codes Let C be an $[n,k,d]$ code over F_q and let T be any set of t coordinates. Consider the set $C(T)$ of codewords which are 0 on T; this set is a sub-code of C. Puncturing $C(T)$ on T gives a code over F_q of length $n-t$ called the code shortened on T and denoted by C_T.

Example 1.3.4. *[29] Let* C *be* $[6,3,2]$ *binary code with generator matrix*

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

If the coordinates are labeled 1, 2,......, 6, let $T=[5,6]$. *Then*

$$G_T=\begin{bmatrix}1&0&1&0\\0&1&1&0\end{bmatrix}\ \textit{and}\ G^T=\begin{bmatrix}1&0&0&1\\0&1&0&1\\0&0&1&1\end{bmatrix}.$$

$$(G_T)^{\perp}=\begin{bmatrix}1&1&1&0\\0&0&0&1\end{bmatrix}\ \textit{and}\ (G^T)^{\perp}=\begin{bmatrix}1&1&1&1\end{bmatrix}.$$

Shortening and puncturing the dual code gives

$$(G^{\perp})_T=\begin{bmatrix}1&1&1&1\end{bmatrix}\ \textit{and}\ (G^{\perp})^T=\begin{bmatrix}1&1&1&1\\1&1&1&0\end{bmatrix}.$$

Notice that $(C^{\perp})_T=(C^T)^{\perp}$ *and* $(C^{\perp})^T=(C_T)^{\perp}$.

Definition 1.3.7. (Cyclic code) a linear code $C\subset F_q^n$ is cyclic if $c_0c_1......c_{n-1}\in C$ implies $c_{n-1}c_0c_1......c_{n-2}\in C$.

For example, the code $C = \{000, 110, 101, 011\}$ is a linear cyclic code, but the code $C = \{000, 011, 111\}$ is not cyclic, since $101 \notin C$

Definition 1.3.8. The sphere of radius Let x be a word in F^2 where $|F| = q$, and Let r be any nonzero positive real number. The sphere of radius r about x is the set $S_q(n, r) = \{y \in F^n | d(x, y) \leq r\}$.

Definition 1.3.9. Perfect code Let $C \subset F^n$ be a code. **The packing radius** of C is the largest integer r for which the sphere $S_q(c, r)$ about each codeword c are disjoint. **The covering radius** of C is the smallest integer s for which the sphere $S_q(c, s)$ about each codeword c over F^n, that is for which the union of the sphere $S_q(c, s)$ is F^n.Acode C is said to be perfect if the packing radius of C equals the **covering radius** of C.

1.4 Encoding and decoding

Encoding: We have to determine a code to use for sending our messages. We must make some choices. First, we select a positive integer k, the length of each binary word corresponding to a message. Since each message must be assigned a different binary word of length k, k must be a chosen so that $|M| \leq |q^k = 2^k|$. Next, we decide how many digits we need to add each word of length k to ensure that as many errors can be corrected or detected as we require; this is the choice of the codewords and the length of the code n. To transmit a particular message, the transmitter finds the word of length k assigned to that message then transmits the codeword of length n corresponding to that word of length k.

Decoding: The process of decoding,that is determining which codeword (massage $\mathbf{x}$) was sent when a vector $\mathbf{y}$ is received . In general, encoding is easy, and decoding is hard if the code has a reasonably large size .

Theorem 1.4.1. *[4] A code C of distance d will at least detect all non-zero error patterns of weight less than or equal to $d-1$. Moreover, there is at least one error pattern of weight d which C will not detect.*

Example 1.4.1. *The code $C = \{000, 111\}$, $d = 3$ detects all error patterns of weight 1 or 2 and C does not detect the only error patterns of weight 3.*

Theorem 1.4.2. *[4] A code C of distance d will correct all error patterns of weight less than or equal to $[(d-1)/2]$. Moreover, there is at least one error pattern of weight $1 + [(d-1)/2]$ which C will not correct.*

Example 1.4.2. *The code* $C = \{000, 111\}$, $d = 3$ *correct all error patterns of weight 0 or 1, since* $(d-1)/2 = (3-1)/2 = 1$.

Example 1.4.3. *Consider the binary code with generator matrix*

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

This code encode source symbols from F_2^3. *In particular, for each* $x = (x_1, x_2, x_3) \in F_2^3$, *we associate the codeword*

$$\begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} x_1 + x_3, x_1 + x_2, x_2 + x_3, x_2 \end{bmatrix}.$$

Let $x = (101) \Rightarrow xG = [0, 1, 1, 0]$.

Example 1.4.4. *[29] The matrix* $G = \begin{bmatrix} I_4 | A \end{bmatrix}$, *where*

$$G = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right]$$

is a generator matrix in standard form for a $[7, 4]$ *binary code that we denote by* H_3, *by theorem (1.2.3)*

$$H = \begin{bmatrix} -A^T | I_3 \end{bmatrix} = \left[\begin{array}{cccc|ccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right].$$

In binary system A^T *and* $-A^T$ *are the same.*
This code is called the $[7, 4]$*Hamming code.*

Notation: The Hamming code H_3 can encode source words from F_2^4 as follows

$$xG = [x_1 x_2 x_3 x_4] \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$= [x_1, x_2, x_3, x_4, x_2 + x_3 + x_4, x_1 + x_3 + x_4, x_1 + x_2 + x_4].$$

Since G is in standard form, the original source message appears as the first k symbols of it's codeword.
An efficient decoding process for linear codes can be obtained through the use of parity check matrices which will be of great value in designing decoding schemes.

Definition 1.4.1. Syndrome[21] and [29] The syndrome of a vector x in F_q^n with respect to the parity check matrix H is the vector in F_q^{n-k} defined by
$Syn(x) = Hx^T$(others defined syndrome as, $Syn(x) = xH^T$)
Thus $x \in C$ if and only if the syndrome of x is 0.

Example 1.4.5. *Let C be the Hamming code*

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

To decode the received vector $x = (0, 1, 1, 0, 1, 0, 0)$, we fined syndrome of x,

$$Syn(x) = Hx^T = (1, 1, 0),$$

which is the 4^{th} column of H,, then the error vector is

$$e = (0, 0, 0, 1, 0, 0, 0),$$

and

$$y = x + e = (0, 1, 1, 1, 1, 0, 0).$$

Definition 1.4.2. Coset of C. If $C \subset F_q^n$ is a linear code (i.e subspace) the quotient space of F_q^n, modulo C is defined by

$$F_q^n/C = \{x + C | x \in F_q^n\}.$$

The set $x + C = \{x + c | c \in C\}$ is called a coset of C.

Note that $|x + C| = |C|$.
Because our code C is an elementary abelian subgroup of the additive group of F_q^n, its distinct cosets $x + C$ partition F_q^n into q^{n-k} cosets of size q^k. Two vectors x and y belong to the same coset if and only if $y - x \in C$. The weight of a coset is the smallest weight of vector in the coset, and any vector of this smallest weight in the coset is called a coset leader. The zero vector is the unique coset leader of the code C. More generally, every coset weight at most $t = [(d - 1)/2]$ has unique coset leader.

Proposition 1.4.3. *[21] and [29] Two vectors belong to the same coset if and only if they have the same syndrome.*

Proof. Let $x_1, x_2 \in F_q^n$ are in the same coset of C, then $x_1 - x_2 = c \in C$. Therefore $syn(x_1) = H(x_2+c)^T = Hx_2^T + Hc^T = Hx_2^T = syn(x_2)$. Convensely if $syn(x_1) = syn(x_2)$, then $H(x_2 - x_1)^T = 0$ and so $x_2 - x_1 \in C$. $\square$

Example 1.4.6. *[21] Let C be the binary $[4, 2]$-code with generator matrix*

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

The coset of C are:

$0000 + C = \{0000, 0100, 1101, 1001\}$

$1000 + C = \{1000, 1100, 0101, 0001\}$

$0010 + C = \{0010, 0110, 1111, 1011\}$

$1010 + C = \{1010, 1110, 0111, 0011\}$.

Since the coset leaders were chosen with minimum weight, the table of coset leaders is

0000	0100	1101	1001
1000	1100	0101	0001
0010	0110	1111	1011
1010	1110	0111	0011

We write G in standard form as

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

Coset leader	*Syndrome*
0000	00
1000	01
0010	10
1010	11

To decode the received word $x = 1110$, for instance, we compute its syndrome

$$1110.H^T = 11.$$

Hence, according to the syndrome table, the coset leader is 1010 and we decode x as

$$1110 + 1010 = 0100.$$

Chapter 2

Self-dual codes over rings and fields

In this chapter, we will introduce self dual codes and some types of them. These codes are important because many of the best codes known of this type and they have rich mathematical theory. Topics covered in this chapter include codes over $F_2, F_3, F_4, Z_4, Z_m, F_2 + uF_2$ and $F_2 + vF_2$, which is isomorphic to $F_2 \times F_2$. We review the literature for self-dual codes such as weight enumerators , MacWilliams formulas, Gray maps, bounds on codes, types of self dual codes, Extremal and optimal codes. More information can be found in [2], [6], [9], [10], [11], [21], [23], [24] and [29].

2.1 Inner product

Let F be a finite set called the alphabet. A code C over F of length n is any subset of F^n. If F has the structure of an additive group then C is additive if it is an additive subgroup of F^n. If F has ring structure then C is linear over F if it is additive and also closed under multiplication by elements of F (we will always assume that, multiplication in F is commutative). In order to define dual codes, we must equip F with an inner product. The vector space F_q^n has a natural or Euclidean inner (dot or scaler) product on it.

Definition 2.1.1. Euclidean Inner product The Euclidean inner product of $x = (x_1, x_2, x_3, ..., x_n)$ and $y = (y_1, y_2, y_3, ..., y_n)$ on F_q^n defined by:

$$(x, y) = x.y = x_1y_1 + x_2y_2 + ...x_ny_n = \sum_{i=1}^{n} x_iy_i$$

we may use the notation (x, y) for $x.y$ and require that it satisfies the following conditions for all $x, y, z \in F_q^n$ and $\alpha \in F_q$

1) $(x + y, z) = (x, z) + (y, z)$.

2) $(x, y + z) = (x, y) + (x, z)$.

3) $If(x, y) = 0$ for all x then $y = 0$.

4) If (x, y)=0 for all y then $x = 0$.

5) $(\alpha x, y) = (x, \alpha y) = \alpha(x, y)$.

This means that the inner product over F_q^n is a symmetric bilinear-form.
Note: we say that x and y are orthogonal $(x \perp y)$ if $(x.y) = 0$.
When studying quaternary codes over the field F_4, it is often useful to consider another product given by the following definition.

Definition 2.1.2. Hermitian inner product The Hermitian inner product for two codeswords x and y is given by

$$\langle x, y \rangle = x.\bar{y} = \sum_{i=1}^{n} x_i \bar{y}_i,$$

where $^{-}$called conjugation, and $\bar{C} = \{\bar{c} | c \in C\}$ where $\bar{c} = \bar{c_1}\bar{c_2}......\bar{c_n}$ and $c = c_1 c_2......c_n$.

Example 2.1.1. *For* $F_4 = \{0, 1, w, \bar{w}\}$ *, conjugation is given by* $\bar{0} = 0, \bar{1} = 1$ *and* $\bar{w} = w$ *i.e* $\forall x \in F_4, \bar{x} = x^2$
The Hermitian inner product is satisfying the following:

1) $\bar{\bar{x}} = x$.

2) $\overline{x + y} = \bar{x} + \bar{y}$.

3) $\overline{xy} = \bar{x}\bar{y}$.

4) $\langle x, y \rangle = \overline{\langle y, x \rangle}$.

5) $\langle \alpha x, y \rangle = \langle x, \bar{\alpha} y \rangle$.

6) $\langle x, \alpha y \rangle = \bar{\alpha} \langle x, y \rangle$.

Analogous to $C^{\perp}$ we can define $C^{\perp H}$.

Definition 2.1.3. [29] Hermitian dual of quaternary code C is

$$C^{\perp H} = \{x \in F_q^n | \langle x, y \rangle = 0 \ , \quad for \ all \ c \in C\}.$$

Following [20], For a linear code C over $F_{q^2}^n$, its Hermitian dual is defined as:

$$C^{\perp H} = \{x \in F_{q^2}^n | \langle x, y \rangle = 0 \ , \quad for \ all \ c \in C\}.$$

Remark 2.1.1. If C is a code over F_4, then $C^{\perp H} = \bar{C}^{\perp}$.

Proof.

$$C^{\perp H} = \{x \in F_4^n | \langle x, c\rangle = x.\bar{c} = 0, \ \forall c \in C\}$$

$$\bar{C}^{\perp} = \{x \in F_4^n | x.\bar{c} = 0, \ \forall \ \bar{c} \in \bar{C}\}$$

$$= \{x \in F_4^n = \langle x.c\rangle = 0, \ \forall \ c \in C\}.$$

And so the result achieved. □

Definition 2.1.4. Self orthogonal and self-dual codes A code C is self-orthogonal provided that $C \subseteq C^{\perp}$ and self-dual provided $C = C^{\perp}$. We also have Hermitian self orthogonality if $C \subseteq C^{\perp H}$, and Hermitian self-dual if $C = C^{\perp H}$.

Note: The self-dual binary code has even length n and dimension $n/2$.

In [6] Rains and Sloane considered the following :-

(2) Binary Linear codes : $F = F_2 = \{0, 1\}$, with inner product $(x, y) = xy, C =$ subspace of F_2^n.

(3) Ternary linear codes:F : $F_3 = \{0, 1, 2\}, (x, y) = xy, C =$ subspace of F_3^n.

(4^H) Quaternary linear codes:$F = F_4 = \{0, 1, w, w^2\}$where $w^2+w+1 = 0, w^3 = 1, \bar{x} = x^2$ for $x \in F_4$ with the Hermitian inner product $\langle x, y\rangle = x\bar{y}, C =$ subspace of F_4^n. **Note** that for $x, y \in F_4, (x + y)^2 = x^2 + y^2$.

(4^E) Quaternary linear codes :$F = F_4$,but with the Euclidean inner product $(x, y) = xy$.

(4^Z) Z_4 Linear codes :$F = Z_4 = \{0, 1, 2, 3\}$ with $(x, y) = xy(mod 4), C =$ linear subspace of Z_4^n or strictly speaking, a Z_4-submodule.

(m^Z) $F = Z_m = Z/mZ$,where m is an integer ≥ 2 with $(x, y) = xy(mod\ m)$, C is a Z_m-submodule.

Example 2.1.2. *The hexa code has generator matrix G_6 in standard form is Hermitian F_4- self-dual*

$$G_6 = \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & w & w \\ 0 & 1 & 0 & w & 1 & w \\ 0 & 0 & 1 & w & w & 1 \end{array}\right].$$

Theorem 2.1.1. *[21] Let G be a generator matrix for a q-ary linear code C, then C is self orthogonal if and only if distinct rows of G orthogonal and have weight divisible by q.*

Theorem 2.1.2. *[29] If every codeword of a binary code C has weight divisible by 4 then C is self-orthogonal.*

Proof. let x and y be rows of the generator matrix

$$\begin{aligned} wt(x+y) &= wt(x) + wt(y) - 2wt(x \wedge y) \\ &= 0 + 0 - 2wt(x \wedge y) \end{aligned}$$

but $x, y \in F_2^n$ then $wt(x \wedge y) = x \cdot y(mod2)$ which implies that $2(x \cdot y) \equiv 2wt(x \wedge y) \equiv 2wt(x \wedge y) - wt(x) - wt(y) \equiv -wt(x+y) \equiv 0(mod4)$. Thus $x \cdot y \equiv 0(mod2)$ and so C is self orthogonal. □

Example 2.1.3. *[29] According to previous theorem the binary $[7,3]$ code C with generator matrix,*

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

is self orthogonal and all codeword weights are divisible by 4. The dual code $C^{\perp}$ of the code has generator matrix,

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

by adding an overall parity check to this code , we obtain $\hat{C}$ with generator matrix

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

This code is self orthogonal $[8,4]$-code , and so it is self-dual.
Notice that, if a code C is self-dual then any generating matrix G is also a parity check matrix H.

Theorem 2.1.3. *[21] A q-ary self-dual $[n, n/2]$-code exists if and only if one of the following holds :*

1) *q and n are both even.*

2) *$q \equiv 1(mod4)$ and n is even.*

3) $q \equiv 3(mod4)$*and* n *is divisible by 4.*

In particular, we note that a binary self-dual $[n, n/2]$ -code exist for all positive even integers n , and a ternary self-dual $[n, n/2]$-code exist if and only if n is divisible by 4.

Definition 2.1.5. [29] doubly or singly-even code A binary self-dual code C has the property that all codeword weights are even. If, in addition, all codeword weights in C are divisible by 4, then C is said to be an even (or doubly-even) code. One which is not doubly-even is called singly-even.

Theorem 2.1.4. *[21] An even* $[n, n/2]$*-code exists if and only if* n *is divisible by 8.*

$\hat{G}$ in Example (2.1.3) is example of even code.

