REPUBLIC OF TURKEY
YILDIZ TECHNICAL UNIVERSITY
GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

QUANTUM CODES OVER EISENSTEIN-JACOBI INTEGERS

EDA YILDIZ

MSc. THESIS
DEPARTMENT OF MATHEMATICS
PROGRAM OF MATHEMATICS

ADVISER
ASSOC. PROF. DR. FATİH DEMİRKALE

ISTANBUL, 2017

REPUBLIC OF TURKEY
YILDIZ TECHNICAL UNIVERSITY
GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

QUANTUM CODES OVER EISENSTEIN-JACOBI INTEGERS

A thesis submitted by Eda YILDIZ in partial fulfillment of the requirements for the degree of MASTER OF SCIENCE is approved by the committee on 23.05.2017 in Department of Mathematics, Program of Mathematics.

Thesis Adviser

Assoc.Prof. Dr. Fatih DEMİRKALE

Yıldız Technical University

Approved by the Examining Committee

Assoc.Prof. Dr. Fatih DEMİRKALE

Yildiz Technical University ______________________

Assoc.Prof. Dr. Emre KOLOTOĞLU, Member

Yildiz Technical University ______________________

Assoc. Prof. Dr. Sibel ÖZKAN, Member

Gebze Technical University ______________________

ACKNOWLEDGEMENTS

I am thankful to my advisor Assoc. Prof. Dr. Fatih DEMİRKALE for his guidances and suggestions. He helped me about writing an academic paper and led to writing my thesis in more attention. He motivated me not only in this thesis but also in the other academic issues and his support made possible the completion of this thesis.

I also thank to members of my thesis committee Assoc. Prof. Dr. Emre KOLOTOĞLU and Assoc. Prof. Dr. Sibel ÖZKAN for their comments and questions during my thesis defense.

Also, I am indebted to Prof. Dr. İrfan ŞİAP for his valuable comments and suggestions. He guided to determine the topic of my thesis and he did not hesitate to help all time of the day when I need. I have gained much more virtues from him.

I wish thanks to all the members of Department of Mathematics in Yildiz Technical University. They contributed to me for coming to these days and they did not refrain to support about anything. Specially, I also thank to separately each member of Coding Theory seminar group. Moreover, I would like to thanks to my friends who always believe in and motivate me.

The last but not the least, my special thanks go to dear my mother, my father and my sister to give big support both material and spiritual in my student and personal life. Furthermore, they were patient and self-sacrificing from beginning to end of my education.

May, 2017

Eda YILDIZ

TABLE OF CONTENTS

Page

LIST OF SYMBOLS

$\oplus_2$	Addition modulo 2
$\langle \ \vert$	Bra vector
$Z(\mathcal{S})$	Centralizer of $\mathcal{S}$
$V_{\mathcal{S}}$	Code space which is fixed by $\mathcal{S}$
$P(a_i \vert a_j)$	Conditional probability of a_i based on a_j
$dim(C)$	Dimension of C
H^*	Dual space of H
F_q	Finite field with q elements
$d(a,b)$	Hamming distance between a and b
$wt(a)$	Hamming weight of a
$(\vert x_1\rangle)^+$	Hermitian conjugate of $\vert x_1\rangle$
$\langle a \vert b\rangle$	Inner product of a and b
$\cong$	Isomorphism
$\llbracket n,k \rrbracket$	k −dimensional quantum code of length n
$\llbracket n,k,d \rrbracket$	k −dimensional quantum code of length n with minimum distance d
$\llbracket n,k,d;c \rrbracket$	k −dimensional quantum code of length n with minimum distance d and c entangled pairs
$Ker(r)$	Kernel of r
$\vert \ \rangle$	Ket vector
F_q^n	n −dimensional vector space over F_q
$\Vert \ \Vert$	Norm of a vector
$N(\mathcal{S})$	Normalizer of $\mathcal{S}$
$S^{\perp}$	Orthogonal complement of S

P_n	Pauli group acting on n qubits
$\mathbb{C}^q$	q times tensor product of $\mathbb{C}$
$\sim$	Row equivalence of a matrix
$\langle S \rangle$	Spanning set of S
$C(\mathcal{S})$	Stabilizer code which is fixed by $\mathcal{S}$
$S(a)$	Syndrome of a
$\otimes$	Tensor product
$\mathbb{C}$	The set of complex numbers
$\|C\|$	The size of C
J	The set of Eisenstein-Jacobi integers
J_π	The set of Eisenstein-Jacobi integers modulo π
Z	The set of integers
A^t	Transpose of a matrix A
$Tr(\ \ )$	Trace function
Z_2^{2n}	$2n$ $-$dimensional vector space over Z_2
$w(A)$	Weight of an operator A

LIST OF ABBREVIATIONS

CSS	Calderbank-Shor-Steane
EJ	Eisenstein-Jacobi
EAQECC	Entanglement assisted quantum error correction code
QECC	Quantum error correction code
RREF	Reduced row echelon form
REF	Row echelon form
Sch	Schmidt number

LIST OF TABLES

Page

LIST OF FIGURES

Page

ABSTRACT

QUANTUM CODES OVER EISENSTEIN-JACOBI INTEGERS

Eda YILDIZ

Department of Mathematics

MSc. Thesis

Advisor: Assoc.Prof.Dr. Fatih DEMİRKALE

Though classical computers have been developed day by day, a new machine which is based on quantum mechanics and is called quantum computer is expected more powerful than a classical one. For instance, RSA which is a powerful cryptographic algorithm in classical computers is used in recent security systems and this algorithm cannot be cracked by using a classical computer. However, it is expected that a quantum computer can easily break this algorithm. If these computers can be built in practice, then a quantum error correction process which is based on principles of quantum mechanics is needed. Hence, quantum error correcting codes have been developed.

In this thesis, in Chapter 1 development of quantum coding theory from the beginning to today is mentioned and many studies made in this process are explained.

In Chapter 2, main definitions and theorems of algebraic coding theory is gave to place.

In Chapter 3, notations, matrices, operators which are used in quantum computation and their operations have been explained with properties.

In Chapter 4, the differences of quantum error correction from classical error correction and quantum error correcting codes are explained. CSS code, stabilizer code and entanglement assisted quantum codes are analyzed in detail and they are illustrated with examples.

In Chapter 5, quantum codes over Eisenstein-Jacobi integers have been constructed. Error detection and correction procedures of this new type of quantum codes have been explained and they are intensified with examples. Error matrices, error bases and a new distance of these codes are defined. Commutative condition of error operators is given and it is proved. Finally, it is showed that these new codes may give new and better parameters.

Keywords: Quantum codes, error correcting codes, CSS code, stabilizer code, entanglement, Eisenstein- Jacobi integers

ÖZET

EISENSTEIN-JACOBI TAMSAYILARI ÜZERİNDE KUANTUM KODLAR

Eda YILDIZ

Matematik Anabilim Dalı

Yüksek Lisans Tezi

Tez Danışmanı: Doç.Dr. Fatih DEMİRKALE

Klasik bilgisayarlar günden güne geliştiriliyor olsa da kuantum bilgisayar adı verilen ve kuantum mekaniğine dayandırılan yeni bir makinenin klasik bilgisayarların çok daha üstünde performans göstermesi beklenmektedir. Örneğin; klasik bilgisayarda güçlü kriptografik bir algoritma olan RSA, günümüzde güvenlik sistemlerinde kullanılmaktadır ve bu algoritma klasik bilgisayarlar kullanılarak kırılamamaktadır. Ancak kuantum bilgisayarların kendilerine özgü özellikler sayesinde bu algoritmayı kırabilecekleri düşünülmektedir. Eğer bu güçlü bilgisayarlar pratikte yapılabilirse, kuantum mekaniğini temel alan yeni bir hata düzeltme süreci de gerekli olacaktır. Bu yüzden kuantum hata düzelten kodlar geliştirilmiştir.

Bu tezde, ilk bölümde kuantum kodlama teorisinin başlangıçtan günümüze kadar gelen süreçteki gelişiminden söz edilmiş ve bu süreçte yapılan çalışmalar anlatılmıştır.

İkinci bölümde cebirsel kodlama teorisindeki temel tanım ve teoremlere yer verilmiştir.

Üçüncü bölümde kuantum hesaplamada kullanılan notasyonlar, matrisler, operatörler ve bunlarla yapılan işlemler özellikleriyle açıklanmıştır.

Dördüncü bölümde kuantum hata düzeltme sürecinin klasik hata düzeltmeden farkları anlatılarak kuantum hata düzelten kodlardan bahsedilmiş, bunlardan CSS kod, stabilizer kod ve dolaşık çiftler yardımıyla oluşturulan kuantum kodlar örneklerle ayrıntılı bir şekilde açıklanmıştır.

Beşinci bölümde Eisenstein-Jacobi tamsayıları üzerinde kuantum kodlar inşa edilmiştir. Kuantum kodların bu yeni sınıfının hata farketme ve düzeltme süreçleri açıklanmış ve bunlar örneklerle pekiştirilmiştir. Bu kodlar üzerinde hata matrisleri, hata tabanları ve yeni bir uzaklık tanımlanmıştır. Bu hata operatörlerinin değişmeli olma şartı verilmiş ve bu ispatlanmıştır. Son olarak da bu yeni kodlarla yeni parametreli kodlar üretilebileceği örneklendirilmiştir.

Anahtar Kelimeler: Kuantum kodlar, hata düzelten kodlar, CSS kod, stabilizer kod, dolaşıklık, Eisenstein-Jacobi tamsayıları

CHAPTER 1

INTRODUCTION

1.1 Literature Review

In 1948, Shannon published a paper [1] and he said that error correction is an important part of communication. When information transmits in a communication channel, some errors may occur. Hence, error correcting process is needed in classical computers [1]. Some codes over different structures are constructed to obtain good parameters.

In 1976, Ingarden showed Shannon's information theory cannot be generalized to the quantum case. So, a new information theory which is based on quantum mechanics is needed [2]. Benioff introduced an idea of a quantum computer in 1980 [3]. Deutsch described first universal quantum computer in 1985. A computer which is based on quantum mechanics is faster than classical one [4]. Error detection and correction process is needed in a quantum computer similar to a classical computer. Therefore, some codes which are based on the principles of a quantum computer are constructed.

In 1994, Huber defined codes over Eisenstein-Jacobi integers [5]. He defined a new minimum distance and he said that these codes are efficient in encoding and decoding processes. Also, he showed that there is an isomorphism between Eisenstein-Jacobi integers and finite fields. In 1998, Dong, Soh and Gunowan showed that Eisenstein-Jacobi integers give an efficient algorithms for coding QAM signals [6]. Firstly, in 1995 Shor invented a 9-qubit quantum code which corrects an error on a single qubit [7]. In 1996, Steane constructed a quantum code that encodes a single qubit to seven qubits [8]. In 1996, Calderbank and Shor described a quantum code which is obtained from two classical codes [9]. They showed that a quantum code can be constructed by using a linear code containing its dual. Furthermore, the structures of some other error correcting codes are analyzed in [10], [11], [12] and [13].

In 1997, Gottesman studied a new class of quantum codes which is called stabilizer codes in his PhD thesis [14]. He used group theory to construct this type of codes and he showed error detection and correction conditions. In 1998, Calderbank et al. obtained a quantum code from classical codes over $GF(4)$ [15]. So, quantum codes over finite fields are obtained. In 2006, Ketkar et al. generalized quantum codes over finite fields [16] and [17]. In 2006, Brun, Devetak and Hsieh constructed a quantum code by using entanglement [18]. Thus, they obtained codes with better parameters via entangled pairs. There are other studies about quantum codes with entanglement in [19], [20] and [21]. Again in 2006, Aly, Klappenecker and Sarvepalli described quantum subsystem codes [22]. They divided a system into subsystems and made passive error correction.

There are many studies on error correcting codes. In [23], [24] and [25] classical error correcting codes are studied. Articles [26], [27], [28], [29], [30], [31], [32], [33] and [34] give some information about quantum computation and quantum information theory. In general, main aim is finding error correcting codes over distinct mathematical structures to obtain better parameters.

1.2 Objective of Thesis

In this study, some class of quantum codes are studied. Error detection and correction conditions of these codes are analyzed and they are explained with illustrative examples. Also, a new class of quantum codes over Eisenstein-Jacobi integers are constructed. Some theorical properties of this code are explained and proven. Examples are given to show that this type of codes has good parameters and they have advantages over quantum codes which are constructed over finite fields.

1.3 Hypothesis

Quantum computers have many advantages over classical computers. Hence, quantum computers may become popular machines in the near future. Therefore, error correcting codes which is adapted to quantum computers play a significant role in recent topics. The existence of good quantum error correcting codes are studied by many researchers.

In Chapter 2, we will introduce the basics of algebraic coding theory. In Chapter 3, we will state some definitions and mathematical properties of quantum mechanics. In

Chapter 4, we will study some types of quantum error correcting codes. In Chapter 5, we will mention about the construction of classical block codes over Eisenstein-Jacobi integers. Moreover, we will present the construction of quantum codes over Eisenstein-Jacobi integers and we will illustrate it with examples. Also, we will define error bases and will state some properties of these new codes.

CHAPTER 2

BASICS OF THE CODING THEORY

In this chapter, we give some definitions and theorems which are necessary for the next chapters about algebraic coding theory. In general, references [23], [24] and [25] are used for well-known definitions and theorems.

2.1 Preliminaries

Definition 2.1 Let $A = \{a_1, a_2, \dots, a_q\}$ be a set with q elements.

i) A sequence $s = s_1 s_2 \dots s_n$ for $s_i \in A$ is a q-*ary word* of length n over A. The sequence s is also known as the vector $(s_1, s_2, \dots, s_n)$.

ii) A collection of q −ary words of length n with alphabet A is called a q −*ary block code* over A.

iii) Let C be a q −ary block code over A. An element of C is called a *codeword*.

iv) The notation $|C|$ denotes the number of elements in C and it is called the *size* of C.

v) The number $log_q|C|/n$ defines the *information rate* of the code C of length n.

vi) The *parameters* of the code C of length n and size M is denoted by (n, M).

Note that we will refer to A as a code alphabet and its elements are code symbols.

Definition 2.2

- A code is called a *binary code* if the code alphabet is $F_2 = \{0,1\}$.
- A code is called a *ternary code* if the code alphabet is $F_3 = \{0,1,2\}$.
- A code is called a *quaternary code* if the code alphabet is F_4 or Z_4.

Example 2.3

$C_1 = \{00, 01, 10, 11\}$ is a binary $(2,4)$ $-$code.

$C_2 = \{00000, 10000, 11000, 01011, 00111, 10101, 10001\}$ is a binary $(5,7)$ $-$code.

$C_3 = \{112, 121, 222, 111, 210\}$ is a ternary $(3,5)$ $-$code.