Definition 2.1.6. [29] Even like or odd like code a vector $x = x_1, x_2, x_3, ..., x_n$ in F_q^n is even-like provided that $\sum_{i=1}^{n} x_i = 0$ and is odd-like otherwise. We say that a code is even-like if it has only even-like codewords; a code is odd-like if it is not even-like. The even-like vectors in a code form a subcode over F_q.
The vector (1, 1, 1) in F_3^3 and $(1, w, \overline{w})$ in F_4^3 are examples.

2.2 Weight enumerators

There are several weight enumerators associated with a code C , they are given in the following definitions, for more details see [6], [11] and[29]. We defined the Hamming weight of a vector $x = (x_1, x_2, ..., x_n) \in F^n$ by the number of nonzero component x_i. Two other types of "weight" are useful for studying non binary codes. For the codes in families $(4^Z), (m^Z)$ and hence , for (2), (3), and if q is a prime for (q^E) . We define the Lee weight and Euclidean norm of $x \in F$ by

$$Lee(x) = min\{|x|, |F| - |x|\}.$$

$$Eculidean(x) = (Lee(x))^2.$$

for a vector $x = (x_1, x_2, ...x_n) \in F^n$, we set

$$Lee(x) = \sum_{i=1}^{n} Lee(x_i).$$

$$Eculidean(x) = \sum_{i=1}^{n} Eculidean(x_i).$$

of course , if x is a binary vector, $wt_H(x) = wt_L(x) = wt_E(x)$.

Definition 2.2.1. Weight distribution For each $1 \leq i \leq n$, let $A_H(i), A_L(i), ...,$ $and A_E(i)$ be the number of codewords of Hamming, Lee,......, and Euclidean i in the code C.

Definition 2.2.2. The Hamming weight enumerator The Hamming weight enumerator (Hwe) of C is a polynomial defined by

$$\begin{aligned} W_c(x,y) or Ham(x,y) &= \sum_{c \in C} (x)^{n-w_H(c)} y^{w_H(c)} \\ &= \sum_{i=0}^{n} A_i(C) x^{n-i} y^i. \end{aligned}$$

(The adjective Hamming is often omitted). There is analogous definition for nonlinear or nonadditive code.

Much more information about a code C is supplied by the following weight enumerators.

Definition 2.2.3. [6] Complete weight enumerator Let the elements of the alphabet F be $\xi_1, \xi_2, ..., \xi_a$ and introduce corresponding indeterminates $x_0, x_1, ..., x_a$. Then

$$cwe(x_0, x_1, ..., x_a) = \sum_{u \in c} x_0^{n_0(u)} x_1^{n_1(u)} ...... x_a^{n_a(u)},$$

where $n_i(u)$ is the number of components of u that takes the value ξ_i. If there is a natural way to pair up some of the symbol in F , we can often reduce the number of variables in the cwe without losing any essential information, by identifying indeterminates corresponding to paired symbols. The result is a symmetrized weight enumerator (abbreviated swe).
Note that permutation equivalent codes have, the same cwe ,but in general two equivalent class of codes may have different $swe's$.
The swe contains only about half as many variables as the complete weight enumerators. Some examples make this clear. For linear codes over F_4

$$swe_C(x,y,z) = \sum_{4 \in c} x^{n_0(u)} y^{n_1(u)} z^{N_w(u)} = cwe(x,y,z,z),$$

where $N_w(u)$ is the number of components in u that are equal to either w or $\overline{w}$. For linear code over Z_4

$$swe_C(x,y,z) = \sum_{u\in C} x^{n_0(u)} y^{n_{\pm(u)}} z^{n_2(x)} = cwe_C(x,y,z,y),$$

where $n_{\pm(u)}$ is the number of components of u that are equal to either $+1$ or -1.

2.3 Examples of self-dual codes and their weight enumerators

[6] we write $[n,k,d]_q$ to indicate a linear code of length n, dimension k and minimum distance d over the field F_q omitting q when it is equal to 2.

1) $\hat{C}$ in Example 2.1.3, the [8, 4, 4] Hamming code e_8 is self dual with weight enumerator

$$W_{e_8}(x,y) = x^8 + 14x^4y^4 + y^8.$$

2) The $[4,2,3]_3$ tetra code t_4 generated by $\{1110, 0121\}$ has

$$w_{t_4}(x,y) = x^4 + 8xy^3.$$

3) (4^H) The $[2,1,2]_4$ repetition code $i_2 = \{00, 11, ww, \overline{ww}\}$ has

$$\begin{aligned} W_{i_2}(x,y) &= x^2 + 3y^{2\cdot} \\ swe &= x^2 + y^2 + 2x^2. \\ cwe &= x^2 + y^2 + z^2 + t^2. \end{aligned}$$

4) (4^H) The $[6,3,4]$ Hexacode in the form with generator matrix

$$\begin{bmatrix} 1 & 0 & 0 & 1 & w & w \\ 0 & 1 & 0 & w & 1 & w \\ 0 & 0 & 1 & w & w & 1 \end{bmatrix}.$$

$$\begin{aligned} W_{h_6}(x,y) &= x^6 + 45x^2y^4 + 18y^6. \\ swe &= x^6 + y^6 + 2z^6 + 15(2x^2y^2z^2 + x^2z^4 + y^2x^4). \\ cwe &= x^6 + y^6 + z^6 + t^6 + 15(x^2y^2z^2 + x^2y^2t^2 + x^2z^2t^2 + y^2z^2t^2). \end{aligned}$$

5) (4^E) The $[4,2,3]_4$ read soloman code

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & w & \overline{w} \end{bmatrix},$$

where $C = \{0000, 1111, 01w\overline{w}, 10\overline{w}w, wwww, w\overline{w}01, \overline{w}\ \overline{w}\ \overline{w}\ \overline{w}, \overline{w}w10,$
$0w\overline{w}1, 1\overline{w}w0, w01\overline{w}, \overline{w}10w, 0\overline{w}1w, 1w0\overline{w}, w1\overline{w}0, \overline{w}0w1\}$ has

$$\begin{aligned} w(x,y) &= x^4 + 12xy^3 + 3y^4. \\ swe &= x^4 + y^4 + 2z^4 + 12xyz^2. \\ cwe &= x^4 + y^4 + z^4 + t^4 + 12xyzt. \end{aligned}$$

6) (4^Z) the octacode O_8 with generator matrix

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

having minimal Lee weight 6 and minimal Euclidian weight 8

$$swe = x^8 + 16y^8 + z^8 + 14x^4z^4 + 112xy^4z(x^2+z^2).$$

2.4 MacWilliams Theorems

A linear code C is uniquely determined by its dual $C^\perp$. In particular, the weight distribution of C is uniquely determined by the weight distribution of $C^\perp$ and vice versa. For more details, see [29]. The simplest formulation is always in term of the weight enumerator polynomials.

Theorem 2.4.1. *[6], MacWilliams and others*

(2) *Three equivalent formulation of the result for binary self dual codes are :*

$$W_{C^\perp}(x,y) = \frac{1}{|C|} W_C(x+y, x-y). \tag{2.4.1}$$

$$\sum_{u \in C^\perp} x^{n-wt(u)} y^{wt(u)} = \frac{1}{|C|} \sum_{4 \in C} (x+y)^{n-wt(u)} (x-y)^{wt(u)}. \tag{2.4.2}$$

and, if $\{A_0^\perp, A_1^\perp, ...\}$ *is the weight distribution of* $C^\perp$,

$$A_k^\perp = \frac{1}{|C|}\sum_{i=0}^{n} A_i P_k(i). \tag{2.4.3}$$

where

$$P_K(x) = \sum_{j=0}^{k} (-1)^j \begin{pmatrix} x \\ j \end{pmatrix} \begin{pmatrix} n-x \\ k-j \end{pmatrix} \quad , k = 0, ...n$$

is a Krowtchouk polynomial.

For the remaining cases we give just the formulation terms of weight enumerator.

(3) $W_{C^\perp}(x,y) = \frac{1}{|C|}W_C(x+2y, x-y).,$
$swe(x,y,z) = \frac{1}{|C|}cwe_C(x+y+z, x+wy+\overline{w}z, x+\overline{w}y+wz).$

(4^H) *and* (4^{H+}), $W_{C^\perp}(x,y) = \frac{1}{|C|}W_C(x+3y, x-y),$
$swe_{C^\perp}(x,y,z) = \frac{1}{|C|}swe_C(x+y+2z, x+y-2z, x-y),$
$cwe_{C^\perp}(x,y,z,t) = \frac{1}{|C|}cwe_C(x+y+z+t, x+y-z-t, x-y+z-t, x-y-z+t).$

(4^E) $W_{C^\perp} = \frac{1}{|C|}W_C(x+3y, x-y),$
$swe_{C^\perp}(x,y,z) = \frac{1}{|C|}swe_C(x+y+2z, x+y-2z, x-y),$
$cwe_{C^\perp}(x,y,z,t) = \frac{1}{|C|}cwe_C(x+y+z+t, x+y-z-t, x-y-z+t, x-y+z-t).$

(q^H)

$$W_{C^\perp} = \frac{1}{|C|}W_C(x+(q-1)y, x-y). \tag{2.4.4}$$

(4^Z) $W_{C^\perp}(x,y) = \frac{1}{|C|}W_C(x+3y, x-y),$
$swe_{C^\perp}(x,y,z) = \frac{1}{|C|}swe_C(x+2y+z, x-y, x-2y+z),$
$cwe_{C^\perp}(x,y,z,t) = \frac{1}{|C|}cwe_C(x+y+z+t, x+iy-z-it, x-y+z-t, x-iy-z+it).$

(m^Z) $W_{C^\perp}(x,y) = \frac{1}{|C|}W_C(x+(m-1)y, x-y).$

Proof. see [6]. □

Example 2.4.1. *The repetition code* C *over a field* F_q *has Hamming weight enumerator*

$$W_C(x,y) = x^n + (q-1)y^n,$$

by (2.4.4) we deduce that the dual code $C^{\perp}$, the zero-sum code, has weight enumerator

$$W_{C^{\perp}}(x,y) = \frac{1}{q}\{(x+(q-1)y)^n + (q-1)(x-y)^n\}.$$

Note that when $n = 2, W_{C^{\perp}} = W_C$.

2.5 Isodual and formally self-dual

All of the definitions and facts in this section can be found in [6], [24] and [29].

Definition 2.5.1. Formally self-dual A (possibly nonlinear)code with the property that the code and its dual have identical Hamming weight enumerator.

Definition 2.5.2. Isodual self-dual A linear code which is equivalent to its dual is called isodual.An isodual code is automatically formally self-dual. The code $C = \{111100, 110011, 101010\}$ is [6, 3, 3] isodual code.

Definition 2.5.3. Divisible self -dual Formally self-dual code is divisible if there exists a positive integer $\delta > 1$ such that δ divides all nonzero weights in the code, δ is called a divisor of C.

Theorem 2.5.1. ***Gleason-pierce [6] and [24]*** *If C is a self dual code belonging to any of the families of (2) through (m^Z) which has all its Hamming weight divisible by an integer $\delta > 1$ then one or more of the following holds:*

$$\begin{array}{lllll}
1) & TypeI: & |F| = 2, & \delta = 2 & (\textit{so family2}) \\
2) & TypeII: & |F| = 2, & \delta = 4 & (\textit{so family2}) \\
3) & TypeIII: & |F| = 3, & \delta = 3 & (\textit{so family3}) \\
4) & TypeIV: & |F| = 4, & \delta = 2 & (\textit{so families } 4^4, 4^E, 4^Z) \\
5) & TypeV: & |F| = q, & q \textit{ arbitrary} & \delta = 2
\end{array}$$

, and the Hamming weight enumerator of C is

$$(x^2 + (q-1)y^2)^{n/2}.$$

Remark 2.5.1.

1) The same conclusion holds if "C" is self-dual " is replaced by "C is formally self-dual".

2) For proof and generalization of the above theorem see [29] [Theorem 9.1.1(Gleason-pierce-word)].

3) The binary self-dual codes that are not doubly even (or Type II) are called (singly even) or (Type I).

4) The above theorem can be applied to codes over finite commutative rings for which the MacWilliams relations hold, for example to codes over all finite rings of order 4.

5) Any self-dual divisible code over a ring of order 4 which is not Type V is necessarily Type IV.

6) There are many examples of codes with weight enumerator $(x^2 + (q-1)y^2)^{n/2}$ that are not self dual.

7) There are binary divisible codes that is not formally.

For the last two remarks we have the following Examples:

Example 2.5.1. *[29] The linear binary code [6, 3, 2] with generator matrix*

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

$C = [000000, 100111, 010111, 001111, 110000, 101000, 011000, 111111]$ *with*

$$W_c(x, y) = x^6 + 3x^4y^2 + 3x^2y^4 + x^6 = (x^2 + y^2)^3.$$

C *is a formally self-dual code divisible by* $\delta = 2$*, that is not self-dual.*

Example 2.5.2. ***Exercise 492 page 339*** *[29] Let* C *be the binary code with generator matrix*

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

show that C *is divisible by* $\delta = 2$ *and is not formally self-dual.*

Solution:

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

$$C = [000000, 110000, 101000, 000110, 011000, 110110, 101000, 011110],$$

$$W_c(x, y) = x^6 + 5x^4y^2 + 2x^2y^4.$$

$$C^{\perp} = [000000, 001100, 000010, 110001, 001110, 111101, 11011, 111111]$$

$$W_{c^{\perp}}(x, y) = x^6 + x^5y + x^4y^2 + 2x^3y^3 + x^2y^4 + xy^5 + y^6.$$

Clearly $W_{c^{\perp}}(x, y) \neq W_c(x, y)$ *which implies that* C *is not formally self-dual.*

2.6 Self dual code over rings of four alphabets

In this section, we turn to a general discussion of self dual codes over rings, especially of order 4. We begin with some definitions. All definitions in this section from [6], [9], [10], [24]and [29].
Let$R$ be either the ring Z_4 of integers modulo 4, $F_2 + uF_2 = \{0, 1, u, 1 + u\}$ with $u^2 = 0$ or $F_2 + vF_2 = \{0, 1, v, 1 + v\}$ with $v^2 = v$. Throughout this section, if the statement does not depend on which ring we are using , we shall denote the ring by R. A code C over a ring R of length n is a subset of R^n, if it is an additive subgroup of R^n then it is called a linear code. An R-code of length n is an R-submodule of R^n. All codes are assumed to be linear unless otherwise specified.

Definition 2.6.1. Weights and distances We consider several different weights and distances used for codes over rings. For example, the Hamming weight wt_H, the Euclidean weight wt_E, the Lee weight wt_L and the Bachoc weight wt_B. The corresponding distance are denoted by d_H, d_E, d_L and d_B. The Hamming weight of a codeword is the number of nonzero components. The Euclidean weights for the elements of Z_4 are 0, 1, 4 and 1 respectively, and for the element of $F_2 + uF_2 = \{0, 1, u, 1 + u\}$, the Euclidean weights are 0, 1, 4 and 1. The Lee weights of the elements of Z_4 are 0, 1, 2 and 1 respectively 0, 1, 2, and 1 for $F_2 + uF_2$, and 0, 2, 1 and 1 for $F_2 + vF_2 = \{0, 1, v, 1 + v\}$.

Note that:

$$wt_E(x) = \sum_{i=1}^{n} (wt_L(x_i))^2.$$

The Euclidean distance between vectors $x, y \in R^n$, $[R^n = Z_4^n$ or $R^n = (F_2 + uF_2)^n]$ is defined as

$$d_E(x, y) = \sum_{i=1}^{n} (wt_L(x_i - y_i))^2,$$

it follows that

$$d_E(x,y) = wt_E(x-y).$$

For the ring F_2+vF_2 another weight (we call it Bachoc weight) is defined in [2] and [23]. The Hamming, Euclidean , Lee and Bachoc weights of a codeword is the rational sum of the Hamming, Euclidean, Lee and Bachoc weights of a codewords is the rational sum of the Hamming, Euclidean, Lee and Bachoc weights of its components respectively. Let C be a code over R, the minimum distance of C is the smallest distance $d(x,y)$ where $x, y \in C$ and $x \neq y$. The minimum Hamming, Euclidean, Lee and Bachoc weights d_H, d_E, d_L and d_B of C are the smallest Hamming, Euclidean, Lee and Bachoc weights among all nonzero codewords of C respectively.

Definition 2.6.2. [24] Gray maps Let consider the following rings and maps :

$$\begin{array}{ccccc} F_2+uF_2 & \xrightarrow{\psi} & F_2^2 & \xleftarrow{\phi} & Z_4 \\ & & \varphi \uparrow & & \\ & & F_2+vF_2 & & \end{array}$$

ψ	ϕ	φ
$\psi(0)=00$	$\phi(0)=00$	$\varphi(0)=00$
$\psi(1)=01$	$\phi(1)=01$	$\varphi(v)=01$
$\psi(1+u)=10$	$\phi(2)=11$	$\varphi(1+v)=10$
$\psi(u)=11$	$\phi(3)=10$	$\varphi(1)=11$

The maps ψ, ϕ *and* φ are isometries from (R, Lee distance) to (F_2^2, Hamming distance), and are called Gray maps. These are extended to R^n naturally. The maps ψ and φ are linear but ϕ is not, since $(\phi(1+1) \neq \phi(1)+\phi(1))$.