Definition 2.4 A set of the channel possibilities $P(a_j$ received$|a_i$ sent) which satisfies $\sum_{j=1}^{q} P\left(a_j\, received\middle|a_i\, sent\right) = 1$ where $1 \leq i \leq q$ with $A = \{a_1, a_2, \ldots, a_q\}$ is called a *communication channel.*

Definition 2.5 Let $x = x_1x_2 \ldots x_n$ be a sent word let $y = y_1y_2 \ldots y_n$ be a received word of length n. Then,

$$P(y\, received|x\, sent) = \prod_{i=1}^{n} P(y_i\, received|x_i\, sent).$$

In other words, the outcome of a transmission is independent of the outcome of the previous transmission. This type of the channels is called a *memoryless channel.*

Definition 2.6 Let C be a channel which satisfies the following properties:

i) Each symbol which is transmitted has the same probability p.

ii) If any error is occurred, then each of the $q - 1$ possible errors has equivalent probability.

Then, C is called a q *$-$ary symmetric channel.*

Remark 2.7 If the probabilities of the channel are $P(1\, received|0\, sent) = P(0\, received|1\, sent) = p$ and $P(0\, received|0\, sent) = P(1\, received|1\, sent) = 1 - p$ with the channel alphabet $\{0, 1\}$, then the channel is called a *binary symmetric channel.*

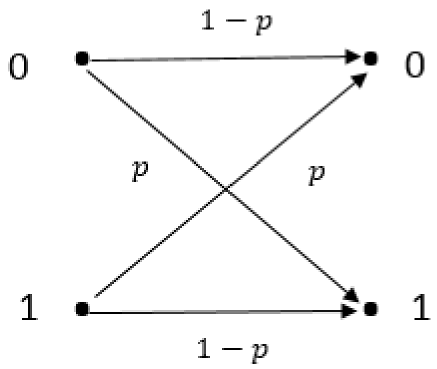

Figure 2. 1 Probability of binary symmetric channel

Example 2.8 Let $\{100, 111\}$ be a code. The codewords are sent over a binary symmetric channel with $p = 0.06$. Suppose that the word $r = 011$ is received. Then,

$$P(011|100) = P(0|1)P(1|0)P(1|0) = (0.06)(0.06)(0.06) = 0.000216,$$

$$P(011|111) = P(0|1)P(1|1)P(1|1) = (0.06)(0.94)(0.94) = 0.053016.$$

111 is more likely the codeword sent, since $0.053016 > 0.000216$.

2.1.1 Maximum Likelihood Decoding

Let c be a codeword which belongs to the code C. If we sent this codeword over a communication channel and a word r is received, then channel probabilities can be computed as $P(r\ received|\ c\ sent)$ for all $c \in C$.

If $P(r\ received|\ c_r\ sent) = \max_{c \in C} P(r\ received|\ c\ sent)$, then c_r is the maximum likely codeword which is transmitted. This rule is called maximum likelihood decoding (MLD) rule.

2.1.2 Hamming Distance

Let a and b be words of length n over an alphabet A. The number of different coordinates of a from b is called *Hamming distance* and denoted by $d(a, b)$ [23].

For $a = a_1 a_2 \dots a_n$ and $b = b_1 b_2 \dots b_n$, we define

$$d(a, b) = d(a_1, b_1) + d(a_2, b_2) + \cdots + d(a_n, b_n)$$

where $d(a_i, b_i) = \begin{cases} 1, & if\ a_i \neq b_i \\ 0, & if\ a_i = b_i \end{cases}$.

Example 2.9 Let $A = \{0,1,2\}$ and let $a = 101210,\ b = 221011, c = 100210$. Then,

$$d(a,b) = 4,$$

$$d(b,c) = 5,$$

$$d(a,c) = 1.$$

Proposition 2.10 Let a, b and c be words of length n over alphabet A.

Hamming distance d satisfies the following metric properties:

i) $0 \leq d(a,b) \leq n$.

ii) $d(a,b) = 0$ if and only if $a = b$.

iii) $d(a,b) = d(b,a)$. So d is symmetric.

iv) $d(a,c) \leq d(a,b) + d(b,c)$ (Triangle inequality).

2.1.3 Nearest Minimum Distance Decoding

Let c be a codeword which belongs to the code C. If $d(r, c_r) = \max_{c \in C}(r, c)$ where r is the received vector, then the nearest minimum distance decoding rule will decode r to c_r.

Example 2.11 Let $C = \{0001, 1011, 1001, 1111, 0010\}$. Assume that $r = 1000$ is received. Then,

$$\begin{aligned} d(1000,0001) &= 2, \\ d(1000,1011) &= 2, \\ d(1000,1001) &= 1, \\ d(1000,1111) &= 3, \\ d(1000,0010) &= 2. \end{aligned} \tag{2.1}$$

Since $\min_{c \in C} d(1000, c) = 1$. We decode 1000 to 1001.

2.1.4 Distance of a Code

Besides the length and the size of a code, its distance is another parameter to define the code. The distance of a code is a crucial factor, because it determines the capabilities of the error detection and correction of a code. These capabilities are main aim of the codes.

Definition 2.12 Let C be a code which has at least two codewords. The *minimum distance* of C is denoted by $d(C)$ and it is defined as:

$$d(C) = min\{d(a,b) |\, a, b \in C, a \neq b\} \tag{2.2}$$

Definition 2.13 Let C be a code of length n and size M. If the minimum distance of C is d, then C is called an (n, M, d) −code. The numbers n, M and d are parameters of C.

Example 2.14 Let $C = \{001201, 111000, 212100, 200012\}$ be a ternary code.

$$d(001201, 111000) = 4,$$

$$d(001201, 212100) = 5,$$

$$d(001201, 200012) = 5,$$

$$d(111000, 212100) = 3,$$

$$d(111000, 200012) = 5,$$

$$d(212100, 200012) = 5.$$

C is a ternary (6,4,3)-code, since $d(C) = 3$.

Definition 2.15 Let e be a positive integer. If the minimum distance decoding can detect e or fewer errors, then a code C is *e-error detecting*. If C is e-error detecting but not $(e + 1)$-error detecting, then it is *exactly e-error detecting*.

Example 2.16 $C = \{0000, 0101, 1011\}$ is 1-error detecting.

The vector 0000 transforms into 0101 by changing two coordinates.

The vector 0000 transforms into 1011 by changing three coordinates.

The vector 0101 transforms into 1011 by changing three coordinates.

If an error occurs in only one position, then this word is not in C. So, one error can be detected. But, if two errors occur in two positions, this word might be another codeword in C. So, some two errors cannot be detected. For instance; when the codeword 0000 changes to 0101, the word 0101 is also a codeword in C. Hence, this error cannot be detected.

Also, C is exactly 1-error detecting, because C is 1-error detecting but not 2-error detecting.

Definition 2.17 Let k be a positive integer. If the minimum distance decoding can correct k or fewer errors, then a code C is *k-error correcting*. If C is k-error correcting but not $(k+1)$-error correcting, then it is *exactly k-error correcting*.

Example 2.18 Let $C = \{0000,1011\}$ be a code.

If 0000 is sent and one error occurs, then the possible received words are $1000, 0100, 0010, 0001$. Since none of them is in C, they will be decoded as 0000. If 1011 is sent and one error occurs, then the possible received words are $0011, 1111, 1001$ and 1010. Since none of them is in the code C, they will be decoded to 1011. In all cases, one error can be corrected. So, C is a one-error-correcting code. But if at least two errors occur, the minimum distance decoding may lead to a wrong codeword. So, C is exactly one-error-correcting.

2.2 Linear Codes

A linear code of length n over the finite field F_q is a subspace of the vector space F_q^n. So, the algebraic properties of linear codes take some advantages over nonlinear codes. Firstly, we introduce some basics of vector spaces.

2.2.1 Vector Spaces

Definition 2.19 Let F_q be a finite field with q elements. The nonempty set V is a *vector space* over F_q if it satisfies the following properties. For all $\alpha, \beta \in V$ and $k_1, k_2 \in F_q$:

i) $(V, +)$ is an abelian group,
ii) $k_1(\alpha + \beta) = k_1\alpha + k_1\beta$, $(k_1 + k_2)\alpha = k_1\alpha + k_2\alpha$,
iii) $(k_1k_2)\alpha = k_1(k_2\alpha)$,
iv) If 1_v is the multiplicative identity of F_q, $1\alpha = \alpha$.

Note that if $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n), \beta = (\beta_1, \beta_2, \dots, \beta_n) \in F_q^n$, then

$$\alpha + \beta = (\alpha_1 + \beta_1, \alpha_2 + \beta_2, \dots, \alpha_n + \beta_n) \in F_q^n \text{ and}$$

$$k_1\alpha = (k_1\alpha_1, k_1\alpha_2, \dots, k_1\alpha_n) \in F_q^n,$$

where $F_q^n = \{(\alpha_1, \alpha_2, \dots, \alpha_n) | \alpha_i \in F_q\}$. So, F_q^n is a vector space.

Example 2.20 The following sets are vector spaces over F_q.

i. $C_1 = \{0\}$ and $C_2 = F_q^n$.

ii. $C_3 = \left\{(k, k, \dots, k) \middle| k \in F_q\right\}$.

iii. $C_4 = \{(0,0,0), (1,0,0), (0,1,0), (1,1,0)\}$ over F_2.

iv. $C_5 = \{(0,0,0,0), (1,1,2,0), (2,2,1,0)\}$ over F_3.

A vector $(\alpha_1, \alpha_2, \dots, \alpha_n)$ can be written as $\alpha_1 \alpha_2 \dots \alpha_n$.

Definition 2.21 Let S be a subset of a vector space V. If S is also a vector space, then it is called a *subspace* of V.

Example 2.22

i. $\{0\}$ is a subspace of all vector spaces.

ii. $\{(0,0,0), (1,0,0), (0,1,0), (1,1,0)\}$ is a subspace of F_2^3.

iii. $\{(0,0,0), (1,1,1), (2,2,2)\}$ is a subspace of F_3^3.

Definition 2.23 Let V be a vector space over F_q and $S = \{s_1, s_2, \dots, s_m\}$ be a nonempty subset of V.

$$< S >= \{k_1 s_1 + \cdots + k_m s_m \, | k_i \in F_q \; and \; s_i \in S\}.$$

This set is called *span* of S. If $C =< S >$, then S is called a *spanning set* of C.

Definition 2.24 Let V be a vector space over F_q. The nonempty subset B of V is called a *basis* for V if $V =< B >$ and B is linearly independent.

Note that the number of elements of a basis for V is called dimension V and it is denoted by $dim(V)$.

Theorem 2.25 Let V be a vector space over F_q. If $\dim(V) = k$, then

i. V has q^k elements.

ii. V has $\frac{1}{k!}\prod_{i=0}^{k-1}(q^k - q^i)$ different bases.

Example 2.26 $q = 3, S = \{1012, 2011\}$. Let V be generated by S, $V = \langle S \rangle$. Then,

$$V = \{0000, 1012, 0020, 2011, 1002, 2001, 1022, 0010, 2021\}.$$

Here, $q = 3, k = 2$ and so,

$$\frac{1}{2!}\prod_{i=0}^{1}(3^2 - 3^i) = \frac{1}{2!}(3^2 - 3^0)(3^2 - 3^1) = \frac{1}{2!}.8.6 = 24.$$

Hence, V has 24 different bases.

Definition 2.27 Let $u = (u_1, u_2, \ldots, u_n),\ v = (v_1, v_2, \ldots, v_n) \in F_q^n$. The Euclidian inner product (or dot product) of u and v is defined as $u_1v_1 + u_2v_2 + \cdots + u_nv_n$ and it is denoted by $u \cdot v$. Let S be a nonempty subset of F_q^n. The vectors u and v are called *orthogonal* if $u \cdot v = 0$. The set $S^{\perp} = \{u \in F_q^n \mid u.v = 0\ for\ all\ v \in S\}$ is called the *orthogonal complement* of S.

Remark 2.28 If $S = \emptyset$, then $S^{\perp} = F_q^n$.

Example 2.29

i. Let $q = 2$ and $n = 5$. Let $u_1 = (1{,}0{,}1{,}0{,}1)$, $u_2 = (0{,}1{,}0{,}1{,}0)$ and $u_3 = (1{,}1{,}1{,}1{,}1)$ be elements of F_2^5. Then,

$$u_1.u_2 = 1.0 + 0.1 + 1.0 + 0.1 + 1.0 = 0.$$

$$u_1.u_3 = 1.1 + 0.1 + 1.1 + 0.1 + 1.1 = 1.$$

$$u_2.u_3 = 1.0 + 1.1 + 1.0 + 1.1 + 1.0 = 0.$$

So, u_1, u_2 and u_2, u_3 are pairwise orthogonal.

ii. Let $q = 2$ and $S = \{0000, 0101, 1010, 1111\}$. Let's find the complement of S.

Let $u = (u_1, u_2, u_3, u_4)$ be an element of F_2^4.

$$u.(0{,}1{,}0{,}1) = u_2 + u_4 = 0,$$

$$u.(1{,}0{,}1{,}0) = u_1 + u_3 = 0,$$

$$u = (1{,}1{,}1{,}1) = u_1 + u_2 + u_3 + u_4 = 0.$$

Thus, $u_1 = u_3, u_2 = u_4$ and $u_1 + u_2 + u_3 + u_4 = 0$. It follows that $S^{\perp} = \{0000, 0101, 1010, 1111\}$.

2.2.2 Linear Codes

Definition 2.30 Let C be a subspace of F_q^n. Then, C is called a *linear code* of length n over F_q.

Example 2.31

i) Let $C = \{(u, u, u, \dots, u) | u \in F_q\}$. This is called a *repetition code*. A repetition code is a linear code over F_q.

ii) Let $q = 2$ and $C = \{000, 100, 010, 001, 111, 110, 101, 011\}$. C is a binary linear code.

iii) Let $q = 3$ and $C = \{0000, 1000, 2000\}$. C is a ternary linear code.

Definition 2.32 Let C be a linear code in F_q^n.

i) The dual code of C is the orthogonal complement of C and it is denoted by $C^\perp$.

ii) The dimension of C is the dimension of C as a vector space over F_q^n and it is denoted by $dim(C)$.

Theorem 2.33 Let C be a linear code of length n over F_q. Then,

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

ii) $C^\perp$ is also a linear code and $di\,m(C) + \dim(C^\perp) = n$.

iii) $(C^\perp)^\perp = C$.

Proof.

i) The dimension of the code C is the dimension of C as a vector space over F_q. A vector space V over F_q has q^k elements where the dimension of V is k. So, C has $q^{dim(C)}$ elements since $dim(C)$ is the dimension of C as a vector space.

ii) From the Rank-Nullity Theorem, we have already known that $dim(\langle C\rangle) + dim(C^\perp) = n$ where C is a subset of F_q^n. In here, C is a subspace of F_q^n since it is a linear code. So, $\langle C\rangle = C$. Then, $dim(C) + dim(C^\perp) = n$.

iii) For any $c \in C$, $c.c' = 0$ for all $c' \in C^\perp$. Then, $c \in (C^\perp)^\perp$. Thus, $C \subseteq (C^\perp)^\perp$. We conclude that $(C^\perp)^\perp = C$ since $dim(C) = dim((C^\perp)^\perp)$ and $C \subseteq (C^\perp)^\perp$.

Example 2.34 Let $q = 3$ and

$C = \{0000, 0001, 0002, 0100, 0101, 0102, 0201, 0202, 0102\}$.

So, $\dim(C) = \log_3|C| = \log_3 9 = 2$.

$$C^\perp = \{0000, 1000, 2000, 0010, 0020, 0101, 1020, 2010, 2020\}.$$

Then, $\dim(C^\perp) = \log_3|C^\perp| = \log_3 9 = 2$.