Remark 2.6.1. Note that self-dual codes exist for all $n > 0$ for both codes over Z_4 and F_2+uF_2 since 2 and u generate self dual codes of length 1. Self dual codes exist only for even lengths over F_2+vF_2 for the Euclidean inner product but they exist for all lengths with the Hermition inner product since v generates a self-dual code of length 1. In this thesis, codes with respect to Euclidean (resp. Hermition) inner product are said to be Euclidian (resp. Hermition) codes.

Definition 2.6.3. Equivalent codes we say that two codes are equivalent if one can be obtained from the other by permuting the coordinates, and (if necessary) interchanging the two elements 1 and 3 (of certain coordinates for $R = Z_4$ [possibly followed by multiplying some coordinates by 3(sign changes)] and the two elements 1 and $1+u$ of certain coordinates for $R = F_2+uF_2$. Codes differing by only a permutation of coordinates are called permutation equivalent. For $R = F_2 + vF_2$, we say that C and $\grave{C}$ are permutation-equivalent or C is permutation-equivalent to the code obtained from $\grave{C}$ by changing v and $1+v$ in all coordinates. For $R = Z_4$ and $F_2 + uF_2$, the automorphism group $Aut(C)$ of C consist of all permutation and changes of the above two elements of the coordinates that preserve C.

Remark 2.6.2. If C_1 and C_2 are equivalent codes then $d(C_1) = d(C_2)$.

More details about the ring $F_2 + vF_2$ will be discussed in the next chapter. The following two subsections are a survey of self-dual codes over the rings Z_4 and $F_2 + uF_2$.

2.6.1 Codes over Z_4 (Family 4^Z)

Following [11]and [29] a Z_4-linear code C of length n is an additive subgroup of Z_4^n. Such a subgroup is a Z_4-module, which may or may not be free. We will still term elements of Z_4^n "vectors" even though Z_4^n is not a vector space.

Definition 2.6.4. Generator matrix Any code over Z_4 (Family 4^Z) is equivalent to one with the generator matrix of the standard form

$$G = \begin{bmatrix} I_{k_1} & A & B_1 + 2B_2 \\ 0 & 2I_{k_2} & 2C \end{bmatrix}, \tag{2.6.1}$$

where A, B_1, B_2 and C are binary matrices, $\mathbf{0}$ is the $k_1 \times k_2$ zero matrix, and I_k is the identity matrix of order k. Then C is an elementary abelian group of Type $4^{k_1}2^{k_2}$ containing $2^{2k_1+k_2}$ words (i.e $|C| = 4^{k_1}2^{k_2}$), containing $2^{2k_1+k_2}$ words (i.e $|C| = 4^{k_1}2^{k_2}$).And $C^\perp$ has generator matrix

$$H = G^\perp = \begin{bmatrix} -(B_1 + 2B_2)^T - C^T A^T & C^T & I_{n-k_1-k_2} \\ 2A^T & 2I_{k_2} & 0 \end{bmatrix}, \tag{2.6.2}$$

and $|C^\perp| = 4^{n-k_1-k_2}2^{k_2}$.

It is easy to show that HG^T is the zero matrix; hence, the rows of H are orthogonal to the rows of G which implies that

$$|C||C^\perp| = 4^n \text{ and } C \subset C^{\perp\perp}.$$

Example 2.6.1. 1) *for* $G = \begin{bmatrix} 1 & 1 & 1 & 3 \\ 0 & 2 & 0 & 2 \\ 0 & 0 & 2 & 2 \end{bmatrix}, G^\perp = \begin{bmatrix} 3 & 1 & 1 & 1 \\ 2 & 2 & 0 & 0 \\ 2 & 0 & 2 & 0 \end{bmatrix}.$

Then $|C| = 4^1 2^2 = 16$ *and* $|C^\perp| = 4^1 2^2 = 16$ *which implies* $|C||C^\perp| = 16 \times 16 = 4^4$.

2) *for* $G = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}, G^{\perp} = \begin{bmatrix} 2 & 2 \end{bmatrix}$.

Then $|C| = 4^1 2^1 = 8$ *and* $|C^{\perp}| = 4^0 2^1 = 2$ *which implies* $|C||C^{\perp}| = 8 \times 2 = 16 = 4^2$.

Again much of the study of self dual codes over Z_4 parallels that of self-dual codes over F_q. One important difference, namely there are self-dual codes of odd length over Z_4. One can associated two binary codes with C as follows.

Definition 2.6.5. [11] **Residue and Torsion codes** The residue code $C^{(1)}$ of C is given by :

$$C^{(1)} = \{(\overline{c_1}, \overline{c_2}, ..., \overline{c_n}) : (c_1, c_2, ..., c_n) \in C\},$$

where $\overline{c_i}$ denotes the reduction of c_i modulo 2 . Another binary linear code $C^{(2)}$, called the torsion code of C is given by:

$$C^{(2)} = \{\frac{c}{2} : c = (c_1, c_2, ..., c_n) \in C \text{ and } c_i \equiv 0(mod2) \text{ for} 1 \leq i \leq n\}.$$

If $k_2 = 0$ then $C^{(1)} = C^{(2)}$. The generator matrices of these codes are given by $G^{(1)}$ and $G^{(2)}$, respectively. Where

$$G_{res} = G^{(1)} = \begin{bmatrix} I_{k_1} & A & B_1 \end{bmatrix}. \tag{2.6.3}$$

$$G_{tor} = G^{(2)} = \begin{bmatrix} I_{k_1} & A & B_1 \\ 0 & I_{k_2} & C \end{bmatrix}. \tag{2.6.4}$$

If C is self orthogonal then $C^{(1)}$ is doubly even and $C^{(1)} \subseteq C^{(2)} \subseteq C^{(1)\perp}$ and if C is self dual then $C^{(2)} = C^{(1)\perp}$ as in [11] and [29].

Corollary 2.6.1. *[28] A Z_4-code C is self-dual if and only if it has a generator matrix of the form*

$$G = \begin{bmatrix} D & E & I_k + 2B \\ 0 & 2I_{n-2k} & 2C \end{bmatrix},$$

where B, C, D and E are binary matrices,

$$G_1' = \begin{bmatrix} D & E & I_k \end{bmatrix},$$

is the generator matrix for a doubly-even binary code C_1,

$$G_2' = \begin{bmatrix} D & E & I_k \\ 0 & I_{n-2k} & C \end{bmatrix},$$

is generator matrix for $C_2 = C_1^{\perp}$ and B is chosen in such a way that the first k rows of G are orthogonal in Z_4.

Definition 2.6.6. Type I and Type II codes [29] a self-dual Z_4-linear code is Type II if the Euclidean weight of every codeword is a multiple of 8. A self-dual Z_4-linear code is Type I if the Euclidean weight of some code word is not a multiple of 8.

Remark 2.6.3. In [29] and [28] it is shown that Type II codes exist only for length $n \equiv 0(mod 8)$.
These codes also contain a codeword with all coordinates ± 1 . In [8] any self-dual code of length 15 is shortened code of Type II length 16 code. There is also an upper bound on the Euclidean weight of a type I on Type II code for Z_4.

Definition 2.6.7. Type IV-codes [24] Self-dual codes over R with even Hamming weights will be called Type IV. If a code is Type IV then we shall denote it as a Type IV-I (resp. Type IV-II) if it is also a Type I (resp. Type II) code.

Example 2.6.2. *Let O_s be the Z_4-linear code, , called the octacode, with generator matrix*

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

this code is self-orthogonal has type 4^4, so it is self-dual , each codeword of O_8 has Euclidean weight a multiple of 8, and so it is of type II. O_8 is not a Type IV since $d_H = 5$. $d_L = 6$ therefore the Gray image $\phi(O_8)$ is a [16.256, 6] self-dual binary non linear code which is called Nordstrom -robinson code.

Lemma 2.6.2. *[24] If C is a Type IV code over Z_4 then the residue code $C^{(1)}$ contains the all-ones vector 1.*

Proposition 2.6.3. *[24] A type IV code C over Z_4 is Type IV-II if and only if all the Hamming weights of $C^{(1)}$ are multiples of 8.*

Proposition 2.6.4. *[24] If C is a Type IV Z_4-code of length n then all the Lee weights of C are divisible by four and its Gray image $\phi(C)$ is a self-dual Type II binary code.*

Corollary 2.6.5. *[24] A Type IV code over Z_4 of length n exist if and only if* $n \equiv 0(mod 4)$.

Corollary 2.6.6. *[24] There is no Type IV-II code of Type $4^{n/2}$ where n is the length of the code. Also there is no Type IV-I code of type $4^{n/2}$ for length $n \leq 12$.*

Also last two results agree with the Octacode (O_8) which has Type 4^4.
Here Let us undertake a review of main results of Bounds for Z_4-codes. For more information and proofs see [5], [6], [24], [28], and [29].

1) The minimum Euclidean weight d_E of a Type II Z_4-code of length n is at most

$$d_E \leq 8\left\lfloor \frac{n}{24} \right\rfloor + 8.$$

2) The minimum Euclidean weight d_E of a Type I Z_4-code of length n is at most

$$d_E \leq \begin{cases} 8\left\lfloor \frac{n}{24} \right\rfloor + 8, & n \neq 23; \\ 8\left\lfloor \frac{n}{24} \right\rfloor + 12, & n = 23. \end{cases}$$

If equality holds in this later bounds, then C is obtained by shorting a Type II code of length $n+1$.

Codes meeting these bounds are called **Euclidean extermal**.

3) The minimum Lee weight d_L of a self-dual Z_4-code of length n is at most

$$d_L \leq 2\left\lfloor \frac{n}{4} \right\rfloor + 2.$$

4) The minimum Lee weight d_L of a Type IV Z_4-code of length n is at most

$$d_L \leq 4\left\lfloor \frac{n}{12} \right\rfloor + 4.$$

In [5] Bannai, Dougherty, Harada and Oura genealized the previous results and presented methods to construct self-dual codes over Z_{2^k}.

2.6.2 Self-dual code over $R = F_2 + uF_2$

Recently, there has been interested in the ring $F_2+uF_2 = \{0, 1, u, u+1\}$ with $u^2 = 0$ (Here $F_2 = \{0, 1\}$ is the binary field) R is introduced in [1],[12],[17], [19], [24], [26]. Addition and multiplication operation in R are given as in the following tables:

+	0	1	u	1+u
0	0	1	u	1+u
1	1	0	1+u	u
u	u	1+u	0	1
1+u	1+u	u	1	0

·	0	1	u	1+u
0	0	0	0	0
1	0	1	u	1+u
u	0	u	0	u
1+u	0	1+u	u	1

The ring $F_2 + uF_2$ shares some properties of both Z_4 and F_4 when $1 + u$ and u are replaced by 3 and 2 respectively. The addition table is similar to that of the Galois field $F_4 = \{0, 1, \alpha, \alpha^2 = \alpha + 1\}$ when u and $1+u$ are replaced by α and α^2. From definition of the ring $F_2 + uF_2$ the characteristic is equal to 2 over F_2. If C is R submodule of R^n we say that C is called a linear code over R.
Moreover the sets $\{0, 1\}, \{0, u\}$ and $\{0, 1 + u\}$ form three subspaces in $F_2 + uF_2$ and the subspace $\{0, 1\} = F_2$ is a subring. For convenience, we set $v = 1 + u$. Following [1] , [17] and [25]. A nonzero linear code C over $R = F_2 + uF_2$ has a generator matrix can be written in the form

$$G = \begin{bmatrix} I_{k_1} & A & B_1 + uB_2 \\ 0 & uI_{k_2} & uD \end{bmatrix}, \tag{2.6.5}$$

where A_1, B_1, B_2 and D are matrices over F_2, we associate to such a code, two binary codes : the residue code $C^{(1)}$, and the torsion code $C^{(2)}$ as follows

$$C^{(1)} = \{x \in F_2^n | \exists y \in F_2^n | x + uy \in C\},$$

and

$$C^{(2)} = \{x \in F_2^n | ux \in C\}.$$

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

$$G^{(1)} = \begin{bmatrix} I_{k_1} & A & B_1 \end{bmatrix},$$

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

$$G^{(2)} = \begin{bmatrix} I_{k_1} & A & B_1 \\ 0 & I_{k_2} & D \end{bmatrix}.$$

If C is self-dual then $C^{(1)}$ is self orthogonal and $C^{(2)} = C^{(1)^{\perp}}$

We also have

$$|C| = |C^{(1)}| \cdot |C^{(2)}| = 2^{k_1}2^{k_1+k_2} = 2^{2k_1+k_2} = 4^{k_1}2^{k_2}.$$

The dual code of C has generator matrix in the form

$$H = \begin{bmatrix} -(B_1 + uB_2)^T - D^T A^T & D^T & I_{n-k_2} \\ uA^T & uI_{k_2} & 0 \end{bmatrix}. \tag{2.6.6}$$

Proposition 2.6.7. *[25] The set of self-dual code over R is the set of codes over R which are permutation-equivalent to a code C with a generator matrix of the form*

$$\begin{bmatrix} I_{k_1} + uB & A \\ 0 & uD \end{bmatrix},$$

where A, B and D are matrices over F_2 satisfying:

1) *B is symmetric.*

2) *A and D are such that $C^{(1)} = C^{(2)}$ and $C^{(1)}$ is even.*

Proposition 2.6.8. *[25] If C is a self-dual code over R and x and y are two code words of C such that $w_L(x) \equiv w_L(y) \equiv 0(mod4)$ then $w_L(x+y) \equiv 0(mod4)$.*

Proposition 2.6.9. *[25] If C is a self-dual code then C contains the all-u vectors.*

The above proposition corresponds to the result that $\Psi(C)$ contains the all-one vector. Recall definition 2.6.2 of Gray maps over rings of four elements.

$$\psi : R \to F_2^2$$

$$\psi(x+uy) = (y, x+y) \text{ where } x, y \in F_2 \text{ and } (x+uy) \in R.$$

We extend this in an obvious way to vectors over R,

$$\psi(x+uy) = (y, x+y) \text{ where } x, y \in F_2^n \text{ and } (x+uy) \in R^n.$$

From the definition of Gray map and the Lee weight, we have the following lemma.

Lemma 2.6.10. *[1] If a code C is linear or self-dual so is $\psi(C)$. The minimum Lee weight of C is equal to the minimum Hamming weight of $\psi(C)$.*

Thus a code $C = [n, 4^{k_1}2^{k_2}, d_L]$ over R of length $n, 4^{k_1}2^{k_2}$ codewords with minimum Lee distance of d_L gives rise to binary code $\psi(C) = [2n_1, 2k_1 + k_2, d_H = d_L]$.

Lemma 2.6.11. *Let C and C' be equivalent self-dual codes over R then $\psi(C)$ and $\psi(C')$ are equivalent.*

In [6] Rains proved the following lemma for Z_4 and in [13] AL-Ashker generalized it for $R = F_2 + uF_2$.

Lemma 2.6.12. *[13] Let C be a linear code over R then*

$$d_H \geq \left\lfloor \tfrac{d_L}{2} \right\rfloor.$$

A linear code C over R is said to be of type $\alpha(\beta)$ if $d_H = \left\lfloor \frac{d_L}{2} \right\rfloor \left(d_H > \left\lfloor \frac{d_L}{2} \right\rfloor \right)$.

Definition 2.6.8. A self-dual code over R is said to be Type II if the Lee weight of every codeword is a multiple of 4 and Type I otherwise. It is of Type IV if it has an even Hamming weight.

Proposition 2.6.13. *[25] If C is self orthogonal so is $\psi(C)$, $\psi(C)$ is a Type II code if and only if the code C is Type II.*

Corollary 2.6.14. *[25] There exists a Type II code of length n if and only if $n \equiv 0(mod 4)$.*

Lemma 2.6.15. *[24] If C is a Type IV code over $F_2 + uF_2$ then the residue code $C^{(1)}$ contains the all-ones vector 1.*

Proposition 2.6.16. *[24] A Type IV code C over $F_2 + uF_2$ is Type IV. II if and only if $C^{(1)}$ is doubly-even.*

Remark 2.6.4. Recall to proposition 2.7.4. Although the Gray image $\phi(C)$ of a Type IV Z_4 code of length n is a self-dual Type II binary code. The binary Gray map image of a Type IV $F_2 + uF_2$ code is a self-dual code but not necessarily a Type II binary code, this clear in the following example.