Consequently, $dim(C) + dim(C^{\perp}) = 2 + 2 = 4 = n$.

A code C of length n and size M over F_q is called an $(n, M) - code$. If the code C is a linear code, M can be written as a power of q. Then, $M = q^k$ where $k = \dim(C)$. Hence, C is also called an $[n, k] - code$ if C is a linear code.

Definition 2.35 Let C be a linear code.

i) If $C \subseteq C^{\perp}$, then C is called self-orthogonal.

ii) If $C = C^{\perp}$, then C is called self-dual.

Proposition 2.36

i) The dimension of a self-orthogonal code of length n is less than or equal to ${}^{n}/_{2}$.

ii) The dimension of a self-dual code of length n is ${}^{n}/_{2}$.

Proof.

i) From the ii) part of theorem 2.32, we know that $dim(C) + dim(C^{\perp}) = n$. If C is self-orthogonal, that is $C \subseteq C^{\perp}$, then $dim(C) \leq dim(C^{\perp})$. Thus,

$$dim(C) + dim(C) \leq dim(C) + dim(C^{\perp}) = n. \tag{2.3}$$

Hence, $2dim(C) \leq n$ implies $dim(C) \leq \frac{n}{2}$.

ii) If C is a self-dual code, then $C = C^{\perp}$. So,

$$dim(C) + dim(C) = dim(C) + dim(C^{\perp}) = n. \tag{2.4}$$

So, $2dim(C) = n$ implies that $dim(C) = \frac{n}{2}$.

Example 2.37 Let $q = 2$ and $C = \{0000, 1010, 0101, 1111\}$. Then,

$$C^{\perp} = \{0000, 1010, 0101, 1111\}.$$

C is a self-dual code since $C = C^{\perp}$.

2.2.3 Hamming Weight

Definition 2.38 [23] Let $a = (a_1, a_2, \ldots, a_n) \in F_q^n$. The Hamming weight of a is defined as the number of nonzero coordinates in a and it is denoted by $wt(a)$. That is $wt(a) = d(a, \bar{0})$ where $\bar{0}$ is the zero vector.

$$wt(a_i) = d(a_i, 0) = \begin{cases} 1 & if\ a_i \neq 0 \\ 0 & if\ a_i = 0 \end{cases} \tag{2.5}$$

Then, the Hamming weight of a can be written as $wt(a) = wt(a_1) + wt(a_2) + \cdots + wt(a_n)$.

Lemma 2.39 Let a and b be elements of F_q^n. Then, $d(a,b) = wt(a-b)$.

Proof: If $d(a,b) = 0$, then $a = b$ since d is a metric. Then, $wt(a-b) = wt(0) = 0$. Thus, $d(a,b) = 0 = wt(a-b)$.

If $d(a,b) \neq 0$, then $d(a,b) = |\{i|a_i \neq b_i\}| = |\{i \mid a_i - b_i \neq 0\}| = d(a-b,0) = wt(a-b)$.

Lemma 2.40 Let $a = (a_1, a_2, \dots, a_n)$ and $b = (b_1, b_2, \dots, b_n)$ be elements of F_2^n. Then,

$$wt(a+b) = wt(a) + wt(b) - 2wt(a*b). \tag{2.6}$$

where $a * b$ is defined as $(a_1b_1, a_2b_2, \dots, a_nb_n)$.

Table 2. 1 Table of Lemma 2.40

a	b	$a*b$	$wt(a+b) = wt(a) + wt(b) - 2wt(a*b)$	$wt(a+b)$
0	0	0	0	0
0	1	0	1	1
1	0	0	1	1
1	1	1	0	0

Proof. From the definition of Hamming distance, it is true for $a, b \in F_2$ by Table 2.1. In general, it can be verified as in Table 2.1.

Lemma 2.41 Let $a, b \in F_q^n$. Then,

$$wt(a) + wt(b) \geq wt(a+b) \geq wt(a) - wt(b). \tag{2.7}$$

Definition 2.42 Let C be a code. The *minimum Hamming weight* of C is the smallest of the weights of nonzero codewords of C and it is denoted by $wt(C)$. More formally,

$$wt(C) = \min\{wt(c_i)|c_i \in C \text{ and } c_i \neq 0\}. \tag{2.8}$$

Theorem 2.43 [23] Let C be a linear code over F_q. Then, Hamming weight of the code C is equal to Hamming distance of the code C, that is $wt(C) = d(C)$.

Proof. Let C be a linear code and let $a, b \in C$, we have $d(a, b) = wt(a - b)$. There exist $a', b' \in C$ such that $d(a', b') = d(C)$. Then,

$$d(C) = d(a', b') = wt(a' - b') \geq wt(C). \quad (2.9)$$

Since $wt(C)$ is the smallest of the weights of the nonzero codewords of C. So, d(C)$\geq$ $wt(C)$.

On the other hand, there is a $c \in C$ such that $wt(C) = wt(c)$.

$$wt(C) = wt(c) = d(c, 0) \geq d(C). \quad (2.10)$$

So, $wt(C) \geq d(C)$.

Therefore, we obtain that $wt(C) = d(C)$ if C is a linear code.

Example 2.44 Let $C = \{00000, 00001, 10000, 10001, 11010, 11011, 01010, 01011\}$ is a linear code over F_2. Then,

$$wt(00001) = wt(10000) = 1, wt(10001) = wt(01010) = 2,$$
$$wt(11010) = wt(01011) = 3, \qquad wt(11011) = 4.$$

Thus, $wt(C) = min\{wt(c_i)|c_i \in C \ and \ c_i \neq 0\} = min\{1, 2, 3, 4\} = 1$. Hence, $d(C) = 1$.

2.2.4 Basis for Linear Codes

Linear codes can be described by a basis since they are vector spaces. Therefore, finding a basis of a linear code is important. There are many methods to obtain a basis of a vector space. We will mention some of them here.

Definition 2.45 Let M be a matrix over F_q. The following operations are elementary row operations:

i) swapping two rows,

ii) multiplying a row by a scalar,

iii) replacing a row by its sum with a scalar multiple of another row.

Definition 2.46 Two matrices are called *row equivalent* if one can be obtained from the other by a sequence of elementary row operations.

Remark 2.47

i) Any matrix M over F_q can be put in row echelon form (REF) or reduced row echelon form (RREF) by a sequence of elementary row operations. In other words, a matrix is row equivalent to a matrix in REF or in RREF.

ii) For a given matrix, its RREF is unique, but it may have different REFs. (Recall that the difference between the RREF and the REF is that the leading nonzero entry of a row in the RREF is equal to 1 and it is the only nonzero entry in its column.)

2.2.4.1 Method 1

Let S be a nonempty subset of F_q^n, let C be a linear code generated by S; that is, $C = \langle S \rangle$ and M be a matrix whose rows are the words of S. The row echelon form of M is found by using the elementary row operations. The nonzero rows of the last matrix form a basis for C.

Example 2.48 Let $q = 2$ and $S = \{00001, 11011, 11111, 10100, 10101\}$. Let's find a basis for C which is generated by S.

$$M = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

The last matrix is a row reduced form of M. So, $\{10000, 01010, 00100, 00001\}$ is a basis for C.

Note that the notation $\sim$ denotes the row equivalent matrix.

2.2.4.2 Method 2

Let S be a nonempty subset of F_q^n, let C be a linear code generated by S; that is, $C = \langle S \rangle$ and M be a matrix whose columns are the words of S. The row echelon form of M is found by using elementary row operations. The leading columns are located in the row echelon form. The columns of the initial state of M which correspond to the leading columns form a basis for the code.

Example 2.49 Let $q = 3$ and $S = \{1020,1102, 2000, 0102\}$. Find a basis for C which is generated by S.

$$M=\begin{pmatrix}1&1&2&0\\0&1&0&1\\2&0&0&0\\0&2&0&2\end{pmatrix}\sim\begin{pmatrix}1&1&2&0\\0&1&0&1\\0&1&2&0\\0&0&0&0\end{pmatrix}\sim\begin{pmatrix}1&1&2&0\\0&1&0&1\\0&0&2&2\\0&0&0&0\end{pmatrix}\sim\begin{pmatrix}1&1&0&1\\0&1&0&1\\0&0&1&1\\0&0&0&0\end{pmatrix}\sim\begin{pmatrix}1&0&0&0\\0&1&0&1\\0&0&1&1\\0&0&0&0\end{pmatrix}.$$

Columns 1, 2 and 3 of the row echelon form are the leading columns. So, the set $B=\{1020,1102,2000\}$ is obtained from the original columns of M which correspond to the leading columns. Therefore, from the method 2, $B=\{1020,1102,2000\}$ is a basis for C.

Remark 2.50 Although the obtained basis is a subset of S in the method 2, it is not necessary for the method 1.

2.2.4.3 Method 3

Let S be a nonempty subset of F_q^n, let C be a linear code which is generated by S and M be a matrix whose rows are the words of S. The reduced row echelon form (RREF) of M is found by using elementary row operations.

Let G be a matrix which consists of nonzero rows of the reduced row echelon form. So, M transforms into a form as $\binom{G}{0}$ where G is $k\times n$ matrix and 0 denotes the zero matrix. G has k leading columns. We construct the matrix G' by permuting the columns of G such that it contains a $k\times k$ identity matrix on the left side and a $k\times(n-k)$ matrix on the right side; that is, $G'=(I_k|A)$. The matrix H is formed as $H=(-A^t|I_{n-k})$ in which A^t is the transpose of A. Then, the inverse of the permutation is applied to the columns of H and a matrix H' is obtained. Finally, the rows of H' form a basis for the dual code of C.

Example 2.51 Let C be a linear code over F_2 and let G be a reduced row echelon form of M whose rows are the codewords in C;

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

The columns 1, 4, 5 and 7 form an identity matrix. So, we obtain the following matrix by permuting these columns:

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

Then,

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

Applying the inverse permutation, we obtain

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

The rows of H' form a basis for the dual code of C.

2.2.5 Generator and Parity-Check Matrix of a Code

Linear codes are important in Coding Theory since they can be represented by a basis. A basis for a code provides description of all codewords of the code. Bases are represented by a matrix so that operations can be applied easily, when the size of the code is large. A matrix which represents a code is called a generator matrix for the code and a matrix which represents the dual of a code is called a parity-check matrix of the code.

Definition 2.52 Let C be a linear code.

i) A matrix whose rows form a basis of C is called a *generator matrix* for C.

ii) A generator matrix of the dual code of C is called a *parity-check matrix* of C.

Definition 2.53 Let C be an $[n, k]$ −linear code.

i) If a generator matrix has a form $(I_k|A)$, then it is said to be in the *standard form*.

ii) If a parity-check matrix has a form $(B|I_{n-k})$, then it is said to be in the *standard form*.

Example 2.54 Let $q = 3$ and $S = \{10001, 01010, 11011, 00011, 11100\}$. Let C be a linear code such that $C = \langle S \rangle$.

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

where ∼ denotes the row equivalences. Then,

$$G=\begin{pmatrix}1&0&0&0&1\\0&1&0&0&1\\0&0&1&0&0\\0&0&0&1&1\end{pmatrix}_{4\times 5}\quad,\qquad H=(1\ \ 1\ \ 0\ \ 1\ \ 1)_{1\times 5}.$$

Remark 2.55 Every linear code may not have a generator matrix in the standard form.

Example 2.56 Let $C=\{0000,1000,0001,1001\}$ be a linear code over F_2. Each of the sets $\{1000,0001\}$, $\{1000,1001\}$ and $\{0001,1001\}$ is a basis for C. So, each of the following matrices is a generator matrix of C:

$$\begin{pmatrix}1&0&0&0\\0&0&0&1\end{pmatrix},\ \begin{pmatrix}0&0&0&1\\1&0&0&0\end{pmatrix},\ \begin{pmatrix}1&0&0&0\\1&0&0&1\end{pmatrix},\ \begin{pmatrix}1&0&0&1\\1&0&0&0\end{pmatrix},\ \begin{pmatrix}0&0&0&1\\1&0&0&1\end{pmatrix},\ \begin{pmatrix}1&0&0&1\\0&0&0&1\end{pmatrix}.$$

However, none of them is in standard form.

Lemma 2.57 Let C be an $[n,k]$ $-$linear code over F_q and let G be a generator matrix of C. Then, $u\in C^{\perp}$ if and only if $Gu^t=0$.

Let H be an $(n-k)\times n$ matrix. The matrix H is a parity-check matrix of C if and only if the rows of the matrix are linearly independent and $GH^t=0$.

Equivalently for the first statement, $a\in C$ if and only if $aH^t=0$.

Proof. Let g_i be the ith row of G. Any element of C can be written as a linear combination of the rows of G, since the rows of G form a basis for C. In other words, for all $c\in C$,

$$c=\mu_1 g_1+\mu_2 g_2+\cdots+\mu_k g_k$$

where $\mu_i\in F_q$ for $1\le i\le k$. If $c\in C$, then $c\cdot c'=0$ for all $c'\in C^{\perp}$. The product $c\cdot c'=0$ implies that $(\mu_1 g_1+\mu_2 g_2+\cdots+\mu_k g_k).c'=0$. Thus, c' is orthogonal to g_i for $i\in\{1,2,..,k\}$; that is, $Gu^t=0$.

On the other hand, if Gu^t=0, then $g_i\cdot\ c=0$ for all $1\le i\le k$. Then,

$$c\cdot c'=(\mu_1 g_1+\mu_2 g_2+\cdots+\mu_k g_k).c'=\mu_1(g_1.c')+\mu_2(g_2.c')+\cdots+\mu_k(g_k.c')=0$$

since $c=\mu_1 g_1+\mu_2 g_2+\cdots+\mu_k g_k$ and $g_i.c'=0$ for all $i\in\{1,2,..,k\}$.

From Definition 2.51 ii), the rows of H are linearly independent since H is a parity-check matrix and from the former statement, $GH^t=0$ since the rows of H are codewords in $C^{\perp}$.

Conversely, assume $GH^t = 0$ and let $R(H)$ be the row space of H. By the former statement, we have $R(H) \subseteq C^{\perp}$. Then, $R(H)$ has dimension $n-k$ since the rows of H are linearly independent, thus $R(H) = C^{\perp}$. Thus, H is a parity-check matrix of C.

Theorem 2.58 Let C be a linear code and let H be a parity-check matrix of C.

i) A set of d columns of H is linearly dependent if and only if the distance of C is less than or equal to d.

ii) Any $d-1$ columns of H are linearly independent if and only if the distance of C is greater than or equal to d.

Proof.

i) If d columns are linearly dependent, then a linear combination of them is equal to zero; that is, u_1h_1+$u_2h_2 + \cdots + u_dh_d = 0$ where h_i is ith column of H and u_i is an element of F_q for all $1 \leq i \leq d$. Then, at least one of these coefficients u_i is nonzero. The nonzero coefficients u_i define a vector u of length d or less which satisfies $uH^t = 0$.

Conversely, let the distance of C be less than or equal to d. Then, there exists $c = (c_1, c_2, \ldots, c_n) \in C$ such that $wt(c) = wt(C) = d(C) \leq d$ since C is a linear code. So, $n-d$ coordinates of c are zero by the definition of the weight. Then, the remaining d columns of H are linearly dependent.

ii) It is similar to the first statement of the proof.

Example 2.59 Let C be a linear code over F_2, let d be the minimum distance of C and let H be a parity-check matrix of C where

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

Any two columns of H are linearly independent. But, three columns are linearly dependent since the sum of the columns 1, 2 and 3 is zero. So, $d = 3$.

Theorem 2.60 Let C be an $[n,k]$ −linear code. If G =$(I_k|A)$ is a generator matrix of C which is in standard form, then the matrix H =$(-A^t|I_{n-k})$ is a parity-check matrix of C.

Proof. Let $G = \begin{pmatrix} 1 & 0 & 0 \cdots 0 & a_{11} \cdots a_{1,n-k} \\ 0 & 1 & 0 \cdots 0 & a_{21} \cdots a_{2,n-k} \\ & & \vdots & \\ 0 & 0 & 0 \cdots 1 & a_{k,1} \cdots a_{k,n-k} \end{pmatrix}$ and $H = \begin{pmatrix} -a_{11} \cdots -a_{k,1} & 1 & 0 & \cdots & 0 \\ -a_{12} \cdots -a_{k,2} & 0 & 1 & \cdots & 0 \\ \vdots & & & & \\ -a_{1,n-k} \cdots -a_{k,n-k} & 0 & 0 & \cdots & 1 \end{pmatrix}$. It is clear that the rows of H are linearly independent. The product of the ith row of G and jth row of H gives $0 + 0 + \cdots + a_{ij} + 0 + 0 + \cdots + (-a_{ij}) + 0 = 0$. This shows that H is orthogonal to G. Then, H is a parity-check matrix for C by lemma 2.56.

2.2.6 Encoding Procedure in Linear Codes

Let C be an $[n, k]$ −linear code over F_q. Each codeword in C carries an information. So, C carries q^k information since C has q^k codewords. Let $\{\beta_1, \beta_2, \dots, \beta_k\}$ be a basis for C. Then, each codeword c in C can be written as $c = \mu_1\beta_1 + \mu_2\beta_2 + \cdots + \mu_k\beta_k$ where $\mu_i \in F_q$ for all $1 \leq i \leq k$. Let the vector β_i be the ith row of matrix G. The vector $c = \mu. G = \mu_1\beta_1 + \mu_2\beta_2 + \cdots + \mu_k\beta_k$ is an element of C where $\mu = (\mu_1, \mu_2, \dots, \mu_k)$. In other words, any codeword in C can be written as $c = aG$. So, every element of F_q^n can be encoded as $c = aG$.

Describing an element of F_q^n as a codeword of C is called *encoding*. An element $a \in F_q^n$ transforms into c by $c = aG$ where G is a generator matrix of C.

Example 2.61 Let C be a $[7,4]$ −linear code over F_2 and let G be a generator matrix of C:

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

Let $a = 1101$ be a message which is sent. Then,

$$c = aG = (1\ \ 1\ \ 0\ \ 1) \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} = (1\ \ 1\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0).$$

The encoded vector $c = (1\ \ 1\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0)$ is a codeword in C.

2.2.7 Decoding Procedure in Linear Codes

If a decoding method of a code can be applied easily, then the code is practical.

Cosets play an important role in the decoding methods. So, firstly we will introduce the concept of a coset.

2.2.7.1 Cosets

Definition 2.62 Let C be a linear code which is a subspace of F_q^n and let a be an element of F_q^n. A coset of C is defined as

$$a + C = \{a + c \mid c \in C\} = C + a. \tag{2.11}$$

The set $a + C$ is called a *coset* of C.

Example 2.63 Let $C = \{0000, 1000, 0001, 1001\}$ be a code over F_2. Then,

$0000 + C = \{0000, 1000, 0001, 1001\}$, $0100 + C = \{0100, 1100, 0000, 1101\}$,

$0001 + C = \{0001, 1001, 0000, 1000\}$, $0101 + C = \{0101, 1101, 0100, 1100\}$,

$0010 + C = \{0011, 1011, 0010, 1010\}$, $0110 + C = \{0110, 1110, 0111, 1111\}$,

$0011 + C = \{0011, 1011, 0010, 1010\}$, $0111 + C = \{0111, 1111, 0110, 1110\}$,

$1000 + C = \{1000, 0000, 1001, 0001\}$, $1100 + C = \{1100, 0100, 1101, 0101\}$,

$1001 + C = \{1001, 0001, 1000, 0000\}$, $1101 + C = \{1101, 0101, 1100, 0100\}$,

$1010 + C = \{1010, 0010, 1011, 0011\}$, $1110 + C = \{1110, 0110, 1111, 0111\}$,

$1011 + C = \{1011, 0011, 1010, 0010\}$, $1111 + C = \{1111, 0111, 1110, 0111\}$.

Note that $0000 + C = 0001 + C = 1000 + C = 1001 + C = C$.

Theorem 2.64 Let C be an $[n, k]$ −linear code over F_q. Then,

i) The size $|a + C| = |C| = |C + a| = q^k$ for all $a \in F_q^n$.

ii) For all $a, b \in F_q^n$ if $a \in b + C$, then $a + C = b + C$.

iii) Every element of F_q^n is included in some coset of C.

iv) Two cosets are either disjoint or identical.

v) The number of the different cosets of C is q^{n-k}.

vi) For any $a, b \in F_q^n$, $a - b \in C$ if and only if a and b are in the same coset.

Proof.

i) Coset $a + C$ has at most q^k elements since C has q^k elements. Let $a + c$ and $a + c'$ be two elements of $a + C$. The elements $a + c = a + c'$ if and only if $c = c'$. So, $a + C$ has exactly q^k elements.

ii) If $a \in b + C$, then $a + C \subseteq b + C$. From Part i), $|a + C| = |C|$ for all $a \in F_q^n$. So, $|a + C| = |b + C|$ where $a, b \in F_q^n$. Hence, $a + C = b + C$.

iii) Let a be an element of F_q^n. It is clear that $a \in a + C$.

iv) Let $a + C$ and $b + C$ be two coset of C. Assume that the intersection of them is nonempty. Let $u \in (a + C) \cap (b + C)$. Then, $u \in a + C$ and $u \in b + C$. From Part ii), $u + C = a + C$ since $u \in a + C$ and $u + C = b + C$ since $u \in b + C$. Hence, $a + C = u + C = b + C$ and then $a + C = b + C$. This means that if intersection of $a + C$ and $b + C$ is nonempty, then they are identical.

v) The vector space F_q^n has q^n elements. By Part i), the sizes of the cosets of C are q^k. From Parts iii) and iv), we know that every element of F_q^n is included in some coset and the cosets are either disjoint or identical. So, the number of the distinct cosets of C is $\frac{q^n}{q^k} = q^{n-k}$.

vi) Let $a - b = c \in C$. Then, $a = b + c \in b + C$. So, we have that $a + C = b + C$ by Part ii). Element a is contained in $a + C$ and element b is contained in $b + C$. Then $a \in a + C = b + C$ and $b \in b + C = a + C$. Hence, a and b are in the same coset since $a + C = b + C$.

On the other hand, let a and b be in the same coset $u + C$. Then, elements a and b can be written as $a = u + c$ and $b = u + c'$ for some $c, c' \in C$. Thus, $a - b = (u + c) - (u + c') = c - c' \in C$.

2.2.7.2 Decoding Procedure for Linear Codes with Standard Array

Let C be a linear code and let u be a codeword in C which is transmitted. Assume that v is received. Then, $e = v - u$ is the error string. From Theorem 2.63 vi), v and e are in the same coset since $v - e = u \in C$. The method works as following:

1) Firstly, the standard array of C is constructed.
2) The error string e of least weight in the coset $v + C$ is chosen.
3) The vector $u = v - e$ is the original codeword which is transmitted.

Example 2.65 Let $C = \{00000, 11001, 01110, 10111\}$ be a linear code over F_2. Assume that $v = 11111$ is received. Then, the cosets are

$$00000 + C = \{00000, 11001, 01110, 10111\}$$

$$00001 + C = \{00001, 11000, 01111, 10110\}$$

$$00010 + C = \{00010, 11011, 01100, 10101\}$$

$$00100 + C = \{00100, 11101, 01010, 10011\}$$

$$01000 + C = \{01000, 10001, 00110, 11111\}$$

$$10000 + C = \{10000, 01001, 11110, 00111\}$$

$$00011 + C = \{00011, 11010, 01101, 10100\}$$

$$00101 + C = \{00101, 11100, 01011, 10010\}$$

Then, $v = 11111$ is in $01000 + C$. The error string which has the least weight in the coset is 01000 . Thus, $u = v - e = 11111 - 01000 = 10111$ is the most likely codeword which is transmitted.

A vector which has a length of the smallest weight in a coset is called a *coset leader*.

2.2.7.3 Decoding Procedure for Linear Codes with Syndromes

Syndrome decoding is an efficient way in order to decode linear codes. There is a one-to-one correspondence between cosets and syndromes of a code. This correspondence provides an easy decoding method. Thus, the method is known as a general decoding algorithm.

Definition 2.66 Let C be a q-ary $[n, k, d]$ $-$linear code. Let H be a parity-check matrix of C. The *syndrome* of a is denoted by $S(a)$ and it is calculated as $S(a) = aH^t$ for any $a \in F_q^n$. The vector $S(a)$ is an element of F_q^{n-k}.

Theorem 2.67 Let C be a q-ary $[n, k, d]$ $-$linear code and let H be a parity-check matrix of C. Then, for all $a, b \in F_q^n$,

i) $S(a + b) = S(a) + S(b)$.

ii) $S(a) = 0$ if and only if a is a codeword in C.

iii) $S(a) = S(b)$ if and only if a and b are in the same coset.

Proof. Let C be a linear code, let a, $b \in F_q^n$ and H be a parity-check matrix of C.

i) $S(a+b) = (a+b)H^t = aH^t + bH^t = S(a) + S(b)$.

ii) $S(a) = 0$ means $aH^t = 0$. From Lemma 2.56, $aH^t = 0$ if and only if $a \in C$.

iii) If $S(a) = S(b)$, then $S(a) - S(b) = 0$. Then, from Part i), $S(a-b) = 0$. From Part ii), it follows that $a - b$ is a codeword in C if and only if $S(a-b) = 0$. So, a and b are in the same coset by Theorem 2.63 vi).

Definition 2.68 A table which matches each coset leader with its syndrome is called a *syndrome look up table*. This table is constructed by the following steps:

1) Find all cosets of the code and determine the coset leader a of each coset.
2) Calculate the syndrome of a as $S(a) = aH^t$ for each coset leader a where H is a parity-check matrix of the code.

Next, we will describe the decoding procedure.

Firstly, we construct the syndrome look up table. Let b a received word. Then, we compute the syndrome $S(b)$. The coset leader a is found such that $S(b) = S(a)$ in the table. The word b is decoded as $c = b - a$.

Example 2.69 We will construct the syndrome look up table of the linear code $C = \{0000000, 1101000, 0110100, 1011100, 1110010, 0011010, 1000110, 0101110, 1010001, 0111001, 1100101, 0001101, 0100011, 1001011, 0010111, 1111111\}$. A parity-check matrix of C is $H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$.

Example 2.70 The syndrome look up table and a parity-check matrix of the code is given in Table 2.2. We will decode $b = 1001111$.

We first compute $S(b) = bH^t = 011$. In the table, the syndrome 011 corresponds to the coset leader 0000100. Thus, $1001111 + 0000100 = 1001011$ is the most likely codeword which is transmitted.

Table 2. 2 Syndrome table of Example 2.69

Coset Leader a	Syndrome $S(a) = aH^t$
1000000	100
0100000	010
0010000	001
0001000	110
0000100	011
0000010	111
0000001	101
0000000	000

CHAPTER 3

QUANTUM COMPUTATION

The quantum mechanics has certain interesting properties. A quantum computer is a machine which is based on the quantum mechanics. In 1976, R.S. Ingarden published a paper which is titled ‘Quantum Information Theory’ [2]. It shows that Shannon’s classical information theory cannot be adapted to quantum world directly. However, a new information theory can be constructed which is based on quantum mechanics. In 1985, first quantum computer is described by David Deutsch [4]. Then, some quantum computers with small qubits are constructed up to the present.

Recently, there are many studies on quantum computers and they are developed day by day. If a successful quantum computer can be made with all expected properties, then the effects on cryptography and the other related disciplines will be significant.

We will begin with explaining the quantum mechanics to understand the structure of a quantum computer. Hence, in this chapter we introduce the quantum computation which is the fundamental of the quantum mechanics.

In this chapter, the books [27], [28], [29], [30], [31], [32], [33] and [34] are used.

3.1 Dirac Notation

The unit of a quantum computer is called a *quantum bit*, shortly a qubit. While a classical computer works with 0 and 1, a quantum computer works with the vectors $|0\rangle$ and $|1\rangle$ corresponding to 0 and 1 in the classical system, respectively. They are called *ket vectors*.

Besides these vectors, there exists another state in a quantum computer. It is called the quantum superposition.

There is a different notation used in quantum computation. This notation is discovered by Paul Dirac and so, it is known as Dirac notation. While in Physics and Mathematics the vectors are represented by a letter with an arrow, in quantum mechanics a vector is represented by a 'ket'. That is, if x is a vector, then it is denoted by $|x\rangle$. The dual of this vector is denoted by $\langle x|$ and it is known as 'bra'. The matrix representation of the bra vector is a row vector whose elements are complex conjugates of the ket vector. More formally, if $|x\rangle = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}$ then, $\langle x| = (\alpha_1{}^*, \alpha_2{}^*, \ldots, \alpha_n{}^*)$ where $\alpha_i{}^*$ denotes the complex conjugates of α_i for $1 \leq i \leq n$.

Let x be a sequence of length n. Then, the vector $|x\rangle$ corresponds to a column matrix of length 2^n. In fact, Dirac notation provides simplicity in presentation. In general, the set $\{|0\rangle, |1\rangle\}$ is used as a basis and it is called the computational basis (or standard basis). Vectors of length n can be listed by using the computational basis: $|00\ldots0\rangle$, $|00\ldots1\rangle$, $|00\ldots10\rangle$, $|11\ldots1\rangle$. Then, the columns matrices corresponding to these ket vectors can be written as follows:

$$|00\ldots0\rangle = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, |00\ldots1\rangle = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \ldots, |11\ldots1\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}.$$

The above vectors are 2^n $-$dimensional column vectors.

For a small example, assume that take $n = 1$. Then, there are two ket vectors $|0\rangle$ and $|1\rangle$. The column matrices corresponding to these vectors are as follows: $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

Example 3.1 Let $|\varphi\rangle = \frac{1}{\sqrt{5}}|00\rangle + \frac{2}{\sqrt{5}}|10\rangle$. Actually, $|\varphi\rangle = \frac{1}{\sqrt{5}}|0\rangle \otimes |0\rangle + \frac{2}{\sqrt{5}}|1\rangle \otimes |0\rangle$.

Alternatively, this expression is equivalent to a column vector $\begin{pmatrix} 1/\sqrt{5} \\ 0 \\ 2/\sqrt{5} \\ 0 \end{pmatrix}$.