Example 2.6.3. *The code* $C = \{(0,0),(1,1),(u,u),(1+u,1+u)\}$ *is Type IV self-dual and has Hamming weight enumerator* x^2+3y^2*.*
Its binary image is $\{(0,0,0,0),(0,1,0,1),(1,1,1,1),(1,0,1,0)\}$*, which is not doubly-even.*

Proposition 2.6.17. *Let* C, D *be a dual pair of binary codes with even weight and* $C \subseteq D$*, then* $C+uD$ *is a Type IV code over* F_2+uF_2*.*

Corollary 2.6.18. *[24] The minimum Hamming weight weight of Type IV code over* R *of length* n *is bounded by*

$$d_H = 2\left[\ 1+\left\lfloor\ \tfrac{n}{6}\ \right\rfloor\ \right].$$

Corollary 2.6.19. *[25] Let* $d_L(II,n)$ *and* $d_L(I,n)$ *be the highest minimum Lee weight of a Type II code and a Type I code respectively, of length* n*, then*

$$d_L(II,n) \leq 4\left\lfloor\ \tfrac{n}{12}\ \right\rfloor + 4.$$

$$d_L(I,n) \leq \begin{cases} 4\left\lfloor\ \tfrac{n}{12}\ \right\rfloor + 4, & \text{if } n \not\equiv 22 (\text{mod } 24); \\ \\ 4\left\lfloor\ \tfrac{n}{24}\ \right\rfloor + 6, & \text{otherwise.} \end{cases}$$

Proposition 2.6.20. *[26] The highest minimum Hamming weights of length 18 and 24 are determined. The highest minimum Euclidean weights of length 14, 18 and 24 are determined.*

Remarks 2.6.1.

1) The result stated in the above proposition were announced in [24] (except for the highest minimum Euclidean weight of length 24).

2) In [24] Harada and Sole showed that there is no Type IV code with minimum Hamming weight 10 over Z_4 and F_2+uF_2.

Chapter 3

Self-dual codes over $F_2 + vF_2$

The main tool in this chapter is the following theorems.

3.1 Chinese Remainder theorem

Theorem 3.1.1. *[27] Let $I_1, I_2, ..., I_n$ be ideals in a ring R such that*

1) $I_1 + I_2, ... + I_n = R$ *and,*

2) *for each $k(1 \leq k \leq n), I_k \cap (I_1 + ... + I_{k-1} + I_{k+1} ...... + I_n) = 0$. Then there is a ring isomorphic $R \cong I_1 \times I_2 \times ...... \times I_n$.*

Theorem 3.1.2. ***Chinese Remainder theorem****[27] Let $I_1, I_2, ..., I_n$ be ideals in a ring R such that $R^2 + I_i = R$ for all i and $I_i + I_j = R$ for all $i \neq j$. If $b_1, ..., b_n \in R$ then there exist $b \in R$ such that*

$$b \equiv b_i (mod\ I_i) \qquad (i = 1, 2, ..., n).$$

Furthermore b is uniquely up to congruence modulo the ideal

$$I_1 \cap I_2 \cap ...... \cap I_n.$$

Remark 3.1.1. [27] If R has an identity, then $R^2 = R$, whence $R^2 + I = R$ (for every ideal I of R).

The ring $R = \mathbb{F}_2 + v\mathbb{F}_2 = \{0, 1, v, 1 + v\}$ where $v^2 = v$ and $\mathbb{F}_2 = \{0, 1\}$ is a commutative ring with four elements introduced in [2], [9], [10], [23] and [24]. In [25] it was shown that this ring is isomorphic to the ring $\mathbb{F}_2 \times \mathbb{F}_2$ by the Chinese Remainder Theorem (CRT)[22]. Addition and multiplication operations over R are given in the following tables:

+	0	1	v	1+v
0	0	1	v	1+v
1	1	0	1+v	v
v	v	1+v	0	1
1+v	1+v	v	1	0

.	0	1	v	1+v
0	0	0	0	0
1	0	1	v	1+v
v	0	v	v	0
1+v	0	1+v	0	1+v

For conveniens, we set $1 + v = w$ and $R = F_2 + vF_2$. The above table shows that v and w are orthogonal idempotents ($vw = 0$), and their sum equals **1**. Following [23] This ring is a semi-local ring it has two maximal ideals $\langle v\rangle$ and $\langle 1 + v\rangle$. Observe that $R/\langle v\rangle$ and $R/\langle 1 + v\rangle$ are isomorphic to F_2. In other word :

$R/\langle v\rangle = \{0 + \langle v\rangle, 1 + \langle v\rangle\} \simeq F_2$.
$R/\langle 1+v\rangle = \{0 + \langle 1+v\rangle, 1 + \langle 1+v\rangle\} \simeq F_2$.
$R/\langle v\rangle \cap \langle 1+v\rangle \simeq R/\langle v\rangle \oplus R \setminus \langle v+1\rangle \simeq F_2 \oplus F_2$.
The CRT tells us that

$$R = \langle v\rangle \oplus \langle 1 + v\rangle.$$

By linear algebra over F_2 we show that

$$a + vb = (a + b)v + a(v + 1)\ ,\ \text{ for all }\ a, b \in F_2^n.$$

A linear code C of length n over R is an R-submodule of $R^n = (F_2 + vF_2)^n$. An element of C is called a codeword of C. For $R = F_2 + vF_2$ we say C and C' are equivalent if either C and C' are permutation equivalent or C is permutation equivalent to the code obtained from C' by changing v and $1 + v$ in all coordinates.

Example 3.1.1. *Consider the code C with generator matrix,*

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

then the generator matrix of the code C' is

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

3.1.1 B-ordering over the ring $R = F_2 + vF_2$

Elatrash in [16] defined **B**-ordering over the ring Z_4. And Al-Ashkar in [12] define **B**-ordering over the ring $F_2 + uF_2$. We define a **B**-ordering over $F_2 + vF_2$ as follows:

Definition 3.1.1. Let $B = \{b_1, b_2, ..., b_n\}$ be a basis for the module $(R)^n$ over R . We define the **B-**ordering as follows: The first 4 vectors are $0, b_1, vb_1, wb_1$. The **B-**ordering is then generated recursively , where if 4^k vectors of the ordering have been generated using basis elements, $b_1, b_2, ..., b_k$, then the next $3(4^k)$ vectors are generated by adding ib_{k+1} to those vectors already produced, in order $i = 1, v, w$.

Example 3.1.2. *Let $B = \{b_1, b_2\}$ be a basis of a free module $(R)^2$ over R, then the **B**-ordering is :*

$0, b_1, vb_1, wb_1$,

$b_2, b_2 + b_1, b_2 + vb_1, b_2 + wb_1$,

$vb_2, vb_2 + b_1, vb_2 + vb_1, vb_2 + wb_1$,

$wb_2, wb_2 + b_1, wb_2 + vb_1, wb_2 + wb_1$.

There are three different weights for codes over R are known, namely the Hamming, Lee and Bachoc weights.

Definition 3.1.2. The Hamming weight of a codeword is the number of nonzero components.

Definition 3.1.3. The Lee weights of the elements $0,\ 1, v$ and $1+v$ are $0, 2, 1$ and 1 respectively. The Bachoc weight is defined in [2] and the weights of the elements $0,\ 1, v$ and $1+v$ are $0, 1, 2$ and 2 respectively. The Lee and Bachoc weights of a codeword are the rational sums of the Bachoc weights of its components, respectively. The Lee weight for a codeword $x = (x_1, x_2, ..., x_n) \in R^n$ is defined by, $wt_L(x) = \sum_{i=1}^{n} wt_L(x_i)$, where

$$wt_L(x_i) = \begin{cases} 0 & \text{if } x_i = 0, \\ 1 & \text{if } x_i = v \text{ or } 1+v, \\ 2 & \text{if } x_i = 1. \end{cases}$$

Definition 3.1.4. The Bachoc weight is given by the relation $wt_B(x) = \sum_{i=1}^{n} wt_B(x_i)$, where

$$wt_B(x_i) = \begin{cases} 0 & \text{if } x_i = 0, \\ 1 & \text{if } x_i = 1, \\ 2 & \text{if } x_i = v \text{ or } 1 + v. \end{cases}$$

Note that $\forall x_i \neq 0 \quad wt_L(x_i) + wt_B(x_i) = 3$.

Remark 3.1.2. Let $n_0(x)$ be the number of components i for which $x_i = 0$, $n_1(x)$ be the number of components i of which $x_i = 1$ and $n_2(x) = n - n_0(x) - n_1(x)$, i.e., n_2 be the number of $v's$ and $(1+v)'s$ in x. Then the Lee weight $wt_L(x)$ (resp. the Bachoc weight $wt_B(x)$) of $x = (x_1, x_2, ...x_n) \in R^n$ can also be obtained as:

$$wt_L(x) = n_2(x) + 2n_1(x),$$

and

$$wt_B(x) = n_1(x) + 2n_2(x).$$

For

$$x = (x_1, x_2, ..., x_n),\ y = (y_1, y_2, ..., y_n) \in R^n,$$

the Hamming distance between x and y is denoted by

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

The Lee distance between x and $y \in R^n$ is denoted by,

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

The Bachoc distance between x and $y \in R^n$ is denoted by,

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

Definition 3.1.5. The minimum Hamming, Lee and Bachoc weights, $d_H,\ d_L$ and d_B of C are the smallest Hamming, Lee and Bachoc weights among all non-zero codewords of C, respectively.

Example 3.1.3. *Let* $B = \{0v1v, wv01, ww1v, v0vw\}$ *be a basis of* R^4 *over* F_2 *then by the additive* B*-ordering.*

$C = \{0000, 0v1v, wv01, w01w, ww1v, w100, 011w, 0w01, v0vw, vvw1, 1vvv, 10w0, 1ww1, 11vw, v1w0, vwvv\}$.

Let

$x = ww1v \quad , \; y = v0vw \quad , \; z = 10w0.$

$wt_H(x) = 4 \quad , \; wt_H(y) = 3 \quad , \; wt_H(z) = 2.$

$wt_L(x) = 5 \quad , \; wt_L(y) = 3 \quad , \; wt_L(z) = 3.$

$wt_B(x) = 7 \quad , \; wt_B(y) = 6 \quad , \; wt_B(z) = 3.$

$d_H = 2, \quad d_L = 3, \quad d_B = 3.$

3.1.2 The Macwilliams Relations

In [23] the Hamming weight enumerator for a code over R is defined by:

$$W_C(x, y) = \sum_{u \in C} x^{n-wt(u)} y^{wt(u)} = \sum_{i=0}^{n} A_i x^{n-i} y^i.$$

The complete weight enumerator for a code over R is defined by:

$$cwe_C(x_0, x_1, x_v, x_{1+v}) = \sum_{c \in C} cwt(c)$$

where $cwt(c) = \prod a^{n_0(c)} b^{n_1(c)} c^{n_v(c)} d^{n_{1+v}(c)}$ and n_α is the number of times α appears in c. Now define the Lee composition of x say $L_i(x) = 0,\ 1,\ 2$ as the number of entries in x of Lee weight i. The symmetrized weight enumerator (swe) is defined by:

$$swe_C(a, b, c) = \sum_{x \in C} a^{L_0(x)} b^{L_1(x)} c^{L_2(x)}$$

and is given by

$$swe_C(a, b, c) = cwe(a, c, b, b).$$

The Hamming weight enumerator for a code C is given by

$$W_C(x, y) = cwe_C(x, y, y, y).$$

Example 3.1.4. *consider the code* C *with generator matrix*

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

To find complete and symmetrized weight enumerator of C over R, We write,
$C = \{000, v11, 10v, 1w0, w1w, wv1, 0wv, vvw, vvv, wv0, w1v, 0ww, 1w1, 10w, v10, 001,$
$v0v, 01w, wwv, 1vw, w00, 111, vw0, 0v1, v00, 011, w0v, 11w, ww0, 1v1, vwv, 0vw,$
$0v0, 110, w10, www, v0w, 1ww, 1ww, 0vv, 1v0, wvv, w0w, v01, 101, 00v, v1w, 0w1,$
$0w0, vv1, v1v\}$ *then,*

$$\begin{aligned} cwe(a,b,c,d) = {} & a^3 + b^3 + c^3 + d^3 + 6(abc + abd + acd + bcd) + 3(ac^2 + ab^2 + ad^2 \\ & + a^2c + a^2b + a^2d + bc^2 + b^2c + c^2d + d^2c + db^2 + bd^2). \end{aligned}$$

$$swe(a,b,c,c) = a^3 + b^3 + 8c^3 + 12(abc + bc^2 + ac^2) + 6(a^2c + cb^2) + 3(a^2b + ab^2).$$

Example 3.1.5. *The weight enumerator of the code C with generator matrix,*

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

$$\begin{aligned} W_C(a,b,c) = {} & a^8 + 8a^3b^4c + 4c^2(2a^4b^2 + 5a^2b^4) + 8c^3(a^5 + 4a^3b^2 + 2ab^4) \\ & + 2c^4(5a^4 + 28a^2b^2 + 2b^4) + 8c^5(a^3 + 6ab^2) + 4c^6(3a^2 + 4b^2) \\ & + 8ac^7 + c^8. \end{aligned}$$

Definition 3.1.6. Euclidean and Hermitian inner product
We define two inner products (x, y) and $\langle x, y\rangle$ of x and $y \in R^n$. The Euclidean inner product is defined as:

$$(x, y) = x_1y_2 + x_2y_2 + ... + x_ny_n,$$

and the Hermitian inner product is defined as:

$$\langle x, y\rangle = x_1\overline{y}_2 + x_2\overline{y}_2 + ... + x_n\overline{y}_n,$$

where, $\overline{0} = 0$, $\overline{1} = 1$, $\overline{v} = v + 1$ and $\overline{v+1} = v$.

Definition 3.1.7. The dual code $C^{\perp}$ with respect to the Euclidean inner product of C is defined as:

$$C^{\perp} = \{x \in R^n | (x, y) = 0 \text{ for all } y \in C\},$$

and the dual code $C^{\perp_H}$ with respect to the Hermitian inner product of C is defined as:

$$C^{\perp_H} = \{x \in R^n | \langle x, y \rangle = 0 \text{ for all } y \in C\}.$$

Definition 3.1.8. C is called self orthogonal if $C \subseteq C^{\perp}$ and C is called Hermitian self-orthogonal if $C \subseteq C^{\perp_H}$. C is Euclidean self-dual if $C = C^{\perp}$ and C is Hermitian self dual if $C = C^{\perp_H}$.

Definition 3.1.9. [23] An Euclidean self-dual code is doubly even if the Lee weight of all its words is divisible by 4 and singly even otherwise.

Definition 3.1.10. [23] An Euclidean self-dual code is said to be Type II if the weights of all its words are a multiple of 4, and Type I otherwise.

Definition 3.1.11. [23] A Hermitian self-dual code is said to be of Type S if all its Lee weight are multiple of 4.

Following [24] and [23] Note that an Euclidean self-dual codes exist in length n if and only if n is even, since self-dual codes over F_2 exist only for even lengths, and Type II Euclidean codes can only exist in length multiple of 8 like doubly even binary codes. Hermitian self-dual exist for any length.

Theorem 3.1.3. *[2] and [9] If $C \in R^n$ is a Hermitian (or Euclidean) self-dual code then*

$$d_B \leq 2(1 + \lfloor \frac{n}{3} \rfloor).$$

Codes meeting that bound with equality are called extremal.

Definition 3.1.12. We say that a self-dual code with the highest minimum Bachoc weight among all self-dual codes of that length is optimal.

Example 3.1.6.

1) *The code C with the generator matrix*

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

is extremal self-dual code of Type II

2) *The code C with the generator matrix*

$$\begin{bmatrix} 1 & 0 & 0 & v & v & 1 & w & w & 0 & 0 \\ v & 1 & 0 & 0 & v & 0 & 1 & w & w & 0 \\ v & v & 1 & 0 & 0 & 0 & 0 & 1 & w & w \\ 0 & v & v & 1 & 0 & w & 0 & 0 & 1 & w \\ 0 & 0 & v & v & 1 & w & w & 0 & 0 & 1 \end{bmatrix}$$

is extremal self-dual code of Type S.

Definition 3.1.13. [2], [10], [24] Consider the following map,

$$\varphi : F_2 + vF_2 \longrightarrow F_2 \times F_2,$$

defined as $\varphi(x + vy) = (x, x + y)$ for all $x, y \in F_2^n$. φ is a ring isomorphism called Gray map. This map can be extended naturally from $(F_2 + vF_2)^n$ to F_2^{2n}. The Lee weight of $x + vy$ is the Hamming weight of its Gray image.

From definition (2.6.2) we recall that $\varphi(0) = (0, 0), \varphi(1) = (1, 1), \varphi(v) = (0, 1)$ and $\varphi(1 + v) = (1, 0)$ Note that :φ is linear(preserves addition). Since,

$$\begin{aligned} \varphi((x + yv) + (x' + y'v)) &= \varphi(x + x' + (y + y')v) \\ &= (x + x', x + x' + y + y') \\ &= (x + x', x + y + x' + y') \\ &= \varphi(x + yv) + \varphi(x' + y'v). \end{aligned}$$

Also, φ preserves multiplication, since

$$\begin{aligned} \varphi((x + yv)(x' + y'v)) &= \varphi(xx' + xy'v + yx'v + yy'v^2) \\ &= \varphi(xx' + (xy' + yx' + yy')v) \end{aligned}$$

$$
\begin{aligned}
&= (xx', xx' + xy' + yx' + yy') \\
&= (xx', (x+y)x' + (x+y)y') \\
&= (xx', (x+y)(x'+y')) \\
&= (x, (x+y))(x', (x'+y')) \\
&= \varphi(x+yv)\varphi(x'+y'v).
\end{aligned}
$$

3.1.3 The Chinese remainder theorem and self-dual codes

Following [22], Let R be a commutative ring (not necessarily finite)with a multiplicative identity denoted by $\mathbf{1}$. Let $I_1, I_2, I_3, ..., I_k$ be ideals of R such that :

1) $S_i = R/I_i$ is finite ,

2) $I_j + \cap_{k \neq j} I_k = R$ for $1 \leq j \leq k$.