The main reason of using Dirac notation is that it provides an easy representation. For instance, for a 10-qubit state we need a column vector which has 2^{10} components. It leads a complexity in representation. However, it can be represented by a sequence of length 10 if Dirac notation is used.

A Hilbert space is a vector space over complex numbers. An advantage of a Hilbert space is that it can be represented by a basis. So, this space is used in quantum computation.

Next, we will describe the dual space of a Hilbert space.

Definition 3.2 Let H be a Hilbert space. The set H^* is the set of linear transformation from H to $\mathbb{C}$ as $H \to \mathbb{C}$. The elements of H^* are denoted by $\langle T|$ and the action of $\langle T|$ is defined as $\langle T|: |\varphi\rangle \to \langle T|\varphi\rangle$ where $\langle T|\varphi\rangle$ is an inner product of $|T\rangle$ and $|\varphi\rangle$. The set H^* is also a vector space over complex numbers and it is called the *dual space* of H. The vector $\langle T|$ is the dual of $|T\rangle$. While $|T\rangle$ is a column vector, $\langle T|$ is a row vector which is constructed by the complex conjugates of elements of $|T\rangle$.

Example 3.3 Let $|\varphi_1\rangle = \frac{i}{\sqrt{5}}|00\rangle + \sqrt{\frac{6}{5}}|10\rangle$ and $|\varphi_2\rangle = \sqrt{\frac{2}{3}}|00\rangle + \sqrt{\frac{1}{3}}|11\rangle$. Matrix representations of $|\varphi_1\rangle$ and $|\varphi_2\rangle$ are $\begin{pmatrix} i/\sqrt{5} \\ 0 \\ \sqrt{6}/\sqrt{5} \\ 0 \end{pmatrix}$ and $\begin{pmatrix} \sqrt{2}/\sqrt{3} \\ 0 \\ 0 \\ 1/\sqrt{3} \end{pmatrix}$, respectively. Then,

$$\langle\varphi_1|\varphi_2\rangle = \begin{pmatrix} i/\sqrt{5} & 0 & \sqrt{6}/\sqrt{5} & 0 \end{pmatrix} \begin{pmatrix} \sqrt{2}/\sqrt{3} \\ 0 \\ 0 \\ 1/\sqrt{3} \end{pmatrix} = \frac{-\sqrt{2}i}{\sqrt{15}}.$$

Definition 3.4 Let $k_1, k_2, \dots, k_n \in \mathbb{C}$ and let $|x_1\rangle$, $|x_2\rangle$,…, $|x_n\rangle \in \mathbb{C}^{2^n}$ be ket vectors. The superposition of the vectors is also a vector. It can be written as $|\varphi\rangle = k_1|x_1\rangle + k_2|x_2\rangle + \cdots + k_n|x_n\rangle$ where $|k_1|^2 + |k_2|^2 + \cdots + |k_n|^2 = 1$. Here, $|k_i|^2$ denotes the possibilities of $|x_i\rangle$ where $1 \leq i \leq n$. The vector $|\varphi\rangle$ is called a *quantum superposition*.

In particular, let α, $\beta \in \mathbb{C}$ and let $|0\rangle$, $|1\rangle \in \mathbb{C}^2$. The vector $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$ is a quantum superposition acting on the single qubits.

The vector space which is used in the quantum computation is a finite dimensional vector space over complex numbers. Since Hilbert space is an example of such a vector space, it can be used in the quantum computation.

The set of complex numbers is a one-dimensional Hilbert space. The elements of two-dimensional Hilbert space are 2×1 column vectors whose components are complex numbers. More formally, let $\alpha, \beta \in \mathbb{C}$ then $\begin{pmatrix}\alpha\\ \beta\end{pmatrix} \in H^2$. For all $\begin{pmatrix}\alpha\\ \beta\end{pmatrix} \in H^2$, $\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \alpha\begin{pmatrix}1\\ 0\end{pmatrix} + \beta\begin{pmatrix}0\\ 1\end{pmatrix}$ where $\alpha, \beta \in \mathbb{C}$. Therefore, the set of the matrices $\left\{\begin{pmatrix}1\\ 0\end{pmatrix}, \begin{pmatrix}0\\ 1\end{pmatrix}\right\}$ is a basis for H^2.

Let $|\varphi\rangle$ be the superposition acting on the single qubits. Then, $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$. This vector corresponds to a matrix as $\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$. In other words, $\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$ is the matrix representation of $|\varphi\rangle$. Moreover, the matrix can be written as $\begin{pmatrix}\alpha\\ 0\end{pmatrix} + \begin{pmatrix}0\\ \beta\end{pmatrix} = \alpha\begin{pmatrix}1\\ 0\end{pmatrix} + \beta\begin{pmatrix}0\\ 1\end{pmatrix}$. Then, $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$ and $|\varphi\rangle = \alpha\begin{pmatrix}1\\ 0\end{pmatrix} + \beta\begin{pmatrix}0\\ 1\end{pmatrix}$. We obtain that the matrix representations of $|0\rangle$ and $|1\rangle$ as $\begin{pmatrix}1\\ 0\end{pmatrix}$ and $\begin{pmatrix}0\\ 1\end{pmatrix}$, respectively.

Note that if $|x\rangle = \begin{pmatrix}x_1\\ x_2\\ \vdots\\ x_n\end{pmatrix}$, $|y\rangle = \begin{pmatrix}y_1\\ y_2\\ \vdots\\ y_n\end{pmatrix} \in \mathbb{C}^n$ and $k \in \mathbb{C}$, then

i) $|x\rangle + |y\rangle = \begin{pmatrix}x_1 + y_1\\ x_2 + y_2\\ \vdots\\ x_n + y_n\end{pmatrix}$,

ii) $k|x\rangle = \begin{pmatrix}kx_1\\ kx_2\\ \vdots\\ kx_n\end{pmatrix}$.

3.2 Some Linear Algebra about the Quantum Vectors

In quantum systems, Hilbert space is used since it has better algebraic properties. Qubits which are units of quantum computers correspond to vectors in the space. Since we mention about vectors, they have some algebraic properties. These properties provide simplicity in the computation.

Now, we will explain some linear algebraic properties of the quantum vectors.

1) Let $k_1, k_2, \dots, k_n \in \mathbb{C}$ and $|x_1\rangle$, $|x_2\rangle$,…, $|x_n\rangle$ be quantum vectors. If the sum $k_1|x_1\rangle + k_2|x_2\rangle + \cdots + k_n|x_n\rangle = 0$ implies $k_1 = k_2 = \cdots = k_n = 0$, then the set of $\{|x_1\rangle$, $|x_2\rangle$,…, $|x_n\rangle\}$ is called *linearly independent.*
2) There may be many spanning sets and the minimal spanning set is a basis. Therefore, spanning set is not unique.

Example 3.5 Let $|x_1\rangle = \begin{pmatrix}1\\1\end{pmatrix}$ and $|x_2\rangle = \begin{pmatrix}1\\-1\end{pmatrix}$. Assume that we have $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$. This superposition state corresponds to the column matrix $\begin{pmatrix}\alpha\\\beta\end{pmatrix}$. Then,

$$|\varphi\rangle = \begin{pmatrix}\alpha\\\beta\end{pmatrix} = \begin{pmatrix}\alpha\\0\end{pmatrix} + \begin{pmatrix}0\\\beta\end{pmatrix} = \frac{1}{2}\begin{pmatrix}\alpha+\alpha\\\alpha-\alpha\end{pmatrix} + \frac{1}{2}\begin{pmatrix}\beta-\beta\\\beta+\beta\end{pmatrix}$$

$$= \frac{1}{2}\begin{pmatrix}\alpha\\\alpha\end{pmatrix} + \frac{1}{2}\begin{pmatrix}\alpha\\-\alpha\end{pmatrix} + \frac{1}{2}\begin{pmatrix}\beta\\\beta\end{pmatrix} + \frac{1}{2}\begin{pmatrix}-\beta\\\beta\end{pmatrix}$$

$$= \frac{1}{2}\alpha\begin{pmatrix}1\\1\end{pmatrix} + \frac{1}{2}\alpha\begin{pmatrix}1\\-1\end{pmatrix} + \frac{1}{2}\beta\begin{pmatrix}1\\1\end{pmatrix} - \frac{1}{2}\beta\begin{pmatrix}1\\-1\end{pmatrix}$$

$$= \frac{\alpha+\beta}{2}\begin{pmatrix}1\\1\end{pmatrix} + \frac{\alpha-\beta}{2}\begin{pmatrix}1\\-1\end{pmatrix} = \frac{\alpha+\beta}{2}|x_1\rangle + \frac{\alpha-\beta}{2}|x_2\rangle.$$

This shows that $\{|0\rangle, |1\rangle\}$ and $\{|x_1\rangle, |x_2\rangle\}$ are two distinct spanning sets of $|\varphi\rangle$.

3) A vector space may have more than one basis. However, the size of each basis should be the same. In Example 3.5, $\{|0\rangle, |1\rangle\}$ and $\{|x_1\rangle, |x_2\rangle\}$ are two bases for $|\varphi\rangle$.
4) Let $|x_1\rangle$ and $|x_2\rangle$ be two vectors. The inner product of $|x_1\rangle$ and $|x_2\rangle$ is denoted by $\langle x_1|x_2\rangle$. The result of an inner product is a complex number. If the result is zero; that is, $\langle x_1|x_2\rangle = 0$, then $|x_1\rangle$ and $|x_2\rangle$ are called *orthogonal.* The notation $(\langle x_1|x_2\rangle)^*$ denotes the complex conjugate of $\langle x_1|x_2\rangle$ and we can find as $(\langle x_1|x_2\rangle)^* = \langle x_2|x_1\rangle$.

5) The *norm* of any vector $|x_1\rangle$ is defined as $\|x_1\| = \sqrt{\langle x_1|x_1\rangle}$. The result of a norm is a real number. A norm satisfies the following properties:

i) The inner product $\langle x_1|x_1\rangle = 0$ if and only if $|x_1\rangle = 0$.

ii) $\langle x_1|ax_2 + bx_3\rangle = a\langle x_1|x_2\rangle + b\langle x_1|x_3\rangle$.

iii) $\langle ax_1 + bx_2|x_3\rangle = a\langle x_1|x_3\rangle + b\langle x_2|x_3\rangle$.

iv) $(|x_1\rangle)^+ = \langle x_1|$.

Let $|x_1\rangle = \begin{pmatrix}\gamma_1\\ \gamma_2\\ \vdots\\ \gamma_n\end{pmatrix}$ and $|x_2\rangle = \begin{pmatrix}\theta_1\\ \theta_2\\ \vdots\\ \theta_n\end{pmatrix}$ be ket vectors. Note that the dual of the vector is that $(|x_1\rangle)^+ = \begin{pmatrix}\gamma_1\\ \gamma_2\\ \vdots\\ \gamma_n\end{pmatrix}^+ = (\gamma_1{}^*, \gamma_2{}^*, \ldots, \gamma_n{}^*) = \langle x_1|$ and $\langle x_1|x_2\rangle = (\gamma_1{}^*, \gamma_2{}^*, \ldots, \gamma_n{}^*)\begin{pmatrix}\theta_1\\ \theta_2\\ \vdots\\ \theta_n\end{pmatrix} = \sum_{i=1}^{n} \gamma_i{}^*\theta_1$.

6) If the norm of a vector is 1, then this vector is called a *normal vector*. If each vector of a set is normal and the vectors are pairwise, the set is called an *orthonormal set*.

Example 3.6 Let $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$. We know that $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$ and $|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$. Then, the inner products are evaluated as follows: $\langle 0|0\rangle = (1\ 0)\begin{pmatrix}1\\0\end{pmatrix} = 1, \langle 1|1\rangle = (0\ 1)\begin{pmatrix}0\\1\end{pmatrix} = 1, \langle 1|0\rangle = (0\ 1)\begin{pmatrix}1\\0\end{pmatrix} = 0, \langle 0|1\rangle = (1\ 0)\begin{pmatrix}0\\1\end{pmatrix} = 1$. Hence, $\{|0\rangle, |1\rangle\}$ is an orthonormal set since $\|0\| = \|1\| = 1$ and $\langle 1|0\rangle = \langle 0|1\rangle = 0$.

3.3 Matrices and Operators

In quantum computation, matrices and operators play an important role. Each action corresponds to a matrix or operator and it can be represented by a matrix.

First, we will give definition of an operator.

Definition 3.7 An *operator* is a linear transformation from a vector space to the same vector space.

The outer product of $|\varphi_1\rangle$ and $|\varphi_2\rangle$ is denoted by $|\varphi_1\rangle\langle\varphi_2|$ and it is an operator. If this product is applied on $|x\rangle$, then

$$(|\varphi_1\rangle\langle\varphi_2|)|x\rangle = |\varphi_1\rangle(\langle\varphi_2|x\rangle) = (\langle\varphi_2|x\rangle)|\varphi_1\rangle.$$

Let A be an operator and $|x_1\rangle$, $|x_2\rangle$ be two vectors. If $A|x_1\rangle = |x_1\rangle$, then A is said to be an operator which transforms into ket to ket. If $\langle x_2|A = \langle x_2|$, then A is said to be an operator which transforms into bra to bra.

Definition 3.8

i) If $I|\mathrm{x}_1\rangle = |\mathrm{x}_1\rangle$, then I is called *identity operator*.

ii) If $0|\mathrm{x}_1\rangle = 0$, then 0 is called *zero operator*.

iii) If $A(a|\mathrm{x}_1\rangle + b|\mathrm{x}_2\rangle)$ can be written as $a(A|\mathrm{x}_1\rangle + b(A|\mathrm{x}_2\rangle)$, then A is called a *linear operator*.

3.3.1 Pauli Matrices

There are four special matrices such that they have fundamental importance in the quantum computation. These matrices which act on a single qubit are known as the Pauli matrices and they are denoted by X, Y, Z, I [27]. The Pauli matrices are defined as follows:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{3.1}$$

Next, we will give the operator forms of the Pauli matrices by using the matrix representations.

First, $X|0\rangle$ and $X|1\rangle$ are evaluated as:

$$X|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle, X|1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle.$$

Second, actions of Y on $|0\rangle$ and $|1\rangle$ are evaluated:

$$Y|0\rangle = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ i \end{pmatrix} = i\begin{pmatrix} 0 \\ 1 \end{pmatrix} = i|1\rangle, Y|1\rangle = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -i \\ 0 \end{pmatrix} = -i\begin{pmatrix} 1 \\ 0 \end{pmatrix} = -i|0\rangle.$$

Lastly, actions of Z and I are evaluated as:

$$Z|0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle, Z|1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = -\begin{pmatrix} 0 \\ 1 \end{pmatrix} = -|1\rangle.$$

$$I|0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle, I|1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle.$$

X is known as NOT operator since $|0\rangle$ is transformed into $|1\rangle$ and $|1\rangle$ is transformed into $|0\rangle$.

Conversely, we will obtain the matrix representation by using the action of an operator. Let A be an operator. Then, it can be written as follow:

$$A = IAI = \left(\sum_i |x_i\rangle\langle x_i|\right) A \left(\sum_j |x_j\rangle\langle x_j|\right) = \sum_{i,j} \langle x_i|A|x_j\rangle |x_i\rangle\langle x_j| \tag{3.2}$$

since $\sum_i |x_i\rangle\langle x_i| = I$ where $|x_i\rangle$ is the basis vectors.