That is, the ideals are relative prime, since R is commutative.
Set $I = \cap I_i$ and $S = R/I$. Define the map

$$\varphi : S \to (R/I_1) \times (R/I_2) \times ...... \times (R/I_k)$$

by

$$\varphi(\alpha) = (\alpha(modI_1), \alpha(modI_2), ..., \alpha(modI_k)).$$

The map φ^{-1} is a ring isomorphism by the generalized Chinese Remainder Theorem.
Let $C_1, C_2, ..., C_k$ be codes where C_i is a code over S_i, and define the code

$$CRT(C_1, C_2, ..., C_k) = \{\varphi^{-1}(c_1, c_2, ..., c_k) | c_i \in C_i\}.$$

We say that the code $CRT(C_1, C_2, ..., C_k)$ is the Chinese product of codes $C_1, C_2, ..., C_k$. It is clear that $|CRT(C_1, C_2, ..., C_k)| = \Pi_{i=1}^{k} |C_i|$ and that if C_i is self-orthogonal for all i then $CRT(C_1, C_2, ..., C_k)$ is self-orthogonal. This gives the following :

Theorem 3.1.4. *[24] and [25] $CRT(C_1, C_2, ..., C_k)$ is a self-dual code over S if and only if it is the Chinese product of self-dual codes $C_1, ..., C_k$ over $S_1, ..., S_k$, respectively.*

In [10] it was shown that if C is a code over $R = F_2 + vF_2$, then there are binary codes C_1 and C_2 such that $C = \varphi^{-1}(C_1, C_2)$, and we denoted C by $CRT(C_1, C_2)$. Note that C_1 and C_2 are uniquely determined for each $CRT(C_1, C_2)$.
Let c, be a codeword of C then c can be uniquely written as $c = \varphi^{-1}(c_1, c_2)$, where c_1 and c_2 are codewords of C_1 and C_2 respectively.
Let $wt_H(c), wt_L(c)$ and $wt_B(c)$ be the Hamming, Lee and Bachoc weights of c respectively. Then

$$\begin{aligned} wt_H(c) &= wt_H(c_1) + wt_H(c_2) - wt_H(c_1 * c_2). \qquad (3.1.1) \\ wt_L(c) &= wt_H(c_1) + wt_H(c_2). \\ wt_B(c) &= 2wt_H(c_1) + 2wt_H(c_2) - 3wt_H(c_1 * c_2). \end{aligned}$$

Where $c_1 * c_2$ denotes the Hadamard product(componentwise multiplication) of c_1 and c_2. (i.e., for $c_1 = (x_1, x_2, ..., x_n)$ and $c_2 = (y_1, y_2, ..., y_n)$ then $c_1 * c_2 = (x_1y_1, x_2y_2, ..., x_ny_n)$).

Example 3.1.7. *Let c is a codeword of the code C over R such that $c = 01vw$, then*
$c_1 = 0101, c_2 = 0110$
$wt_H(c) = 2 + 2 - 1 = 3.$
$wt_L(c) = 2 + 2 = 4.$
$wt_B(c) = 2 \times 2 + 2 \times 2 - 3 \times 1 = 8 - 3 = 5.$

Proposition 3.1.5. *[10] Let d_H and d_L be the minimum Hamming and Lee weights of*

$$C = \varphi^{-1}(C_1, C_2),$$

respectively. Then $d_H = d_L = min\{d(C_1), d(C_2)\}$, where $d(C_i)$ denotes the minimum weight of a binary code C_i.

Proof. We shall show that $d_H = \min\{d(C_1), d(C_2)\}$. Let c be a codeword of $CRT(C_1, C_2)$ then $c = \varphi^{-1}(c_1, c_2)$ where c_1 and c_2 are codewords of C_1 and C_2 respectively. Then it follows from (3.1.1) that $wt_H(c) \geq \max\{wt_H(c_1), wt_H(c_2)\}$. Thus $d_H \geq \min\{d(C_1), d(C_2)\}$. Assume that $d(C_1) \geq d(C_2)$. Let c_2' be a codeword with weight $d(C_2)$ in C_2 then $\varphi^{-1}(0, c_2')$ is a codeword of Hamming weight $d(C_2)$. The result follows. In similar way, we can prove that

$$d_L = \min\{d(C_1), d(C_2)\}.$$

□

Example 3.1.8. *Let C be a code over R with generator matrix,*

$$G = \begin{bmatrix} v & 1 & 1 \\ 1 & 0 & v \\ 1 & w & 0 \end{bmatrix} \textit{ then,}$$

$$C_1 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \quad \textit{and} \quad C_2 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}.$$

$d_L = d_H = 1 = min(d(C_1), d(C_2))$.

Lemma 3.1.6. *[10] and [24] Let $CRT(C_1, C_2)$ and $CRT(C_1', C_2')$ be codes over $F_2 + vF_2$. $CRT(C_1, C_2)$ and $CRT(C_1', C_2')$ are equivalent if and only if there exist a permutation which sends (C_1, C_2) to (C_1', C_2') or to (C_2', C_1').*

3.1.4 Generator matrix and binary Structure of codes over R

Following [23], by the properties of CRT any code over $R = F_2 + vF_2$ is permutation equivalent to a code generated by the following matrix:

$$\begin{bmatrix} I_{k_1} & vB_1 & (1+v)A_1 & (1+v)A_2 + vB_2 & (1+v)A_3 + vB_3 \\ 0 & (1+v)I_{k_2} & 0 & (1+v)A_4 & 0 \\ 0 & 0 & vI_{k_3} & 0 & vB_4 \end{bmatrix},$$

where A_i and B_j are binary matrices, such a code is said to have rank $\{2^{k_1}, 2^{k_2}, 2^{k_3}\}$.
If H is a code over R, Let H^+(resp. H^-) be the binary code such that $(1+v)H^+$(resp. vH^-) is read H mod v (resp. H mod $(1+v)$).
We have

$$H = (1+v)H^+ \oplus vH^-.$$

With

$$H^+ = \{s | \exists t \in F_2^n | (1+v)s + vt \in H\};$$

$$H^- = \{t | \exists s \in F_2^n | (1+v)s + vt \in H\}.$$

The code H^+ is permutation equivalent to a code with generator matrix of the form

$$\begin{bmatrix} I_{k_1} & 0 & A_1 & A_2 & A_3 \\ 0 & I_{k_2} & 0 & A_4 & 0 \end{bmatrix},$$

where A_i are binary matrices.
And the binary code H^- is permutation equivalent to a code with generator matrix of the form:

$$\begin{bmatrix} I_{k_1} & B_1 & 0 & B_2 & B_3 \\ 0 & 0 & I_{k_3} & 0 & B_4 \end{bmatrix},$$

where B_i are binary matrices. The preceding statements show that any code H over R is completely characterized by its associated codes H^+ and H^- and conversely.

Theorem 3.1.7. *Let H be a code of length n over R, with associated binary codes H^+ and H^- then for the Hermitian scalar product :*

$$H^\perp = (1+v)(H^-)^\perp \ \oplus v(H^+)^\perp$$

and the self-dual codes over R are the codes over H with associated binary codes H^+ and H^- verifying $H^+ = (H^-)^\perp$.

Proof. Observe that if c, c', d, d' are binary vectors of length n. Then

$$(cv + d(1+v))\overline{(c'v + d'(1+v))} = av + b(1+v)$$

with $a = cd'$ and $b = dc'$. This shows that $a = b = 0$ if and only if $dc' = cd' = 0$ □

Here is the analogue of the preceding theorem for Euclidean codes.

Theorem 3.1.8. *Let H be a code of length n over R, with associated binary codes H^+ and H^- then for the Euclidean scalar product :*

$$H^\perp = (1+v)(H^+)^\perp \ \oplus v(H^-)^\perp$$

and the self-dual codes over R are the codes over H with associated binary codes H^+ and H^- such that H^+ and H^- are self-dual binary codes.

Proof. Observe that if c, c', d, d' are binary vectors of length n. Then

$$(cv + d(1+v))(c'v + d'(1+v)) = av + b(1+v)$$

with $a = cc'$ and $b = dd'$.

This shows that $a = b = 0$ if and only if $cc' = dd' = 0$. $\square$

Theorem 3.1.9. *Let $H = (1 + v)H^+ \oplus vH^-$ be a R code of length n then H is self-dual for the Euclidean scalar product if and only if the two codes H^+ and H^- are self-dual binary codes.*

Proof. Straightforward from Theorem 3.1.4. $\square$

Corollary 3.1.10. *Let $H = (1 + v)H^+ \oplus vH^-$ be a self-dual Euclidean R code then H is a type II if and only if the codes H^+ and H^- are binary of Type II codes.*

Proof. It follows by noticing that $(w_L(cv + d(1 + v))) = w_H(c) + w_H(d)$. $\square$

Theorem 3.1.11. *Let $H = (1 + v)H^+ \oplus vH^-$ be a R code of length n then H is self-dual for the Hermitian scalar product if and only if the two codes H^+ and H^- are dual of one another.*

Theorem 3.1.12. *Let $H = (1 + v)H^+ \oplus vH^-$ be a R code of length n then H is self-dual for the Hermitian scalar product and of type S if and only if the two codes H^+ and H^- are dual of one another and are both even.*

Theorem 3.1.13. *Let $H(H^-, H^+)$ be a self-dual Euclidean code of length n then $\varphi(H^-(v)+ H^+(1 + v))$ is a self-dual binary code of length $2n$, It is doubly even if H is a Type II.*

Proof. The Gray map φ is linear, moreover $(a + vb)(a' + vb') = 0$ yields by looking at the v-components $bb' + ba' + b'a = 0$ i.e. $\varphi(a + vb)\varphi(a' + vb') = 0$. The first assertion follows, the second assertion follows from the weight property of Type II codes. $\square$

The analogous statement for Hermitian codes is the following.

Theorem 3.1.14. *Let $H(H^-, H^+)$ be a self-dual Hermitian code of length n then $\varphi(H^-(v)+ H^+(1+v))$ is a formally self-dual binary code of length $2n$. It is even if H is Type S, and self-dual if $H^+ \subseteq H^-$.*

Proof. The first statement is a general property of Gray maps. The second statement is immediate. The third follows after a straightforward calculation. Indeed if (c, d) and (c', d') are in $H(H^-, H^+)$ then their dot product is $cd' + dc'$ while the dot product of their Gray images is $cd' + c'd + dd'$. $\square$

3.1.5 Self-dual code of Type IV

Corollary 3.1.15. *[24] Let $CRT(C_1, C_2)$ be an Euclidean self-dual code $CRT(C_1, C_2)$ is Type IV if and only if $C_1 = C_2$.*

Proof. By proposition 3.1.12 $C_1$and C_2 are binary self-dual. Thus, all codewords of C_1 and C_2 have even weights. If $CRT(C_1, C_2)$ is Type IV then $w_H(c)$ is even for any codeword c of $CRT(C_1, C_2)$. by (3.1.1) $w_H(c_1 * c_2)$ is even. It turns out that $C_1 = C_2^{\perp}$ then $C_1 = C_2$. Conversely , if $C_1 = C_2$ then the Hamming weight of any codeword of $CRT(C_1, C_2)$ is even by (3.1.1). □

Proposition 3.1.16. *Bachoc [2] Let C_1 and C_2 be a binary codes $CRT(C_1, C_2)$ is a self-dual code over $F_2 \times F_2$ if and only if $C_2 = C_1^{\perp}$ where $C_1^{\perp}$ denotes the dual code of the binary code C_1.*
Thus, the Bachoc weights of all codewords of self-dual code are even .

Proposition 3.1.17. *[24] $CRT(C_1, C_2)$ is a Hermitian self-dual code if and only if $C_1 = C_2^{\perp}$.*

Corollary 3.1.18. *[24] Let $CRT(C_1, C_2)$ be a Hermitian self-dual code. $CRT(C_1, C_2)$ is a type IV if and only if C_1 and C_2 are even.*

Proof. suppose that $CRT(C_1, C_2)$ is a Type IV. By proposition (3.1.16), $C_1 = C_2^{\perp}$. It follows form (3.1.15) that $w_H(c_1) + w_H(c_2)$ is even for all codewords c_1 and c_2 in C_1 and C_2,. Thus, take the zero vector as c_1 then $w_H(c_2)$ is even. even. Similarly, take the zero-vector as c_2 then $w_H(c_1)$ is even. Therefore, C_1 and C_2 must be even codes.
Conversely, if $C_1 = C_2^{\perp}$, C_1 and C_2 are even then $CRT(C_1, C_2)$ is Type IV by (3.1.1). □

Corollary 3.1.19. *[24] If C is an Euclidean Type IV code, then C is Hermitian Type IV.*

Proof. Let $C = CRT(C_1, C_2)$ then $C_1 = C_2$ by corollary (3.1.15). Recall proposition(3.1.14) C_1 and C_2 are Binary self-dual codes and so $C_1 = C_2^{\perp}$ which implies that $CRT(C_1, C_2)$ is a Hermitian self-dual code. □

Therefore Euclidean Type IV codes are a special class of Hermitian Type IV codes.

We now give divisibly conditions of Lee and Bachoc weight for self-dual codes and Type IV codes over $F_2 + vF_2$.

Corollary 3.1.20. *[24] Let C be an Euclidean self-dual code. Then the Lee weight of a codeword of C is even. Moreover, if C is Type IV then all the Bachoc weights are even.*

Proof. Since $CRT(C_1, C_2)$ is an Euclidean self-dual, so C_1 and C_2 are binary self-dual codes. Thus $wt_L(c) = wt_H(c_1) + wt_H(c_2)$ is even. If C is an Euclidean self-dual code of Type IV, then $C_1 = C_2$, therefore :

$$\begin{aligned} wt_B(c) &= 2wt_H(c_1) + 2wt_H(c_2) - 3wt_H(c_1 * c_2) \\ &= 4wt_H(c_1) - 3wt_H(c_1 * c_2) \\ &= 4wt_H(c_1) = 4wt_H(c_2). \end{aligned}$$

□

Corollary 3.1.21. *Let C be a Hermitian self-dual code. Then the Bachoc weight of a codeword of C is even. Moreover if C is Type IV then all the Lee weights are even.*

Proof. By proposition , since $CRT(C_1, C_2)$ is Hermitian self-dual code, so
$C_1 = C^{\perp}{}_2 = C_2$

$$\begin{aligned} wt_B(c) &= 2wt_H(c_1) + 2wt_H(c_2) - 3wt_H(c_1 * c_2) \\ &= 4wt_H(c_1) = 4wt_H(c_2) \end{aligned}$$

which implies that the Bachoc weight of a codeword of C is even. Moreover if C is Type IV Hermitian self-dual code, C_1 and C_2 will be even by corollary (3.1.18) It follows from (3.1.1) that

$$wt_L(c) = wt_H(c_1) + wt_H(c_2)$$

is even for all codewords c_1 and c_2 in C_1 and C_2 respectively. □

Corollary 3.1.22. *A Hermitian Type IV $F_2 + vF_2$ code of length n exists if and only if n is even.*

Proof. The previous theorems give that if a Hermitian Type IV code of length n exists then n is even. □

Example 3.1.9.

$$\textit{The code } C = \{(0,0), (1,1), (v,v), (1+v, 1+v)\}$$

is Type IV code of length 2.

3.1.6 Construction of extremal self-dual codes

Theorem 3.1.23. *[2] and [9] If $C \in R^n$ is a Hermitian (or Euclidean) self-dual code then*

$$d_B \leq 2(1 + \lfloor \frac{n}{3} \rfloor).$$

Codes meeting that bound with equality are called extremal.

Definition 3.1.14. We say that a self-dual code with the highest minimum Bachoc weight among all self-dual codes of that length is optimal, of course an extremal self-dual code is optimal.

Lemma 3.1.24. *[2] Let $C = C_1 \times C_1^{\perp}$ be a self-dual code over R. Then*

$$wt(C) \geq 6 \Longleftrightarrow \begin{cases} wt(C_1) \geq 3 \\ wt(C_1^{\perp}) \geq 3 \\ wt(C_1 \cap C_1^{\perp}) \geq 6. \end{cases}$$

Theorem 3.1.25. *Bachoc [2] There is no external code of length 6 and 7 over R. There is at least one of length 8 which is $C = C_1 \times C_1^{\perp}$ where C_1 is the binary code generating matrix*

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

Theorem 3.1.26. *There is no external code of length 9 over R. There is at least one of length 10 which is $C = C_1 \times C_1^{\perp}$ where C_1 is the binary double circulant code generating matrix*

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

Lemma 3.1.27. *[9] Let $d_{max}(n, k)$ be the highest minimum weight among all binary linear $[n, k]$ codes. Let $d_B(n)$ be the highest minimum Bachoc weight among all self-dual codes over R of length n then*

$$d_B(n) \leq 2d_{max}(n, \lfloor (n + 1)/2 \rfloor).$$

Lemma 3.1.28. *[9] For $n = 9$ and $n \geq 12$,*

$$d_B(n) \leq 2d_{max}(n, \lfloor (n+1)/2 \rfloor) \leq \lfloor n/3 \rfloor.$$

Lemma 3.1.29. *[9] All binary [11, 6, 4] codes with dual distance 4 are equivalent to the code C_{11} with generator matrix*

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

Theorem 3.1.30. *Extremal self-dual codes over R exist only for lengths 1, 2, 3, 4, 5, 8 and 10.*

More details about classification of all extremal self-dual codes are found in [2] and [10].