Example 3.9 Find the matrix representation of the Pauli matrix X. We know that $X|0\rangle = |1\rangle$ and $X|1\rangle = |0\rangle$. By using the formula,

$$X = \begin{pmatrix} \langle 0|X|0\rangle & \langle 0|X|1\rangle \\ \langle 1|X|0\rangle & \langle 1|X|1\rangle \end{pmatrix} = \begin{pmatrix} \langle 0|(X|0\rangle) & \langle 0|(X|1\rangle) \\ \langle 1|(X|0\rangle) & \langle 1|(X|1\rangle) \end{pmatrix} = \begin{pmatrix} \langle 0|1\rangle & \langle 0|0\rangle \\ \langle 1|1\rangle & \langle 1|0\rangle \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

where $|0\rangle$ and $|1\rangle$ are the basis vectors.

3.3.2 Hermitian, Unitary and Normal Operators

Some special type of operators play an important role in the quantum computation. The Hermitian adjoint of an operator A is denoted by A^+ and it is defined as $\langle a|A^+|b\rangle = \langle b|A|a\rangle^*$.

1) $(aA)^* = a^* A^+$
2) $(|\varphi\rangle)^+ = \langle\varphi|$
3) $(\langle\varphi|)^+ = |\varphi\rangle$
4) $(AB)^+ = B^+ A^+$
5) $(A|\varphi\rangle)^+ = \langle\varphi|A^+$
6) $(AB|\varphi\rangle)^+ = \langle\varphi|B^+ A^+$
7) $(A + B + C)^+ = A^+ + B^+ + C^+$

Definition 3.10 Let A be an operator.

i) If $A = A^+$, then A is called a *Hermitian operator*. Each of the Pauli operators is a Hermitian operator.
ii) If $AA^+ = I = A^+A$, then A is called a *unitary operator*. The Pauli operators are unitary operators.
iii) If $AA^+ = A^+A$, then A is called a *normal operator*.

iv) If $A|\varphi\rangle = \lambda|\varphi\rangle$ where $\lambda \in \mathbb{C}$, then λ is called an *eigenvalue* of A and $|\varphi\rangle$ is called an *eigenvector* of A that corresponds to λ. The characteristic equation of A is $det|A - \lambda I| = 0$.

v) An operator A can be written as $\sum_i \lambda_i |x_i\rangle\langle x_i|$ where λ_i is an eigenvalue of A and $|x_i\rangle$ is a basis vector. This expression is called a *spectral decomposition* of A. For instance, the Pauli operator Z can be written as $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$. Here, 1 and -1 are eigenvalues of Z.

Now, we will give a formal definition of spectral decomposition.

Definition 3.11 Let A be a normal operator which acts on a Hilbert space H. The vectors $|x_i\rangle$ form an orthonormal basis for A where each $|x_i\rangle$ is an eigenvector of A. The operator A can be written as A=$\sum_i \lambda_i |x_i\rangle\langle x_i|$ where λ_i is an eigenvalue of A. This expression is called the *spectral decomposition*. The set of eigenvalues of A is called the *spectrum* of A.

Theorem 3.12 For every finite dimensional normal matrix A, there exist a unitary matrix U such that $A = UDU^+$ where D is a diagonal matrix. The diagonal elements of D are eigenvalues of A and the columns of U are the eigenvectors of D.

Example 3.13 Consider that Pauli operator X whose action is as follows: $X|0\rangle = |1\rangle$ and $X|1\rangle = |0\rangle$. The matrix representation of this operator is $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. It can be diagonalized as follows:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}.$$

Here, $U = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$ is a unitary matrix and $D = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ is a diagonal matrix. The eigenvalues of X are 1 and -1. The eigenvectors of X corresponding to these eigenvalues are $\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$ and $\begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$, respectively. In dirac notation, these matrices are denoted by

$$X = |0\rangle\langle 1| + |1\rangle\langle 0|,$$

$$U = \frac{1}{\sqrt{2}}|0\rangle\langle 0| + \frac{1}{\sqrt{2}}|0\rangle\langle 1| + \frac{1}{\sqrt{2}}|1\rangle\langle 0| - \frac{1}{\sqrt{2}}|1\rangle\langle 1|,$$

$$D = |0\rangle\langle 0| - |1\rangle\langle 1|.$$

Definition 3.14 Let A be an operator. The *trace* of A is defined by $Tr(A) = \sum_i \langle x_i|A|x_i\rangle$ where $|x_i\rangle$ are basis vectors.

Example 3.15 Let $A = 5|0\rangle\langle 0| - 2|0\rangle\langle 1| + 3i|1\rangle\langle 0| + i|1\rangle\langle 1|$ and let $\{|0\rangle,|1\rangle\}$ be the set of basis vectors. From Definition 3.14,

$$Tr(A) = \sum_i \langle x_i|A|x_i\rangle = \langle 0|A|0\rangle + \langle 1|A|1\rangle.$$

$Tr(A) = \langle 0|(5|0\rangle\langle 0|{-}2|0\rangle\langle 1|{+}3i|1\rangle\langle 0|{+}i|1\rangle\langle 1|)|0\rangle +$ $\langle 1|(5|0\rangle\langle 0|{-}2|0\rangle\langle 1|{+}3i|1\rangle\langle 0|{+}i|1\rangle\langle 1|)|1\rangle = (5\langle 0|0\rangle\langle 0|0\rangle - 2\langle 0|0\rangle\langle 1|0\rangle +$ $3i\langle 0|1\rangle\langle 0|0\rangle + i\langle 0|1\rangle\langle 1|0\rangle) + (5\langle 1|0\rangle\langle 0|1\rangle - 2\langle 1|0\rangle\langle 1|1\rangle + 3i\langle 1|1\rangle\langle 0|1\rangle +$ $i\langle 1|1\rangle\langle 1|1\rangle) = 5 + i.$

Remark 3.16 Let A and B be two operators and let $k \in \mathbb{C}$. Then, $Tr(kA) = kTr(A)$ and $Tr(A + B) = Tr(A) + Tr(B)$. In other words, trace is a linear function.

3.3.3 Projection Operators

If an operator P can be written as $P = |\varphi\rangle\langle\varphi|$, then it is called a *projection operator*. A projection operator satisfies the following properties:

i) If P is a projection operator, then it is Hermitian; that is, $P^+ = P$.

ii) A projection operator P satisfies $P^2 = P$.

iii) Projection operators commute. More formally, if P_1 and P_2 are two projection operators, then $P_1P_2 = P_2P_1$.

A spectral decomposition can be rewritten by using the projection operators. Let A be any operator and let $|x_i\rangle$ be basis vectors. Then, $\sum_i \lambda_i\, |x_i\rangle\langle x_i|$ where λ_i are eigenvalues of A. Hence, $A = \sum_i \lambda_i\, P_i$ since $P_i = |x_i\rangle\langle x_i|$ projects onto the subspace that is defined by eigenvalue λ_i.

Example 3.17 We will describe the projection operators with respect to the computational basis.

The set $\{|0\rangle, |1\rangle\}$ is the computational basis. The projection operators are defined by

$$P_0 = |0\rangle\langle 0| = \begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}1 & 0\end{pmatrix} = \begin{pmatrix}1 & 0\\0 & 0\end{pmatrix},$$

$$P_1 = |1\rangle\langle 1| = \begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}0 & 1\end{pmatrix} = \begin{pmatrix}0 & 0\\0 & 1\end{pmatrix}.$$

3.3.4 Hadamard Matrix

[27] There is another matrix that is important in quantum mechanics besides from the Pauli matrices. This matrix which acts on a single qubit is called the *Hadamard matrix* and it is defined by

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}. \tag{3.3}$$

If the Hadamard matrix acts on the vector $|0\rangle$ and $|1\rangle$, then it gives $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$, respectively. More formally, the action of the Hadamard matrix is

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

The Hadamard matrix has a property that if it is applied twice on a quantum state, then it returns to the initial state. To illustrate this, we assume $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$. Then,

$$\begin{aligned} H|\varphi\rangle = H(\alpha|0\rangle + \beta|1\rangle) = \alpha H|0\rangle + \beta H|1\rangle &= \alpha\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) + \beta\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \\ &= \frac{\alpha+\beta}{\sqrt{2}}|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1\rangle \end{aligned}$$

If we apply the Hadamard matrix to last equation one more time, then

$$\begin{aligned} H\left(\frac{\alpha+\beta}{\sqrt{2}}|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1\rangle\right) &= \frac{\alpha+\beta}{\sqrt{2}}H|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}H|1\rangle \\ &= \frac{\alpha+\beta}{\sqrt{2}}\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) + \frac{\alpha-\beta}{\sqrt{2}}\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \\ &= \alpha|0\rangle + \beta|1\rangle = |\varphi\rangle. \end{aligned}$$

Therefore, we obtain the initial quantum state.

3.3.5 CNOT Gate

[27] CNOT gate acts on two qubits, while some operators like Pauli operators and the Hadamard gate act on a single qubit. Here, the first qubit is a check qubit and the second qubit is a target qubit. If the first qubit is 0, then the second qubit is not changed. But, if the first qubit is 1, then the Pauli matrix X is applied on the second qubit. In other words, $|00\rangle$ and $|01\rangle$ are not changed. However, $|10\rangle$ and $|11\rangle$ are transformed into $|11\rangle$ and $|10\rangle$, respectively. The matrix representation of CNOT gate is defined by

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{3.4}$$

3.4 Tensor Product

We use qubits when we make some computations in the quantum theory. However, in some cases, we need more complex structures which are constructed with more than one qubit. Tensor product is used to construct a structure that is a composite of the qubits. Hence, a Hilbert space that is a composite of independent Hilbert spaces can be constructed. Assume that H_1 and H_2 are two Hilbert spaces of dimensions k_1 and k_2, respectively. A larger Hilbert space can be constructed by composing H_1 and H_2. This construction is obtained by tensor product and it is denoted by $\otimes$.

Let $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ and $B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$. Then,

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B \\ a_{21}B & a_{22}B \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{pmatrix}.$$

Tensor product of $|\varphi_1\rangle$ and $|\varphi_2\rangle$ can be denoted by $|\varphi_1\rangle \otimes |\varphi_2\rangle$, $|\varphi_1\rangle|\varphi_2\rangle$ or $|\varphi_1\varphi_2\rangle$.

Let $|\varphi_1\rangle$, $|\varphi_2\rangle$ and $|\varphi_3\rangle$ be three quantum states and let $k \in \mathbb{C}$. Then, tensor product has the following properties:

i) $|\varphi_1\rangle \otimes (|\varphi_2\rangle + |\varphi_3\rangle) = |\varphi_1\rangle \otimes |\varphi_2\rangle + |\varphi_1\rangle \otimes |\varphi_3\rangle$

ii) $(|\varphi_1\rangle + |\varphi_2\rangle) \otimes |\varphi_3\rangle = |\varphi_1\rangle \otimes |\varphi_3\rangle + |\varphi_2\rangle \otimes |\varphi_3\rangle$

iii) $k|\varphi_1\rangle \otimes |\varphi_2\rangle = |\varphi_1\rangle \otimes k|\varphi_2\rangle$

iv) If A_1 and A_2 are two operators, then $(A_1 \otimes A_2)(\,|\varphi_1\rangle \otimes |\varphi_2\rangle) = A_1|\varphi_1\rangle \otimes A_2|\varphi_2\rangle$.

Example 3.18 Let $A = \begin{pmatrix} i & 4 \\ 6 & -2i \end{pmatrix}$ and $B = \begin{pmatrix} 2 \\ i \end{pmatrix}$. Then,

$$A \otimes B = \begin{pmatrix} 2i & 8 \\ -1 & 4i \\ 12 & -4i \\ 6i & 2 \end{pmatrix}.$$

Note that if we take the standard orthonormal basis $\{|0\rangle, |1\rangle\}$, then

- $|0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$,
- $|0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$,
- $|1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$,
- $|1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$.

Remark 3.19 The Pauli operators act on a single qubit. However, they can act on more qubits by combining them with tensor product.

Example 3.20 Let XZY be an operator and $|110\rangle$ be a quantum state. Actually, XZY is defined as the tensor product of X, Z and Y; that is, $XZY = X \otimes Z \otimes Y$. The state $|110\rangle$ can be written as $|1\rangle \otimes |1\rangle \otimes 0\rangle$. Then, $XZY|110\rangle = (X \otimes Z \otimes Y)(|1\rangle \otimes |1\rangle \otimes 0\rangle)$. By using the properties of tensor product, we obtain $X|1\rangle \otimes Z|1\rangle \otimes Y|0\rangle = |0\rangle \otimes -|1\rangle \otimes i|1\rangle = -i|0\rangle \otimes |1\rangle \otimes |1\rangle$. This result can also be written as $-i|011\rangle$.

3.5 Measurement

A quantum system is affected via measurement, whereas classical systems are not affected by measurement. Measurement is a crucial part of quantum mechanics. The state of the system cannot be known, before a measurement is made in a quantum system. Hence, measurement is necessary to determine the system which is uncertain. For example, let's consider a superposition $\alpha|0\rangle + \beta|1\rangle$. Here, α and β denote the square root of the possibilities of $|0\rangle$ and $|1\rangle$, respectively. When a measurement is made, only $|0\rangle$ and $|1\rangle$ will be obtained. However, the possibilities α and β may change in the superposition and so this leads to a deformation in the quantum state. In other words, measurement leads a damage of the initial state.

3.6 Entanglement

In quantum mechanics, systems can become entangled. Systems A_1 and A_2 may affect each other. Even if A_1 and A_2 are separated, the properties of them can become correlated. This idea leads to a new approach which is called *quantum entanglement*.

The idea of entanglement dates to 1935. Einstein, Podolsky and Rosen published a paper which is titled as "Can the quantum mechanical description of reality be considered complete?" [36]. After this paper was published, a new term is introduced to quantum mechanics.

If we have two Hilbert spaces H_1 and H_2, then a composite system of them can be written as $H = H_1 \otimes H_2$. In many cases, these two spaces interact with each other and so it is not possible to separate into two independent components. Thus, they cannot be thought as two independent spaces.

Let $|\alpha_i\rangle$ and $|\beta_i\rangle$ be basis for H_1 and H_2, respectively. Then, $|\alpha_i\rangle \otimes |\beta_i\rangle = |\alpha_i\rangle|\beta_i\rangle = |\alpha_i\beta_i\rangle$ is a basis for composite system H.

The quantum state of each particle cannot be described independently of the others, even when the particles are separated. Actually, a state must be described for the system as a whole.

Definition 3.21 The states which are dependent to each other are called *entangled systems*.

There are four special entangled pairs. They are known as Bell states [37] which are defined by

1) $|\beta_0\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$,
2) $|\beta_1\rangle = \frac{|01\rangle+|10\rangle}{\sqrt{2}}$,
3) $|\beta_2\rangle = \frac{|00\rangle-|11\rangle}{\sqrt{2}}$,
4) $|\beta_3\rangle = \frac{|01\rangle-|10\rangle}{\sqrt{2}}$.