3.2 Self-dual codes over the ring $F_p + vF_p$

Following [2] and [18], the alphabet $F_p + vF_p$ is a semi-local ring. It is as noticed in [2] abstractly isomorphic to $F_p \times F_p$ where p is a prime number.
If $R = F_p \times F_p$ there are two ideals namely $F_p \times \{0\}$ and $\{0\} \times F_p$, which are conjugate.
We can assume that $I = Re, I' = R\bar{e}$ with $e^2 = e$. Then $e + \bar{e} = 1$ and $e\bar{e} = 0$.
We set $C_1 = I$. Then C_1 is self-dual code of length one over R Let I' be a second nontrivial ideal distinct form I , the two ideals define conjugate codes.
For $n \geq 2$

$$C_n = \{(x_1, x_2, ..., x_n) \in R^n | \ \forall i \neq j, x_i \equiv \ x_j \ mod \ I \text{ and } \sum_{i=1}^{n} x_i \equiv 0 \ mod \ I'\}.$$

Then C_n is self-dual over R.

Lemma 3.2.1. *[2] The group R^* of invertible elements of R;*

$$R = F_p \times F_p : \ R^* = \{(a, b) \mid a \neq 0, b \neq 0\}.$$

Definition 3.2.1. Let R be the ring defined in the previous lemma. The Bachoc weight wt on R is defined by :

$$\begin{cases} wt(0) = 0 \\ wt(x) = 1 \quad \text{if} \;\; x \in R^* \\ wt(x) = p \quad \text{if} \;\; x \in R \setminus (R^* \cup \{0\}). \end{cases}$$

To show the efficient of these results, we shall introduce the ring $R = F_3 + vF_3$ as another examples of these rings.

3.2.1 Codes over the ring $F_3 + vF_3$

The alphabet $R = F_3 + vF_3 = \{0, 1, 2, v, 2v, 1+v, 2+v, 1+2v, 2+2v\}$ where $v^2 = 1$ and $F_3 = \{0, 1, 2\}$ is a commutative ring with nine elements introduced in [18]. For $x, y \in F_3$ we have $\overline{x + vy} = x - vy$. In [2], it was shown that this ring is isomorphic to the ring $F_3 \times F_3$ by the Chinese Remainder Theorem (CRT). Following [2] This ring is a semi-local ring it has two maximal ideals $\langle v - 1\rangle$ and $\langle 1 + v\rangle$. Observe that $R/\langle v - 1\rangle$ and $R/\langle 1 + v\rangle$ are isomorphic to F_3. The CRT tells us that:

$$R = \langle v - 1\rangle \oplus \langle 1 + v\rangle.$$

Where

$$\langle v - 1\rangle = \{0, v + 2, 1 + 2v\}.$$

$$\langle 1 + v\rangle = \{0, 1 + v, 2v + 2\}.$$

By linear algebra over F_3, we show that

$$a + vb = (a - b)\langle v - 1\rangle - (a + b)\langle v + 1\rangle \;, \text{ for all } \; a, b \in F_3^n.$$

A code over R is a R-submodule of R^n .

The Euclidean scaler product is $\sum_{i=1}^{n} x_i y_i$.

The Gray map θ from $R_3^n \longrightarrow F_3^{2n}$ is defined as

$$\theta(x + vy) = (x, y) \text{ for all } x, y \in F_3^n.$$

The Lee weight of $x + vy$ is the Hamming weight of its Gray image.

Note that θ is linear, since

$\theta(x + vy + x' + vy') = \theta((x + x') + (y + y')v)$

$$= (x + x', y + y')$$
$$= \theta(x + vy) + \theta(x' + vy')$$

The swap map on F_3^{2n} is defined as:

$$S((x, y)) = (y, x) \qquad \text{for all } x, y \in F_3^n.$$

Notice that the Gray image of multiplication by v is the swap of the Gray image.

$$\theta(v(x + vy)) = (y, x) = S(\theta(x + vy)). \tag{3.2.1}$$

Example 3.2.1. *Let $x \in C$ over R such that $x = (v, 1 + v, 2 + v, 2)$.*
Then $\theta(x)$, $S(x)$, $\theta(v(x))$ and $S(\theta(x))$ as following :
$\theta(v, 1 + v, 2 + v, 2) = ((0, 1), (1, 1), (2, 1), (2, 0))$,
$S(v, 1 + v, 2 + v, 2) = ((1, 0), (1, 1), (1, 2), (0, 2))$,...*(1)*
$\theta(v(x)) = \theta(1, v + 1, 2v + 1, 2v) = ((1, 0), (1, 1), (1, 2), (0, 2))$..............................*(2)*
Form (1) and (2) we noticed that (3.2.1) achieved.

Definition 3.2.2. The Hamming weight of a codeword is the number of nonzero components.

Definition 3.2.3. The Lee weight for a codeword $x = (x_1, x_2, ..., x_n) \in R^n$ is defined by, $wt_L(x) = \sum_{i=1}^{n} wt_L(x_i)$, where

$$wt_L(x_i) = \begin{cases} 0 & \text{if } x_i = 0 \\ 1 & \text{if } x_i = 1, 2, v, \text{ or } 2v \\ 2 & \text{if } x_i = 1 + v, 2 + v, 1 + 2v \text{ or} 2 + 2v. \end{cases}$$

Definition 3.2.4. The Bachoc weight is given by the relation $wt_B(x) = \sum_{i=1}^{n} wt_B(x_i)$, where

$$wt_B(x_i) = \begin{cases} 0 & \text{if } x_i = 0 \\ 1 & \text{if } x_i = 1 + v, 2 + v, 1 + 2v \text{ or} 2 + 2v \\ 3 & \text{if } x_i = 1, 2, v, \text{ or } 2v. \end{cases}$$

Example 3.2.2. *Find the Lee and Bachoc weight of the codeword $x = (v, 2+2v, 2+v, 1+v, 0, 1 + v, 2v, 2)$.*
Solution :

$wt_L(x) = 1+2+2+2+0+2+1+1 = 11.$
$wt_B(x) = 3+1+1+1+0+1+3+3 = 13.$

3.2.2 Structure and duality of codes over $R = F_3 + vF_3$

By the properties of CRT any code over R_3 is permutation-equivalent to a code generated by the following matrix:

$$\begin{bmatrix} I_{k_1} & (1-v)B_1 & (1+v)A_1 & (1+v)A_2+(1-v)B_2 & (1+v)A_3+(1-v)B_3 \\ 0 & (1+v)I_{k_2} & 0 & (1+v)A_4 & 0 \\ 0 & 0 & (1-v)I_{k3} & 0 & (1-v)B_4 \end{bmatrix}.$$

Where A_i and B_j are ternary matrices. Such a code is said to have rank $\{9^{k_1}, 3^{k_2}, 3^{k_3}\}$. If H is a code over R_3, Let H^+(resp. H^-) be the ternary code such that $(1+v)H^+$(resp. $(1-v)H^-$) is read H mod $(1-v)$ (resp. H mod $(1+v)$).
We have

$$H = (1+v)H^+ \oplus (1-v)H^-.$$

With

$$H^+ = \{s | \exists t \in F_3^n | (1+v)s + (1-v)t \in H\}.$$

$$H^- = \{t | \exists s \in F_3^n | (1+v)s + (1-v)t \in H\}.$$

The code H^+ is permutation equivalent to a code with generator matrix of the form :

$$\begin{bmatrix} I_{k_1} & 0 & 2A_1 & 2A_2 & 2A_3 \\ 0 & I_{k_2} & 0 & A_4 & 0 \end{bmatrix},$$

where A_i are ternary matrices. And the ternary code H^- is permutation-equivalent to a code with generator matrix of the form:

$$\begin{bmatrix} I_{k_1} & 2B_1 & 0 & 2B_2 & 2B_3 \\ 0 & 0 & I_{k_3} & 0 & B_4 \end{bmatrix},$$

where B_i are ternary matrices.

Theorem 3.2.2. *[18] Let H be a code of length n over R_3, with associated ternary codes H^+ and H^- then for the Hermitian scaler product :*

$$H^\perp = (1+v)(H^-)^\perp \oplus (1-v)(H^+)^\perp \quad ,$$

and the self-dual codes over R_3 are the codes over H with associated ternary codes H^+ and H^- verifying $H^+ = (H^-)^\perp$.

Proof. Observe that if c, c', d, d' are ternary vectors of length n then

$$(c(1-v) + d(1+v))\overline{(c'(1-v) + d'(1+v))} = a(1-v) + b(1+v)$$

with $-a = cd'$ and $-b = dc'$. This shows that $a = b = 0$ iff $dc' = cd' = 0$. $\square$

Theorem 3.2.3. *[18] Let H be a code of length n over R_3, with associated ternary codes H^+ and H^- then for the Euclidean scalar product :*

$$H^\perp = (1+v)(H^+)^\perp \ \oplus (1-v)(H^-)^\perp$$

and the self-dual codes over R_3 are the codes over H with associated ternary codes H^+ and H^- such that H^+ and H^- are self-dual ternary codes.

Proof. Observe that if c, c', d, d' are ternary vectors of length n then

$$(c(1-v) + d(1+v))(c'(1-v) + d'(1+v)) = a(1-v) + b(1+v)$$

with $-a = cc'$ and $-b = dd'$. This shows that $a = b = 0$ iff $cc' = dd' = 0$. $\square$

Proposition 3.2.4. *An $R-$code H is self-dual for both the Hermitian and Euclidean scalar product if and only if it is self-conjugate. In particular, it is the $R-$span of a ternary matrix the F_3-span of which is self-dual.*

Some codes over R for the lengths n = 4, 6, 8, 9, 10, 11, 12, 13, 14 and 15, Hermitian self-dual and have a minimum length weight of 9 are found in [18].

Chapter 4

Simplex code over the ring $R = F_2 + vF_2$

There are various binary linear codes such as the **Hamming codes**, the first order **Reed Muller codes** and the **simplex codes**. Any nonzero codeword of the simplex code has many of the properties that we would expect from a sequence obtained by tossing a fair coin $2^m - 1$ times. This randomness makes these codewords very useful in number of applications such as range-finding, synchronizing, modulation scrambling etc. Hamming code is the dual of the simplex code. All these codes have been generalized to codes over the Galois fields $GF(q)$. Recently, there has been much interest in codes over finite rings, especially the rings Z_{2^s}, where Z_{2^s} denotes the ring of integers modulo 2^s. In particular, codes over $\mathbb{Z}_4$ and $\mathbb{F}_2 + u\mathbb{F}_2$ have been widely studied [6], [11], [22], [24] and [29].
More recently Z_4-simplex codes and their Gray images have been investigated by M. Bhandari, A. Lal and M. Gupta in [11]. Good binary linear and non-linear codes can be obtained from codes over Z_4 via the Gray map. In [15] Gupta, Clyun and Gulliver studied senary simplex codes over Z_6 of type α and two versions of types (β and γ), self-orthogonality, torsion codes weight distribution and weight hierarchy properties are investigated. They gave a new construction of senary codes via their binary and ternary counter part and show that types α and β simplex codes can be constructed by this method. In [13] and [14] respectively, simplex codes of types α and β over the rings $\mathbb{F}_2+u\mathbb{F}_2$ where $u^2 = 0$ and the ring $\sum_{n=0}^{n=s} u^n\mathbb{F}_2$ were given by generalizations and extensions of simplex codes over $\mathbb{Z}_4$ and over $\mathbb{Z}_{2^s}$. In this chapter, we describe linear simplex codes and their properties over the ring $R = \mathbb{F}_2 + v\mathbb{F}_2$ where $v^2 = v$ and $\mathbb{F}_2 = \{0, 1\}$.

4.1 Simplex code over fields

All information in this section are found in [7] and [29].

The Hamming code is probably the most famous of all error-correcting codes. They are perfect, linear and very easy to decode. The binary Hamming code is equivalent to a cyclic code. **The Hamming** code, C_H of length $n = (q^{k-1})/(q-1), k \geq 1$ over F_q, is a code for which the $k \times n$ parity check matrix H has columns that are pairwise linearly independent. Since H has rank k, C_H is linear of dimension $n-k$. Moreover, any codeword $x \in C_H$ is a linear combination of $wt(x)$ columns of H. As a result, $wt(C_H) = 3$ since their exist at least three, but not fewer, linearly dependent columns of H.

Definition 4.1.1. [29] Hamming binary codes Let $n = 2^k - 1$ with $k \geq 2$. Then the $k \times (2^k - 1)$ matrix C_H whose columns in order are numbers $1, 2, ..., 2^k - 1$ written as binary numerals in the parity check matrix of an $[n = 2^k - 1, k = n - k]$.

Theorem 4.1.1. *[29] and [7] Any $[(q^k - 1)/(q-1), (q^k - 1)/(q-1) - k, 3]$ code over F_q is monomially equivalent to Hamming code C_H*

Example 4.1.1. *[7] Let us consider the 4×15 matrix*

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

H can be used as a parity check matrix to define the binary Hamming code C_H of length 15 with 2^4 words. The codeword

$$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$$

has weight 3.Naturally , H is the generator matrix of the dual code of C_H, which has length 15 and dimension 4 such a code is called a projective code since the columns of the generator matrix represent distinct points in the three dimensional projective space over F_2 . More generally, the dual of a Hamming code is a simplex (projective as in [7]) code.

Definition 4.1.2. [29] The dual of Hamming codes are called simplex codes. They are $[(q^k - 1)/(q-1), k]$, whose codeword weight have a rather, interesting property. The tetra code, being a self-dual Hamming code, is a simplex code its nonzero codeword all have weight 3.

In general, we have the following theorem.

Theorem 4.1.2. *[29] The nonzero codewords of the* $[(q^k-1)/(q-1),k]$ *simplex code over* F_q *all have weights* q^{k-1}.

These codes are produced by a modification of the $(u|u+v)$ construction. For more details see [29] section 1.5.5 . For example :
Let G_2 be the matrix

$$G_2 = \left[\begin{array}{c|c|c} 0 & 1 & 1 \\ \hline 1 & 0 & 1 \end{array}\right].$$

Let G_3 be the matrix

$$G_3 = \left[\begin{array}{ccc|c|ccc} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ \hline 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}\right].$$

For $k \geq 3$ define G_k inductively by

$$\left[\begin{array}{c|c|c} 0\cdots 0 & 1 & 1\cdots 1 \\ \hline & 0 & \\ G_{k-1} & \vdots & G_{k-1} \\ & 0 & \end{array}\right].$$

For example

$$G_4 = \left[\begin{array}{ccccccc|c|ccccccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}\right].$$

By the previous theorem, all nonzero codewords have weight 8.

We claim the code S_k, generated by G_k, is the dual of C_H, clearly G_k has one more row than G_{k-1} and as G_2 has 2 rows G_k has k rows.

Definition 4.1.3. [11] Let $F_q = GF(q) = \{0, 1, \alpha_3, ..., \alpha_q\}$ for a given k and q, Let $G_k(q)$ be a $K \times (q^k - 1)/(q - 1)$ matrix over F_q in which any two columns are linearly independent.
The code $S_k(q)$, generated by the matrix $G_k(q)$ is called the simplex code.Note that $S_k(q)$ a $\left[\ (q^k - 1)/(q - 1), k, q^{k-1} \ \right]$.
It is known that any linear code with the above parameters is equivalent to $S_k(q)$.
$G_k(q)$ can be defined inductively by

$$G_2(q) = \begin{bmatrix} 0 & 1 & 1 & \alpha_3 & \cdots & \alpha_{q-1} & \alpha_q \\ 1 & 0 & 1 & 1 & \cdots & 1 & 1 \end{bmatrix},$$

and

$$G_k(q) = \left[\begin{array}{c|c|c|c|c|c} 000\cdots0 & 1 & 11\cdots1 & \alpha_3\alpha_3\cdots\alpha_3 & \cdots & \alpha_q\cdots\alpha_q \\ \hline G_{k-1}(q) & 0 & G_{k-1}(q) & G_{k-1}(q) & \cdots & G_{k-1}(q) \end{array}\right].$$

every nonzero codeword of $S_k(q)$ has weight q^{k-1}.
The binary simplex code usually denoted by S_k was first discovery by Ronald A. Fisher in 1942 in connection with statistical designs. In 1945 it was further generalized to arbitrary prime powers.