If two systems are entangled, then the composite system of them can only be described as related to the other system. Otherwise, they can be written as a product of each system and the systems are called separable. There are some methods to determine whether the systems are entangled.

3.6.1 Method 1

The following method can be applied to vectors in $\mathbb{C}^4$. Let $|\varphi\rangle = \begin{pmatrix}\alpha_1\\ \alpha_2\\ \alpha_3\\ \alpha_4\end{pmatrix}$. This vector is not entangled if and only if $\alpha_1\alpha_4 = \alpha_2\alpha_3$.

Example 3.22

i) $|\beta_0\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\left[\begin{pmatrix}1\\0\\0\\0\end{pmatrix}+\begin{pmatrix}0\\0\\0\\1\end{pmatrix}\right] = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}$. Here, $\alpha_1 = \alpha_4 = \frac{1}{\sqrt{2}}$ and $\alpha_2 = \alpha_3 = 0$. Then, $\alpha_1\alpha_4 \neq \alpha_2\alpha_3$. Hence, $|\beta_0\rangle$ is entangled.

ii) $|\beta_1\rangle = \frac{|01\rangle+|10\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\left[\begin{pmatrix}0\\1\\0\\0\end{pmatrix}+\begin{pmatrix}0\\0\\1\\0\end{pmatrix}\right] = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\1\\0\end{pmatrix}$. Here, $\alpha_1 = \alpha_4 = 0$ and $\alpha_2 = \alpha_3 = \frac{1}{\sqrt{2}}$. Then, $\alpha_1\alpha_4 \neq \alpha_2\alpha_3$. Hence, $|\beta_1\rangle$ is entangled.

iii) $|\beta_2\rangle = \frac{|00\rangle-|11\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\left[\begin{pmatrix}1\\0\\0\\0\end{pmatrix}-\begin{pmatrix}0\\0\\0\\1\end{pmatrix}\right] = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\-1\end{pmatrix}$. Here, $\alpha_1 = \frac{1}{\sqrt{2}}$, $\alpha_4 = -\frac{1}{\sqrt{2}}$ and $\alpha_2 = \alpha_3 = 0$. Then, $\alpha_1\alpha_4 \neq \alpha_2\alpha_3$. Hence, $|\beta_2\rangle$ is entangled.

iv) $|\beta_3\rangle = \frac{|01\rangle-|10\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\left[\begin{pmatrix}0\\1\\0\\0\end{pmatrix} - \begin{pmatrix}0\\0\\1\\0\end{pmatrix}\right] = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\-1\\0\end{pmatrix}$. Here, $\alpha_1 = \alpha_4 = 0$ and $\alpha_2 = \frac{1}{\sqrt{2}}$, $\alpha_3 = -\frac{1}{\sqrt{2}}$. Then, $\alpha_1\alpha_4 \neq \alpha_2\alpha_3$. Hence, $|\beta_3\rangle$ is entangled.

Therefore, the Bell states are entangled.

Example 3.23 We will determine whether $H \otimes X|11\rangle$ is entangled. Firstly,

$$\left[\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix} \otimes \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\right]\begin{pmatrix}0\\0\\0\\1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}0 & 1 & 0 & 1\\1 & 0 & 1 & 0\\0 & 1 & 0 & -1\\1 & 0 & -1 & 0\end{pmatrix}\begin{pmatrix}0\\0\\0\\1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\-1\\0\end{pmatrix}.$$

So, $\alpha_1 = 1$, $\alpha_2 = 0$, $\alpha_3 = -1$ and $\alpha_4 = 0$. Then, $\alpha_1\alpha_4 = \alpha_2\alpha_3$. Thus, $H \otimes X|11\rangle$ is not entangled. It is separable. This separation can be written as $(|0\rangle - |1\rangle) \otimes \frac{1}{\sqrt{2}}|0\rangle$.

Note that we can also mention about entangled matrix similar to a quantum state.

Example 3.24 Let $A = \begin{pmatrix}0 & 0 & -1 & 0\\0 & 0 & 0 & -1\\1 & 0 & 0 & 0\\0 & -1 & 0 & 0\end{pmatrix}$. This matrix can be written as tensor product of two Pauli matrices: $X \otimes Z = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix} \otimes \begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}$. So, A is a separable matrix.

Note that the matrix representation of CNOT cannot be separated as tensor product of any two matrices. Hence, CNOT is an example of entangled matrix.

3.6.2 Method 2 (Schmidt Decomposition)

Assume that H is a composite system which can be written as $H_1 \otimes H_2$. Let $|\varphi\rangle \in H_1 \otimes H_2$. Then, $|\varphi\rangle$ can be expressed as follows:

$$|\varphi\rangle = \sum_i \lambda_i\, |\alpha_i\rangle|\beta_i\rangle \tag{3.5}$$

where $|\alpha_i\rangle$ and $|\beta_i\rangle$ are orthonormal bases for H_1 and H_2, respectively. Here, $\lambda_i \geq 0$ and $\sum_i {\lambda_i}^2 = 1$. The number λ_i is called *Schmidt coefficients* and Equation 3.5 is said to be *Schmidt decomposition*. The number λ_i is evaluated as $Tr(|\varphi\rangle\langle\varphi|)$. The eigenvalues of this matrix are ${\lambda_i}^2$. The number of nonzero eigenvalues λ_i are the Schmidt numbers [38].

These numbers are denoted by *Sch*. Some properties of the Schmidt numbers are the following:

i) A state is entangled if the Schmidt number is greater than 1.

ii) A state is separable if the Schmidt number is 1.

Example 3.25 Consider $|\varphi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle + |01\rangle + |11\rangle)$. Then, we obtain

$|\varphi\rangle\langle\varphi| = \frac{1}{2}(|00\rangle\langle 00| + |00\rangle\langle 10| + |00\rangle\langle 01| + |00\rangle\langle 11| + |10\rangle\langle 00| + |10\rangle\langle 10| + |10\rangle\langle 01| + |10\rangle\langle 11| + |01\rangle\langle 00| + |01\rangle\langle 10| + |01\rangle\langle 01| + |01\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 10| + |11\rangle\langle 01| + |11\rangle\langle 11|)$. Also,

$$Tr(|\varphi\rangle\langle\varphi|) = \langle 0|\varphi\rangle\langle\varphi|0\rangle + \langle 1|\varphi\rangle\langle\varphi|1\rangle$$

$$= |0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1| + |0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|$$

$$= \frac{1}{2}(2|0\rangle\langle 0| + 2|0\rangle\langle 1| + 2|1\rangle\langle 0| + 2|1\rangle\langle 1| = |0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|$$

$$= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}.$$

The eigenvalues of this matrix are $\lambda_1 = 0$ and $\lambda_1 = 2$. There is one nonzero eigenvalue. Hence, this state is separable since $Sch = 1$. This separation is $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle)$.

CHAPTER 4

QUANTUM ERROR CORRECTING CODES

In this chapter, some types of quantum error correcting codes are analyzed and illustrated with examples. Generally, we take the advantage of reference [29].

4.1 Quantum Error Correcting Codes

Error correction is necessary during a data transmission. When a message is sent, some errors may occur in the communication channel. Some codes are used to correct these errors.

In a quantum system, error correction procedure is different from classical one. A distinct approach is needed for error correction since quantum systems are based on quantum mechanics. Hence, a new method based on quantum mechanics should be constructed.

There are some differences between quantum and classical error corrections. These are described below.

A quantum state cannot be dublicated. So, repetition codes do not exist as in the classical systems.

While there is only bit flip errors in the classical systems, addition to this error there is also phase flip errors in the quantum systems. In other words, error types are more complicated in the quantum systems. Thus, error detection and correction procedures are more complicated.

We need to make a measurement to determine the quantum state in a quantum system. However, measurements destroy a quantum state. We cannot determine the coefficients of a quantum superposition. Therefore, a quantum state cannot be exactly described.

4.2 Error Types in Quantum States

There are three types of errors. First, we will describe bit flip error.

The vectors $|0\rangle$ and $|1\rangle$ transform into $|1\rangle$ and $|0\rangle$, respectively. This error is similar to the classical bit flip error. If we have a quantum state $\alpha|0\rangle + \beta|1\rangle$, then it is transformed into $\beta|0\rangle + \alpha|1\rangle$. In quantum systems, every error can be represented by an operator. So, Pauli X operator leads to a bit flip error. In other words, a quantum bit flip error can be represented by an X operator.

Second, we will describe phase flip error.

The vectors $|0\rangle$ and $|1\rangle$ transform into $|0\rangle$ and $-|1\rangle$, respectively. This type of error is different from the classical systems. If we have a quantum state $\alpha|0\rangle + \beta|1\rangle$, then it is transformed into $\alpha|0\rangle - \beta|1\rangle$. Pauli Z operator leads to a phase flip error.

Lastly, we will describe mixed bit and phase flip errors.

The vectors $|0\rangle$ and $|1\rangle$ transform into $|1\rangle$ and $-|0\rangle$, respectively. If we have a quantum state $\alpha|0\rangle + \beta|1\rangle$, then it is transformed into $\beta|0\rangle - \alpha|1\rangle$. Pauli Y operator leads to this error.

Basically, these errors that act on single qubit are detected by helping projection operators. Suppose that we have a quantum state $\alpha|0\rangle + \beta|1\rangle$. Firstly, it is transformed into 3-qubit flip code in order to detect any error acting single qubit. 3-qubit code send one qubit three times. Hence, this code can be called repetition code. But, it should not interpret like classical repetition code. Because, arbitrary quantum state cannot be copied. 3-qubit flip code is constructed by applying CNOT operator:

1 original qubit and 2 ancilla qubits are used to encoding. Firstly, $\alpha|0\rangle + \beta|1\rangle$ is transformed into$|\varphi_{123}\rangle = \alpha|000\rangle + \beta|100\rangle$. Secondly, CNOT is applied on the first and second qubit:

$$CNOT_{12}(\alpha|000\rangle + \beta|100\rangle) = \alpha|000\rangle + \beta|110\rangle.$$

Lastly, CNOT is applied on the first and third qubit:

$$CNOT_{13}(\alpha|000\rangle + \beta|110\rangle) = \alpha|000\rangle + \beta|111\rangle.$$

Therefore, $\alpha|\bar{0}\rangle + \beta|\bar{1}\rangle$ is constructed where $|\bar{0}\rangle = |000\rangle$ and $|\bar{1}\rangle = |111\rangle$.

Some projection operators are used to error detection procedure:

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|$$
$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$$
$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$$
$$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$$

If error occurred on ith qubit and the state is transformed into $|\varphi_i\rangle$, then $\langle \varphi_i \, \big| \, P_j \, \big| \, \varphi_i \, \rangle = \delta_{ij}$.

Example 4.1 Assume that we have $\alpha|010\rangle + \beta|101\rangle$. We need to determine place of the error.

$$\langle \varphi_i | P_0 | \varphi_i \, \rangle = 0, \langle \varphi_i | P_1 | \varphi_i \, \rangle = 0, \langle \varphi_i | P_2 | \varphi_i \, \rangle = 1, \qquad \langle \varphi_i \, \big| \, P_3 \, \big| \, \varphi_i \, \rangle = 0$$

If we apply these operators on the state with error, then we obtain 0, 0, 1 and 0, respectively. The vector [0,0,1,0] is the syndrome vector of the state and it shows that an error occurred on the second qubit.

Actually, P_i corresponds to $8x8$ matrix. For instance, P_0 is represented as:

$$P_0 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} (1\;0\;0\;0\;0\;0\;0\;0) + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} (0\;0\;0\;0\;0\;0\;0\;1)$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Next, we will give a theorem that is the main difference between quantum and classical error correction.

Theorem 4.2 [27] Let $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$ be a quantum state where $\alpha, \beta \in \mathbb{C}$. Then, $|\varphi\rangle$ can be cloned only when $\alpha\beta = 0$. More formally, there is no operator that clones an arbitrary quantum state.

Proof. Let $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$. The copied state as follow:

$$\begin{aligned}|\varphi\rangle|\varphi\rangle &= (\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle)\\ &= \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle.\end{aligned}$$

It is possible only when $\alpha\beta = 0$. Therefore, every quantum state cannot be cloned without this special case.

Alternatively, let $|\varphi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle$ and $|\varphi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle$ be two quantum states. Assume that $|\varphi_1\rangle$ can be cloned and let U be an operator which clones any quantum state. We can apply U to the below state:

$$U(k|\varphi_1\rangle \otimes |\varphi_2\rangle) = k(U|\varphi_1\rangle \otimes |\varphi_2\rangle) = k(|\varphi_1\rangle \otimes |\varphi_2\rangle).$$

Suppose that $k|\varphi_1\rangle = |a\rangle$. Then, $U(|a\rangle \otimes |\varphi_2\rangle) = |a\rangle \otimes |a\rangle = k|\varphi_1\rangle \otimes k|\varphi_1\rangle = k^2(|\varphi_1\rangle \otimes |\varphi_1\rangle)$. Hence, $k = k^2$ and then $k = 0$ or $k = 1$. Namely, the quantum state can be copied when $k = 0$ or $k = 1$. But, every arbitrary quantum state cannot be copied.

Remark 4.3 Action of the CNOT operator is that $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$ are transformed into $|00\rangle$, $|01\rangle$, $|11\rangle$ and $|10\rangle$, respectively. We can express this action as $|a\rangle \otimes |b\rangle$ is transformed into $|a\rangle \otimes |a \oplus_2 b\rangle$ where $\oplus_2$ denotes addition modulo 2. If $b = 0$, then $|a\rangle \otimes |0\rangle = |a0\rangle$ is transformed into $|a\rangle \otimes |a \oplus_2 0\rangle = |a\rangle \otimes |a\rangle = |aa\rangle$. Therefore, a quantum state can be cloned for some special cases. However, an arbitrary quantum state cannot be cloned.

4.3 Quantum Codes

Quantum codes are defined over Hilbert spaces. A quantum code of length n is a subspace of a 2^n −dimensional Hilbert space. Hence, a quantum code of length n that encodes k qubits to n qubits is a 2^k −dimensional Hilbert space and it is denoted by $[\![n, k]\!]$. An element of this subspace is called a *codeword*.

Example 4.4 The set $\{|\varphi\rangle = \alpha|000\rangle + \beta|111\rangle \mid |\alpha|^2 + |\beta|^2 = 1\}$ is a 2^1 −dimensional subspace of 2^3 −dimensional Hilbert space. Because, the space of 3 −qubit quantum states is a 2^3 −dimensional Hilbert space. Here, 1 qubit is encoded to 3 qubits. Thus, $n = 3$ and $k = 1$. Therefore, this set is a $[\![3,1]\!]$ −quantum code. The states $|000\rangle$ and $|111\rangle$ are the codewords of the quantum code.

Theorem 4.5 [29] Let C be a code and let $E = \{\varepsilon_1, \varepsilon_2, \varepsilon_{3,} \dots\}$ be a set of errors which act on this code. Then, E is a set of correctable errors if and only if for all $a \neq b \in C$ it implies that $\varepsilon_i a \neq \varepsilon_j b$ for all i, j.