4.2 R-Simplex codes of type α over $F_2 + vF_2$

Following [11], [13], and [14]. We construct simplex codes over the ring $R = F_2 + vF_2$ in the following way.
For convenience we set $w = 1 + v$. Let G_k be a $k \times 2^{2k}$ matrix over R defined inductively by.

$$\left[\begin{array}{c|c|c|c} 00\cdots0 & 11\cdots1 & vv\cdots v & ww\cdots w \\ \hline G_{k-1} & G_{k-1} & G_{k-1} & G_{k-1} \end{array}\right], \tag{4.2.1}$$

where $G_1 = (01vw)$.
The columns of G_k consists of all distinct $k-$ tuples over R. The code, S_k^α generated by G_k, has length 2^{2k}.
The following observation are useful to obtain Hamming, Lee, Bachoc and distribution weights of S_k^α.

Remark 4.2.1. If A_{k-1} denotes the $(4^{k-1} \times 4^{k-1})$ array consisting of all codewords in S^{α}_{k-1} and

$\mathbf{i} = (i, i, ..., i)$ then the $(4^k \times 4^k)$ array of codewords of S^{α}_k is given by

$$\begin{bmatrix} A_{k-1} & A_{k-1} & A_{k-1} & A_{k-1} \\ A_{k-1} & \mathbf{1} + A_{k-1} & \mathbf{v} + A_{k-1} & \mathbf{w} + A_{k-1} \\ A_{k-1} & \mathbf{v} + A_{k-1} & \mathbf{v} + A_{k-1} & A_{k-1} \\ A_{k-1} & \mathbf{w} + A_{k-1} & A_{k-1} & \mathbf{w} + A_{k-1} \end{bmatrix}.$$

Example 4.2.1. *To construct the simplex code S_2.*

By (4.2.1) we write

$$G_2 = \left[\begin{array}{c|c|c|c} 0000 & 1111 & vvvv & wwww \\ 01vw & 01vw & 01vw & 01vw \end{array}\right].$$

Then,

$$S_2 = \begin{bmatrix} 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&1&1&1&v&v&v&v&w&w&w&w \\ 0&1&v&w&0&1&v&w&0&1&v&w&0&1&v&w \\ 0&1&v&w&1&0&w&v&v&w&0&1&w&v&1&0 \\ 0&0&0&0&v&v&v&v&v&v&v&v&0&0&0&0 \\ 0&0&0&0&w&w&w&w&0&0&0&0&w&w&w&w \\ 0&1&v&w&v&w&0&1&v&w&0&1&0&1&v&w \\ 0&1&v&w&w&v&1&0&0&1&v&w&w&v&1&0 \\ 0&v&v&0&0&v&v&0&0&v&v&0&0&v&v&0 \\ 0&v&v&0&1&w&w&1&v&0&0&v&w&1&1&w \\ 0&v&v&0&v&0&0&v&v&0&v&0&0&v&v&0 \\ 0&v&v&0&w&1&1&w&0&v&v&0&w&1&1&w \\ 0&w&0&w&0&w&0&w&0&w&0&w&0&w&0&w \\ 0&w&0&w&1&v&1&v&v&1&v&1&w&0&w&0 \\ 0&w&0&w&v&1&v&1&v&1&v&1&0&w&0&w \\ 0&w&0&w&w&0&w&0&0&w&0&w&w&0&w&0 \end{bmatrix}$$

wt_H	wt_L	wt_B
0	0	0
12	16	20
12	16	20
12	16	20
8	8	16
8	8	16
12	16	20
12	16	20
8	8	16
12	16	20
8	8	16
12	16	20
8	8	16
12	16	20
12	16	20
8	8	16

the length of $S_2 = 2^{2k} = 2^4 = 16$.

$d_H = d_L = 8$ *and* $d_B = 16$.

Remark 4.2.2. If $R_1,\ R_2, ..., R_k$ denote the rows of the matrix G_k^{α} then,

- $wt_H(R_i) = 3 \cdot 2^{2(k-1)},\ \ wt_H(vR_i) = wt_H(wR_i) = 2^{2k-1}$.
- $wt_L(R_i) = 2^{2k},\ wt_L(vR_i) = wt_L(wR_i) = 2^{2k-1}$.
- $wt_B(R_i) = 5.2^{2(k-1)},\ wt_B(vR_i) = wt_B(wR_i) = 2^{2k}$.

It may be observed that each element of R occurs equally often in every row of G_k^{α}.
Let $c = (c_1, c_2, ..., c_n) \in C$. For each $j \in R$, Let $w_j(c) = |\{i|c_i = j\}|$, we have the following lemma.

Lemma 4.2.1. *Let* $c \in S_k^{\alpha},\ c \neq 0$

1) If for at least one $i,\ c_i$ *is a unit then* $\forall j \in R,\ \omega_j = 4^{k-1}$ *in* c.

2) If $\forall\ i,\ c_i \in \{0, v\}$ *then* $\forall j \in \{0, v\}\ \omega_j = 2^{2k-1}$ *in* c.

3) If $\forall\ i,\ c_i \in \{0, w\}$ *then* $\forall j \in \{0, w\}\ \omega_j = 2^{2k-1}$ *in* c.

Proof. By Remark (4.2.1), any $x \in S_{k-1}^{\alpha}$ gives rise to the following four codewords of S_k^{α}.

$y_1 = (x|x|x|x)$.

$y_2 = (x|\ \mathbf{1} + x|\ \mathbf{v} + x|\ \mathbf{w} + x)$.

$y_3 = (x|\ \mathbf{v} + x|\ \mathbf{v} + x|x)$.

$y_4 = (x|\ \mathbf{w} + x|\ \mathbf{w} + x|x)$.

Hence, by induction, the assertion follows. □

Now we will give some facts about binary simplex codes.
Let $G(S_k)$ (columns consists of all nonzero binary k-tuples) be the generator matrix for an $[n, k]$ binary simplex code S_k. Then the extended binary simplex code $\widehat{S}_k$ generated by the matrix.

$$G(\widehat{S}_k) = [\mathbf{0}|G(S_k)].$$

Inductively generated by,

$$G(\widehat{S}_k) = \left[\begin{array}{c|c} 00\cdots0 & 11\cdots1 \\ G(\widehat{S}_{k-1}) & G(\widehat{S}_{k-1}) \end{array}\right],\quad \text{with } G(\widehat{S}_1) = [0\ 1]. \tag{4.2.2}$$

Lemma 4.2.2. *The H^+(or H^-) binary codes of S_k^α are equivalent to the 2^k copies of $\widehat{S}_k$.*

Proof. First, we will prove the H^+ case by induction on k. Observe that the binary H^+ code of S_k^α is the set of codewords obtained by replacing w by 1 in all $w-$ linear combination of the rows of the matrix wG_k (where G_k is defined in (4.2.1). For $k=2$ the result holds and.

$$G_2 = \left[\begin{array}{c|c|c|c} 0000 & 1111 & vvvv & wwww \\ 01vw & 01vw & 01vw & 01vw \end{array}\right].$$

$$H^+ = \left[\begin{array}{c|c|c|c} 0000 & 1111 & 0000 & 1111 \\ 0101 & 0101 & 0101 & 0101 \end{array}\right].$$

If wG_{k-1} is permutation equivalent to 2^{k-1} copies of $wG(\widehat{S}_{k-1})$ then the matrix wG_k takes the form:

$$\left[\begin{array}{c|c|c|c} 00\cdots0 & ww\cdots w & 00\cdots0 & ww\cdots w \\ \hline wG(\widehat{S}_{k-1})|\cdots|wG(\widehat{S}_{k-1}) & wG(\widehat{S}_{k-1})|\cdots|wG(\widehat{S}_{k-1}) & wG(\widehat{S}_{k-1})|\cdots|wG(\widehat{S}_{k-1}) & wG(\widehat{S}_{k-1})|\cdots|wG(\widehat{S}_{k-1}) \end{array}\right].$$

Now regrouping the columns according to (4.2.2) gives the desired result. The proof for the H^- case is similar to the above case. □

Definition 4.2.1. For each $1 \leq i \leq n$, let $A_H(i)(A_L(i)$ or $A_B(i))$
be the number of codewords of Hamming, Lee or Bachoc weight i in C.
Then $\{A_H(0), A_H(1), ..., A_H(n)\}, (\{A_L(0), A_L(1), ..., A_L(n)\})$ or
$(\{A_B(0), A_B(1), ..., A_B(n)\})$ is called the Hamming (Lee) or Bachoc weight distribution of C.

The Hamming, Lee and Bachoc weight distributions of S_k^α are given in the following theorem.

Theorem 4.2.3. *Hamming, Lee and Bachoc weight distributions of S_k^α are:*

1.) $A_H(0) = 1,\ A_H(2^{2k-1}) = 2(2^k-1)$ *and* $A_H(3.2^{2(k-1)}) = (2^k-1)(2^k-1)$.

2.) $A_L(0) = 1,\ A_L(2^{2k-1}) = 2(2^k-1)$ *and* $A_L(4^k) = (2^k-1)(2^k-1)$.

3.) $A_B(0) = 1,\ A_B(4^k) = 2(2^k-1),\ A_B(5.2^{2(k-1)}) = (2^k-1)(2^k-1)$.

Proof. **Note** that $A_H(0) = A_L(0) = A_B(0) = 1$, $A_H(2^{2k-1}) = A_L(2^{2k-1}) = A_B(4^k) = 2(2^k-1)$ and $A_H(3\cdot 2^{2(k-1)}) = A_L(4^k) = A_B(5\cdot 2^{2(k-1)}) = (2^k-1)(2^k-1)$. By remark (4.2.2), each nonzero codeword of S_k^α has Hamming weight is either $3\cdot 2^{2(k-1)}$ or 2^{2k-1}, Lee weight is either 4^k or 2^{2k-1} and Bachoc weight is either $5\cdot 2^{2(k-1)}$ or 4^k. And by

Lemma (4.2.2), the dimension of H^+ code of S_k^α is k, thus the number of codewords is 4^k and there will be $(2^k-1)(2^k-1)$ codewords of Hamming weight $3 \cdot 2^{2(k-1)}$. Therefore, the number of codewords having Hamming weight 2^{2k-1} is $4^k - [(2^k-1)(2^k-1)+1] = 4^k - [2^{2k} - 2 \cdot 2^k + 1 + 1] = 4^k - 4^k + 2 \cdot 2^k - 2 = 2 \cdot 2^k - 2 = 2(2^k-1)$. Similar arguments hold for the other weights. $\square$

The symmetrized weight enumerator (swe) of S_k^α is given by the following formula,

$$swe(x,y,z) = x^n + 3^{2(k-1)} x^{4^{k-1}} y^{4^{k-1}} z^{2^{2k-1}} + 2 \cdot 3^{k-1} x^{2^{2k-1}} z^{2^{2k-1}}$$

Remark 4.2.3.

1 The Simplex code S_k^α is not equidistant with respect to Hamming, Lee and Bachoc distances.

2 The minimum weights of S_k^α are:$d_H = 2^{2k-1},\ d_L = 2^{2k-1}$ and $d_B = 2^{2k}$.

3 $d_H = d_L = d_B/2$.

4.3 Simplex codes of type β

The length of S_k^α is large and increases fast, so we can omit some columns from G_k^α to obtain good codes over R of smaller length and we will call the simplex codes of type β. Let λ_k be the $k \times 2^k(2^k-1)$ matrix defined inductively by $\lambda_1 = [1v]$ and

$$\lambda_k = \left[\begin{array}{c|c|c|c} 00\cdots0 & 11\cdots1 & vv\cdots v & ww\cdots w \\ \lambda_{k-1} & G_{k-1}^\alpha & G_{k-1}^\alpha & \lambda_{k-1} \end{array}\right], \tag{4.3.1}$$

for $k \geq 2$ and let δ_k be the $k \times 2^k(2^k-1)$ matrix defined inductively by $\delta_1 = [1w]$ and

$$\delta_k = \left[\begin{array}{c|c|c|c} 00\cdots0 & 11\cdots1 & vv\cdots v & ww\cdots w \\ \delta_{k-1} & G_{k-1}^\alpha & \delta_{k-1} & G_{k-1}^\alpha \end{array}\right], \tag{4.3.2}$$

For $k \geq 2$ where G_{k-1}^α is the generator matrix of S_{k-1}^α.
Now let G_k^β be the $k \times [(2^k-1)(2^k-1)]$ matrix defined inductively by

$$G_2^\beta = \left[\begin{array}{c|c|c|c} 1111 & 0 & vv & ww \\ 01vw & 1 & 1w & 1v \end{array}\right],$$

And for $k > 2$.

$$G_k^\beta = \left[\begin{array}{c|c|c|c} 11\cdots 1 & 00\cdots 0 & vv\cdots v & ww\cdots w \\ G_{k-1}^\alpha & G_{k-1}^\beta & \delta_{k-1} & \lambda_{k-1} \end{array}\right]. \tag{4.3.3}$$

Note that the generator matrix G_k^β is obtained by deleting $2^{k+1}-1$ columns of the generator matrix G_k^α. By induction, it is easy to verify that no two columns of G_k^β are multiple of each other.
Now, let S_k^β be the code generated by G_k^β; to determine the weight distribution of S_k^β, we first make the following observations.

Remark 4.3.1. Each row of G_k^β has Hamming weight $2^{k-2}[3(2^k-1)-1]$, Lee weight $2^k(2^k-1)$ and Bachoc weight $2^k[2(2^{k-1}-1)+2^{k-2}]$.

Proposition 4.3.1. *Each row of G_k^β contains $2^{2(k-1)}$ units and*

$$\omega_v = \omega_w = 2^{2(k-1)} - 2^{k-1} = 2^{k-1}(2^{k-1}-1).$$

Proof. The result can be easily verified for $k = 2$. Assume that the result holds for each row of G_{k-1}^β. Then the number of units in each row of G_{k-1}^β is equal $2^{2(k-2)}$. By Lemma (4.2.1), the number of units in any row of G_{k-1}^α is 2^{2k-3}. Hence, the total number of units in any row of G_k^β will be $2^{2k-3} + 2\cdot 2^{2(k-2)} = 2^{2(k-1)} = 4^{k-1}$. A similar argument holds for the number of $v's$ and $w's$. □

Example 4.3.1. *Construction of S_2^β, the length, d_H, d_L and d_B for this code as the following:*

By (4.3.3) we can write

$$S_2^{\beta} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & v & v & w & w \\ 0 & 1 & v & w & 1 & 1 & w & 1 & v \\ 1 & 0 & w & v & 1 & w & 1 & v & 1 \\ v & v & v & v & 0 & v & v & 0 & 0 \\ w & w & w & w & 0 & 0 & 0 & w & w \\ v & w & 0 & 1 & 1 & w & 1 & 1 & v \\ w & v & 1 & 0 & 1 & 1 & w & v & 1 \\ 0 & v & v & 0 & v & v & 0 & v & v \\ 0 & w & 0 & w & w & w & w & w & 0 \\ 1 & w & w & 1 & v & 0 & v & 1 & 1 \\ 1 & v & 1 & v & w & 1 & 1 & 0 & w \\ v & 0 & 0 & v & v & 0 & v & v & v \\ v & 1 & v & 1 & w & 1 & 1 & w & 0 \\ w & 0 & w & 0 & w & w & w & 0 & w \\ w & 1 & 1 & w & v & v & 0 & 1 & 1 \end{bmatrix}$$

wt_H	wt_L	wt_B
0	0	0
8	12	12
8	12	12
8	12	12
6	6	12
6	6	12
8	12	12
8	12	12
6	6	12
6	6	12
8	12	12
8	12	12
6	6	12
8	12	12
6	6	12
8	12	12

The length $n = 9$.

$d_H = 6, d_L = 6, d_B = 12.$

Example 4.3.2. *To find the length,* d_H, d_L *and* d_B *for the code* C *with the generator matrix* G_3^{β}.

Solution:

By (4.3.1) and (4.3.2) we can write

$$\lambda_2 = \left[\begin{array}{c|c|c|c} 00 & 1111 & vvvv & ww \\ 1v & 01vw & 01vw & 1v \end{array}\right].$$

$$\delta_2 = \left[\begin{array}{c|c|c|c} 00 & 1111 & vv & wwww \\ 1w & 01vw & 1w & 01vw \end{array}\right].$$

By (4.3.3):

$$G_3^{B} = \left[\begin{array}{c|c|c|c} 1111111111111111 & 000000000 & vvvvvvvvvvvv & wwwwwwwwwwww \\ 00001111vvvvwwww & 11110vvww & 001111vvwwww & 001111vvvvww \\ 01vw01vw01vw01vw & 01vw11w1v & 1w01vw1w01vw & 1v01vw01vw1v \end{array}\right].$$

In similar way as in previous example we can deduce that the length $n = 49$, $d_H = d_L = 28$, $d_B = 64$

Theorem 4.3.2. *The hamming, Lee and Bachoc weight distributions of S_k^{β} are:*

1. $A_H(0) = 1,\ A_H(2^{k-2}(3(2^k-1)-1)) = (2^k-1)(2^k-1)$.
   and $A_H(2^{k-1}(2^k-1)) = 2(2^k-1)$.

2. $A_L(0) = 1,\ A_L(2^{k-1}(2^k-1)) = 2(2^k-1)$
   and $A_L(2^k(2^k-1)) = (2^k-1)(2^k-1)$.

3. $A_B(0) = 1,\ A_B(2^k[2(2^{k-1}-1)+2^{k-2}]) = (2^k-1)(3+2^{k-1})$.
   and $A_B(2^k(2^k-1)) = 2 \cdot 3^{k-3}(2^k-1)$.

Proof. Similar to the proof of theorem(4.2.3). ☐

Remark 4.3.2.
1. The minimum Hamming weight of S_k^{β}, is $d_H = 2^{k-1}(2^k-1)$.
2. The minimum Lee weight of S_k^{β}, is $d_L = 2^{k-1}(2^k-1)$.
3. The minimum Bachoc weight of S_k^{β}, is $d_B = 2^k(2(2^{k-1}-1)+2^{k-2})$.

Now we will give the Macwilliams relations of S_k^{β}

Remark 4.3.3.

$$W_c(x,y) = x^n + q(k)x^{n-h(k)}y^{h(k)} + nx^{n-f(k)}y^{f(k)}$$

where $q(k) = 2(2^k-1),\ h(k) = 2^{k-1}(2^k-1),\ f(k) = 2^{k-2}(3(2^k-1)-1)$.

$$swe(x,y,z) = x^n + nx^{\rho(k)}y^{\delta(k)}z^{n-\rho(k)-\delta(k)} + 2(2^k-1)x^{n-h(k)}z^{h(k)}$$

where $n = L(k) = (2^k-1)(2^k-1),\ h(k) = 2^{k-1}(2^k-1),\ \rho(k) = L(k-1) = (2^{k-1}-1)(2^{k-1}-1)$ and $\delta(k) = 2^{2(k-1)}$.

Example 4.3.3.

Remark 4.3.4.

1.) $S_k^{\alpha}(S_k^{\beta})$ are Hermitian self-orthogonal codes

2.) S_k^{α} is self-orthogonal codes with Euclidean inner product, but S_k^{β} is not.

3.) The $S_k^{\alpha}(S_k^{\beta})$ codes dose not achieve the inequality

$$d_B \leq 2(1 + \lfloor \frac{n}{3} \rfloor).$$

and so they are not Hermitian self-dual codes.

4.) The S_K^{α} has $d_H = d_L = d_B/2$.

5.) The S_K^{β} has $d_H = d_L \leq d_B/2$.

Appendix A

Fundamental terminology in ring theory

The following facts are found in [3], [7] and [29]

Ring: A non-empty set R together with two binary operations $(+)$ and $(.)$ called addiction and multiplication respectively, is called a ring, if it has the following three properties .

1) $(R, +)$, is an abelian group,

2) $(R, .)$, is a semi-group and

3) distributive laws hold.

To spell out these conditions, we have the following.

1)Abelian Group **a)** $a, b \in R \Rightarrow a + b \in R$.

b) $a, b, c \in R \Rightarrow (a + b) + c = a + (b + c)$.

c) $\exists\ 0_R \in R$ such that $a + 0_R = a = 0_R + a, \forall a \in R$.

(Such an 0_R is unique and is called the additive identity or the zero element. This 0_R is denoted simply by 0, since no confusion is likely).

d) $\forall a \in R, \exists\ b \in R$ such that $a + b = 0 = b + a$.(such a b is unique and is denoted by $-a$).

e) $\forall a, b \in R, a + b = b + a$.

2)Semi-group

f) $a, b \in R \Rightarrow a.b \in R$

g) $a, b, c \in R \Rightarrow (a.b).c = a.(b.c)$.

3)Distributive laws

h) $\forall a,b,c \in R, \begin{cases} a.(b+c) = a.b + a.c & ; \\ (a+b).c = a.c + b.c & . \end{cases}$

Basic notations :

1) We recall that R is a commutative ring with unity, if a semi-group $(R,.)$ is commutative and has an identity ($\mathbf{1}_R$ or $\mathbf{1}$)

2) An invertible element (unit) $a \in R$ is an element for which their exist a $b \in R$ such that $ab = 1$. The element b is uniquely determined by a and will be denoted by a^{-1}.

3) A ring R is a field if every nonzero element is a unit.

4) A non-empty subset S of R is called a subring of R, if $(S,+)$ is a subgroup of $(R,+)$ and $(S,.)$ is a subsemi-group of $(R,.)$.

5) An element $a \in R$ is said to be a zero divisor if a is either a left zero divisor or a right zero divisor, i.e (if $\exists\ b \neq 0, \ni a.b = 0$ or $\exists\ c \neq 0, \ni c.a \neq 0$).

6) An element $a \in R$ is a nilpotent if $a^n = 0$ for some positive integer n.

7) Provided that R is not the trivial ring a nilpotent is a zero divisor in R, but the converse not generally true.

8) An element $a \in R$ is said to be an idempotent if $a^2 = a$. Two idempotents $a, b \in R$ are said to be orthogonal (to each other) if $ab = 0$.

9) For R has unity and $a$is an idempotent then, $1-a$ is also an idempotent and a and $1-a$ are orthogonal.

10) Given a ring R (commutative or not, with or without unity) by the characteristic of (R) we mean the least positive integer n such that $na = 0, \forall a \in R$, if this n dose not exist then $char(R) = 0$.

11) If R is commutative ring whose characteristic is a prime p then $(a+b)^p = a^p + b^p$ for all a, b in R.

12) An ideal I in a commutative ring R is a non empty subset of the ring that is closed under subtraction such that the product of an element of I with an element of R is always in R. I is a proper ideal if $\{0\} \neq I \subset R$, and this I dose not contain units.

13) A (proper) ideal, I, of R is said to be a prime ideal if, for any $a, b \in R$ such that $a.b \in I$ and $a \notin I, b \in I$.

14) A proper ideal M in R is called maximal ideal, if there is no proper ideal of R, say J such that $M \subset J \subset R$.

15) The ideal $M \subset R$ (commutative ring) is maximal if and only if $R \backslash M$ is a field.

16) In a commutative ring with identity, a maximal ideal is a prime ideal.

17) Let R be a ring with **1**, and $M \neq \langle 0 \rangle$ an ideal such that $x \in R \backslash M$ is a unit then R is a local ring, and M is its unique maximal ideal.

18) A commutative ring with **1** is called a semi-local ring if it has only finitely many maximal ideals.

Module: **1)** Let R be any ring (with or without **1** and commutative or not). By a left $R-$Module M, we mean, an abelian group $(M, +)$ together with a map $R \times M \longrightarrow M, (a, x) \longrightarrow ax$, such that

1) $a(x + y) = ax + ay, \forall a \in R$ and $x, y \in M$,

2) $(a + b)x = ax + bx, \forall a, b \in R$ and $x, y \in M$ and

3) $(ab)x = a(bx), \forall a, b \in R$ and $x, y \in M$.

Elements of R are called scalers.

Submodule: Let M be an $R-$module. A non-empty subset N of M is called $R-$submodule of M if

1) N is an additive subgroup of M, i.e $a, b \in N \Rightarrow a - b \in N$ and

2) N is closed for scaler multiplication i.e $x \in N, a \in R \Rightarrow ax \in N$.

Free module: An $R-$module M is called a free module if M has a basis B, i.e., a linearly independent subset B of M such that M is spanned by B over R.

$R^n = R \times ......R$, n times is a free R-module if R has **1**

Appendix B

Linear Algebra

In this appendix we review several important concepts from linear algebra, for more details see [20] and [4].

A vector space: Let F_q be the finite field of order q. A nonempty set V, together with some (vector) addition (+) and scalar multiplication by elements of F_q, is a vector space (or linear space) over F_q if it satisfies all the following conditions. For all $u, v, w \in V$ and for all $\lambda, \mu \in F_q$:

1) $u + v \in V$;

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

3) there is an element $0 \in V$ with the property $0 + v = v = v + 0$ for all $v \in V$;

4) for each $u \in V$ there is an element of V, called $-u$,such that $u+(-u) = 0 = (-u)+u$;

5) $u + v = v + u$;

6) $\lambda v \in V$;

7) $\lambda(u + v) = \lambda u + \lambda v, (\lambda + \mu)u = \lambda u + \mu u$;

8) $(\lambda\mu)u = \lambda(\mu u)$;

9) if 1 is the multiplicative identity of F_q, then $1u = u$.

Subspace: A nonempty subset C of a vector space V over F_q if and only if the following condition is satisfied:

$$if\ x, y \in C\ and\ \lambda, \mu \in F_q\ ,\ then\ \ \lambda x + \mu y \in C.$$

Linearly independent: A set of vectors $\{v_1, v_2, ..., v_k\}$ in V is linearly independent if

$$\lambda_1 v_1 + \lambda_2 v_2 + ... + \lambda_k v_k = 0 \Rightarrow \lambda_1 = \lambda_2 = ... = \lambda_k = 0.$$

The set is linearly dependent if it is not linearly independent; i.e., if there are $\lambda_1, \lambda_2, ..., \lambda_k \in F_q$, not all zero (but maybe some are!), such that $\lambda_1 v_1 + \lambda_2 v_2 + ... + \lambda_k v_k = 0$.
Note that: The number of linearly independent rows in a matrix is equal to the number of linearly independent columns.

Examples:

1) Any set S which contains 0 is linearly dependent.

2) For any $F_q, \{(0,0,0,1),(0,0,1,0),(0,1,0,0)\}$ is linearly independent.

3) For any $F_q, \{(0,0,0,1),(1,0,0,0),(1,0,0,1)\}$ is linearly dependent.

Basis: a nonempty subset B of vectors from a vector space V is a basis for V if both:

1) B spans $V(thatis, \langle B\rangle = V)$, and

2) B is a linearly independent set.

In general a vector space usually has many bases for a vector space contain the same number of elements. The number of elements in any basis for a vector space is called the dimension of the space.
Rank: The rank of a matrix over F_q is the number of nonzero rows in any REF(reduced echelon form) of the matrix.
If A is an $m \times n$ matrix then the subspace of R^n spanned by he row vectors of A is called the row space of A and the subspace of R^m spanned by the column vectors is called the column space of A. Rank(A) is the common dimension of the row space and the column space of a matrix A.
Linear operator: Let X, Y be linear spaces. Then the function,
$L : X \longrightarrow Y$ is called a linear operation if and only if for all $x_1, x_2 \in X$ and all scalars a, b

$$L(ax_1 + bx_2) = aL(x_1) + bL(x_2).$$

Linear functional: L is a linear functional on X if $L : X \longrightarrow R$ is a linear operator.
kernal: If $T : V \longrightarrow W$ is a linear transformation,then the set of vectors in V that maps into 0 is called the kernal of T.
Remarks: If w_1, w_2 are two subspaces of a finite dimensional vector space V, then:

1) $\dim(w_1 + w_2) = \dim w_1 + \dim w_2 - \dim(w_1 \cap w_2)$.

2) If $w_1 \cap w_2 = \{0\}$, we say that the sum $w_1 + w_2$ is a direct sum of w_1 and w_2 and denoted by $w_1 \oplus w_2$.

3) For $\alpha \in w_1 \oplus w_2$, there exist $\alpha_1 \in w_1$ and $\alpha_2 \in w_2$ such that $\alpha = \alpha_1 + \alpha_2$.

If the sum is direct however α_1 and α_2 are uniquely determined by α.

Conclusion

In this thesis we introduced a survey on Types of self-dual codes over rings of order 4 specially the ring $R = F_2 + vF_2$. We also have studied simplex codes of types α and β over the ring $F_2 + vF_2$. This study can be extended to study simplex codes over more rings such as $F_p + vF_p$ where p is prime integer. For future study one can use near rings of four elements to construct simplex codes.

There are some open research problems related to simplex codes:

1) We hope we can study other types of simplex codes.

2) We hope we can find the number of errors which simplex codes of type α and β will detect and correct.

3) We need further investigation about encoding and decoding process.

Bibliography

[1] A.Bonnecaze and P.Udaya *Cyclic codes and self-dual codes over* $F_2 + uF_2$ IEEE Trans.Inform.Theory45(4)1999, pp1250 -1255.

[2] Christine Bachoc *Application of coding theory to the construction of modular Lattices* , J.Combin.Theory Ser.A78(1997)92-119.

[3] C.Musili *Introduction to Ringd and Modules* University of Hyderabad, India. Second Reversed Edition 1994, Narosa Publishing House ISBN 81-7319-037-2.

[4] D.G.Hoffman, D.A.Leonard, C.C.Lindner, K.T.p helps , C.A.Rodger and J.R.Wall *Coding theory The Essentials*, Printed in the United State Of America 1991

[5] E.Bannai, S.Dougherty, M.Harada, and M.Oura, *Type II codes, even unimodular lattices, and Invariant Rings*, IEEE. Transaction On Information Theory Vol.45.no.4,May 1999.

[6] E.M.Rains and N.J.A.Sloane *Self-dual Codes Information.science research AT and labs- research 180 Park Avenue, Florham Park NJ07932-0971*, 19 May 1998.

[7] Gilberto Bibi and Flaminio Flamini, *"Finite commutative rings and their applications"*, Kluwer Academic Publishers 2002.

[8] J.Fields, B.Gaborit, J.Leon, and V.Pless, *All self-dual* Z_4 *codes of length 15 or less are known* IEEE.Trans.Inform.Theory.Vol.44(1998)pp311-323.

[9] K.Betsumya and M.Harada.*Extremal Slef-dual code over* $F_2 \times F_2$, Design, codes and cryptugraphy 28.

[10] K.Betsumya and M.Harada.*Optimal slef-dual code over* $F_2 \times F_2$, IEEE Trans.Inform. Theory 50(2004)pp356-358.

[11] Manish k.Gupta *On some linear codes over* Z_{2^s} (ph. D.Thesis), Departement of Mathimatics, IIT.Kanpur, India July 2000 P.P 1-98.

[12] M.AL-ASHKER Self-dual codes over Z_4 module . PH.D. , AIN Shams University(Cairo, Egypt)and AL-Aqsa University(Gaza, Palestine) 2002

[13] M. AL-Ashker *Simplex codes over* $\mathbb{F}_2 + u\mathbb{F}_2$, The Arabian Journal for Science and engineering, Volum 30, no. 2A, July 2005, pp 277-285.

[14] M. AL-Ashker *Simplex codes over the ring* $\sum_{n=0}^{s} u^n\mathbb{F}_2$, The Turkish Journal of mathematics, Volum 29 (2005), pp 221-233.

[15] Gupta M. K., Glynn D. G. and Gulliver T. A. *On Senary codes*, Lecture notes in computer Science, Vol 2227, pp. 112-121, November 2001.

[16] M. Elatrash, et.al. *linear codes over the ring* Z_4 *using almost greedy algorithm* Islamic university Jornal, (2003) Vol 11 No.1.

[17] P.caborit, *"Mass formulas for self-dual codes over* Z_4 *and* $F_q + uF_q$*"* IEEE Trnsaction on information theory, , Vol.42, No.4, July 1996 pp 1222-1228.

[18] R.Chapman, S.T.Dougherty , P.Gaborit and P.Solé, *"Self-dual coes over* $F_3 + vF_3$*"* Nombres Bordeaux 14 (2002), no. 1, 73–85..

[19] S.Sadek, M.El Atrach and A.Nagi *Codes of constant Lee or Eudidean weight over the ring* $F_2 + uF_2$, Jornal of Agsa University of Gaza (2000):Primary 94B05.

[20] San Ling and Chaoping Xing *coding Theory* , National University of Singapore, Cambridge University, press 2004.

[21] Stevan.Roman *Coding and information theory* , ISBNO 387-97812-7(Springer-verelag New-york), Berlin Heidelberg 1992.

[22] S.T.Dougherty ,Harada M., and Solé P. *Self-dual codes over Rings and the chinese remainder theorem* , Hokkaido mathematical Journal Vol.28(1999), pp. 253-283.

[23] S.T.Doughert, P.Caborit and P.Solè *Self-dual codes over* $F_2 + vF_2$ March 7,2006.

[24] S.T.Dougherty, P.Caborit, M.Harada, A.Munemasa and P.Solé *Type IV self dual codes over rings* , IEEE Trans.Inform.Theory45(1999)2345-230.

[25] S.Dougherty, P.Caborit, M.Hrada, and P.Sole, Member IEEE, *Type II codes over* $F_2 + uF_2$, IEEE trans.Inform.Theory, Vol.45.pp 32-45.Jon 1999.

[26] T.Aaron Gulliver, Senior Member, IEEE, and Masaki Harada, *Construction of optimal Type IV self Self.Dual-Codes over $F_2 + uF_2$*, IEEE trans.Inform.Theory, Vol.45, No.7, November 1999.

[27] T.W.Hungerford, B.R.Halmos, F.W.Gehring and C.C.Moore , 1974 by springer-Verlag New York Inc. printed in the united state of America 98765432.

[28] V.Pless, J.Lean, and J.Fields, *All Z_4 codes of Type II and length 16 are known* J.Combin.Theory Ser.A.Vol.78(1998).

[29] W.Cary Huffman, Vera Pless *Fundemantal Of Error Correcting Codes* printed in the United Kingdom Cambridge University Pres 2003.