Proof. For necessary condition, suppose that $c = \varepsilon_i a = \varepsilon_j b$ for some $a \neq b$ and for some i, j. If ε_i or ε_j error occurs, then we have same codeword c. So, we cannot determine whether the error is ε_i or ε_j has occured. Therefore, original codeword cannot be obtained.

Conversely, for sufficient condition, assume that if any error occurs, then the vector c is obtained. Then, there exist only one $a \in C$ such that $c = \varepsilon_i a$. Hence, a is the original codeword. We can decode c as a.

Proposition 4.6 [29] If ε_i is invertible, then the above correctability condition is equivalent to the detectability condition.

Proof: Let C be a code, let $E = \{\varepsilon_1, \varepsilon_2, \varepsilon_3 \dots\}$ be a set of correctable errors and let ε_i and ε_j be two invertible error operators. Assume that ${\varepsilon_i}^{-1}\varepsilon_j$ is not detectable. Then, there exist $a \neq b \in C$ such that $a = {\varepsilon_i}^{-1}\varepsilon_j b$. This implies that $\varepsilon_i a = \varepsilon_j b$ since ε_i and ε_j are invertible. Therefore, we conclude that the set E is not correctable by the previous theorem.

Example 4.7 Let $C = \{000, 010, 101, 111\}$ be a code. Assume that we have 4 error operators $\varepsilon_1, \varepsilon_2, \varepsilon_3$ and ε_4, and they act as follows:

i. ε_1 transforms 000 into 100 and fixes the others.
ii. ε_2 transforms 111 into 110 and fixes the others.
iii. ε_3 transforms 010 into 011 and fixes the others.
iv. ε_4 transforms 101 into 001 and fixes the others.

Here, ε_i are invertible. Thus, the detectability and correctability for this code are the same.

The first quantum error correcting code which correct any arbitrary error on a single qubit is Shor code. The code encodes 1 qubit to 9 qubits as $|0\rangle \rightarrow |0_L\rangle$ and $|1\rangle \rightarrow |1_L\rangle$ where

$$|0_L\rangle = \frac{(|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle)}{2\sqrt{2}},$$

$$|1_L\rangle = \frac{(|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle)}{2\sqrt{2}}.$$

4.3.1 The CSS Code

In 1996, a useful quantum code is invented by Robert Calderbank, Peter Shor and Andrew Steane. This code leads to a relation between classical linear codes and quantum codes. Thus, the problem of finding a quantum code transforms into finding a classical linear code containing its dual. This type of quantum codes are known as CSS codes [9].

Definition 4.8 [9] Let C_1 be an $[n,k_1]$-linear code and let C_2 be an $[n,k_2]$-linear code such that $C_2 \subseteq C_1$. Codewords of the quantum code are defined by

$$|a + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{b \in C_2} |a \oplus_2 b\rangle$$

where $\oplus_2$ is addition modulo 2 and $a \in C_1$.

This code which is constructed by using cosets of a linear code is called an $[\![n, k_1 - k_2]\!]$ CSS code and shortly it is denoted by $CSS(C_1, C_2)$. If the minimum distances of C_1 and $C_2^{\perp}$ are d_1 and d_2, respectively, then the minimum distance of $CSS(C_1, C_2)$ is $min\{d_1, d_2\}$. If the dual of C_1 is a subset of C_1, then C_2 can be chosen as the dual of C_1. Hence, $d(C_1) = d\big((C^{\perp})^{\perp}\big) = d(C_2^{\perp}) = d$. Therefore, it needs to find a linear code of the minimum distance d which contains its dual in order to obtain an $[\![\mathrm{n}, k_1 - k_2, d]\!]$ $-$quantum code.

The parameters of $CSS(C_1, C_2)$ depend on the parameters of C_1 and C_2. If $a_1 - a_2 \in C_2$, then $|a_1 + C_2\rangle = |a_2 + C_2\rangle$ where $a_1, a_2 \in C_1$. Also, if a_1 and a_2 belong to distinct cosets of C_2, then there do not exist $b_1, b_2 \in C_2$ such that $a_1 + b_1 = a_2 + b_2$ and so $|a_1 + C_2\rangle$ and $|a_2 + C_2\rangle$ are orthonormal. The number of distinct cosets of C_2 in C_1 is $\frac{|C_1|}{|C_2|} = \frac{2^{k_1}}{2^{k_2}} = 2^{k_1 - k_2}$. It means that the dimension of $CSS(C_1, C_2)$ is $k_1 - k_2$.

Example 4.9 Let $C_1 = \{0000000, 0001011, 0010110, 0011101, 0100111, 0101100,$

$0110001, 0111010, 1000101, 1001110, 1010011, 1011000, 1100010, 11010011, 1110100,$ $1111111\}$. Then, C_1 is a [7,4,3]-linear code. The dual of C_1 can be evaluated and then $C_1^{\perp} =$ $\{0000000, 0011101, 0100111, 0111010, 1001110, 1010011, 1101001, 1110100\}$. The dual $C_1^{\perp}$is a [7,3,4]-linear code. Here, $C_1^{\perp} \subset C_1$. We can choose $C_2 = C_1^{\perp}$. Now, we can construct a quantum code $CSS(C_1, C_2)$. Since $k_1 = 4$ and $k_2 = 3$, $k_1 - k_2 = 1$ and $min\{d(C_1), d(C_2^{\perp})\} = min\{3, 3\} = 3$. Hence, $CSS(C_1, C_2)$ is a $[\![7,1,3]\!]$ −quantum code. Codewords can be written by using cosets. However, some cosets can be same. So, codewords are the different cosets:

$|0000000 + C_2\rangle = \frac{1}{\sqrt{8}}(|0000000\rangle + |0011101\rangle + |0100111\rangle + |0111010\rangle +$ $|1001110\rangle + |1010011\rangle + |1101001\rangle + |1110100\rangle)$.

$|1111111 + C_2\rangle = \frac{1}{\sqrt{8}}(|0001011\rangle + |0010110\rangle + |0101100\rangle + |0110001\rangle +$ $|1000101\rangle + |1011000\rangle + |1100010\rangle + |1111111\rangle)$.

4.3.1.1 Decoding Procedure in CSS codes

Error correcting ability of $CSS(C_1, C_2)$ bases on error correcting abilities of C_1 and $C_2^{\perp}$. If a bit flip error occurs, then the code C_1 is used. If a phase flip error occurs, then the dual of C_1 is used to correct errors in a quantum code.

Let ε be an error operator. Assume that ε_1 and ε_2 are errors corresponding to bit flip and phase flip error, respectively. Action of the error ε on a quantum state $|a\rangle$ is defined by

$$\varepsilon|a\rangle = (-1)^{\langle a,\varepsilon_2\rangle}|a + \varepsilon_1\rangle$$

where $\langle a, \varepsilon_2\rangle$ denotes the standard inner product.

Example 4.10 Let $\varepsilon = ZIXX$ and $|a\rangle = |1010\rangle$. Here, $\varepsilon_1 = 0011$ and $\varepsilon_2 = 1000$. Then, $\varepsilon|a\rangle = (ZIXX)|1010\rangle = -|1001\rangle$. Moreover, action of ε can be evaluated as:

$$\varepsilon|a\rangle = (-1)^{\langle 1010,1000\rangle}|1010 \oplus_2 0011\rangle = (-1)^1|1001\rangle = -|1001\rangle.$$

Error ε_1 is a vector corresponding to bit flip error. So, if X operator acts on some coordinates of a vector, then these coordinates of the vector are 1, otherwise 0.

Error ε_2 is a vector corresponding to phase flip error. So, if Z operator acts on some coordinates of a vector, then these coordinates of the vector are 1, otherwise 0.

Similar to the classical encoding procedure, ancillary qubits are used in the quantum coding procedure.

Action of the Hadamard gate on $|a\rangle$ is defined by

$$\frac{1}{\sqrt{2^n}}\sum_{b\in F_2^n}(-1)^{\langle a,b\rangle}|b\rangle.$$

Example 4.11 Let $|a\rangle = |1001\rangle$. If the Hadamard gate acts on each qubit, then $HHHH$ acts on $|a\rangle$. Here, $n = 4$. Then,

$$\frac{1}{\sqrt{2^4}}\sum_{b\in F_2^4}(-1)^{\langle 1001,b\rangle}|b\rangle$$

$= \frac{1}{4}((-1)^{\langle 1001,0000\rangle}|0000\rangle + (-1)^{\langle 1001,1000\rangle}|1000\rangle + (-1)^{\langle 1001,0100\rangle}|0100\rangle +$
$(-1)^{\langle 1001,0010\rangle}|0010\rangle + (-1)^{\langle 1001,0001\rangle}|0001\rangle + (-1)^{\langle 1001,1001\rangle}|1001\rangle +$
$(-1)^{\langle 1001,1010\rangle}|1010\rangle + (-1)^{\langle 1001,1011\rangle}|1011\rangle + (-1)^{\langle 1001,0101\rangle}|0101\rangle +$
$(-1)^{\langle 1001,0110\rangle}|0110\rangle + (-1)^{\langle 1001,0111\rangle}|0111\rangle + (-1)^{\langle 1001,1101\rangle}|1101\rangle +$
$(-1)^{\langle 1001,1110\rangle}|1110\rangle + (-1)^{\langle 1001,1100\rangle}|1100\rangle + (-1)^{\langle 1001,0011\rangle}|0011\rangle +$
$(-1)^{\langle 1001,1111\rangle}|1111\rangle).$

$= \frac{1}{4}(|0000\rangle - |1000\rangle + |0100\rangle + |0010\rangle - |0001\rangle + |1001\rangle - |1010\rangle + |1011\rangle -$
$|0101\rangle + |0110\rangle - |0111\rangle + |1101\rangle - |1110\rangle - |1100\rangle - |0011\rangle + |1111\rangle).$

Next, we will give error correction procedure in the CSS code.

In order to detect and correct quantum errors, we can use the classical error correcting properties of C_1 and ${C_2}^{\perp}$. An n bit vector ε_1 describes bit flip errors such that there are 1s where bit flips occurred and there are 0s elsewhere. An n bit vector ε_2 describes phase flip errors such that there are 1s where phase flips occurred and there are 0s elsewhere. Let $|a + C_2\rangle$ be the initial state. If some errors occurred, then the corrupted state is:

$$\frac{1}{\sqrt{|C_2|}}\sum_{b\in C_2}(-1)^{(a+b)\varepsilon_2}|a + b + \varepsilon_1\rangle.$$

To detect the location of bit flips, we introduce ancilla qubits. The state $|a + b + \varepsilon_1\rangle|0\rangle$ to $|a + b + \varepsilon_1\rangle|H_1(a + b + \varepsilon_1)\rangle = |a + b + \varepsilon_1\rangle|H_1\varepsilon_1\rangle$ where H_1 is parity-check matrix of C_1 since $(a + b) \in C_1$ is annihilated by matrix H_1 . Then, we obtain

$$\frac{1}{\sqrt{|C_2|}}\sum_{b\in C_2}(-1)^{(a+b)\varepsilon_2}|a+b+\varepsilon_1\rangle\,|H_1\varepsilon_1\rangle.$$

The detection procedure is completed by measuring ancilla qubits, then

$$\frac{1}{\sqrt{|C_2|}}\sum_{b\in C_2}(-1)^{(a+b)\varepsilon_2}|a+b+\varepsilon_1\rangle.$$

Since C_1 can correct up to t errors, if we know the error syndrome $H_1\varepsilon_1$, we can conclude the error ε_1. So, error correction abilities of linear codes C_1 and C_2 are related to the quantum code which are obtained by these linear codes.

4.3.2 Stabilizer Codes

Stabilizer codes are invented by Daniel Gottesman in 1997 [14]. While the set of Pauli matrices I, X, Y, Z is not a group, the set can be extended to a group as $\{\mp I, \mp iI, \mp X, \mp iX, \mp Y, \mp iY, \mp Z, \mp iZ\}$. Each element of this group acts on a single qubit. However, a group which acts on more than one qubit can be constructed by using tensor product. More formally, while $P = \{\mp I, \mp iI, \mp X, \mp iX, \mp Y, \mp iY, \mp Z, \mp iZ\}$ acts on a single qubit, $P_n = P \otimes P \otimes \ldots P$ acts on n qubits. Group theory is used in encoding and decoding procedure of stabilizer codes. A map θ from $P_n \times H^n$ to H^n is defined by

$$\theta: P_n \times H^n \to H^n$$

$$(S, |\varphi\rangle) \to S|\varphi\rangle$$

Stabilizers of a quantum state of length n are the elements of P_n which fix the quantum state.

Example 4.12 Let $|\varphi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. The operators which fix this quantum state are I and X. Because,

$$I|\varphi\rangle = I\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) = \frac{1}{\sqrt{2}}(I|0\rangle + I|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$X|\varphi\rangle = X\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) = \frac{1}{\sqrt{2}}(X|0\rangle + X|1\rangle) = \frac{1}{\sqrt{2}}(|1\rangle + |0\rangle).$$

$\mathcal{S} = \{I, X\}$ is an Abelian subgroup of P which is generated by X. The vector $|\varphi\rangle$ is a quantum state which is fixed by $\mathcal{S}$.

Example 4.13 Let $|\varphi\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |01\rangle)$. The operators $II, ZI, -ZX$ and $-IX$ fix this quantum state. Because,

$$II|\varphi\rangle = II\left(\frac{1}{\sqrt{2}}(|00\rangle - |01\rangle)\right) = \frac{1}{\sqrt{2}}(II|00\rangle - II|01\rangle) = \frac{1}{\sqrt{2}}(|00\rangle - |01\rangle),$$

$$ZI|\varphi\rangle = ZI\left(\frac{1}{\sqrt{2}}(|00\rangle - |01\rangle)\right) = \frac{1}{\sqrt{2}}(ZI|00\rangle - ZI|01\rangle) = \frac{1}{\sqrt{2}}(|00\rangle - |01\rangle),$$

$$-ZX|\varphi\rangle = -ZX\left(\frac{1}{\sqrt{2}}(|00\rangle - |01\rangle)\right) = \frac{1}{\sqrt{2}}(-ZX|00\rangle + ZX|01\rangle)$$
$$= \frac{1}{\sqrt{2}}(-|01\rangle + |00\rangle),$$

$$-IX|\varphi\rangle = -IX\left(\frac{1}{\sqrt{2}}(|00\rangle - |01\rangle)\right) = \frac{1}{\sqrt{2}}(-IX|00\rangle + IX|01\rangle) = \frac{1}{\sqrt{2}}(-|01\rangle + |00\rangle).$$

$\mathcal{S} = \{II, ZI, -ZX, -IX\}$ is an abelian subgroup of P_2. The vector $|\varphi\rangle$ is a quantum state which is fixed by $\mathcal{S}$.

Let $\mathcal{S}$ be a subgroup of P_n and $V_{\mathcal{S}}$ be a subspace of quantum states of length n which is fixed by $\mathcal{S}$. The set $\mathcal{S}$ is called the stabilizer of $V_{\mathcal{S}}$.

Note that $V_{\mathcal{S}}$ is the intersection of spaces of quantum states which is fixed by each element of $\mathcal{S}$.

Example 4.14 Let $\mathcal{S} = \{III, ZZI, ZIZ, IZZ\}$. This set is a subgroup of P_3.

- III fixes all elements of H^3.
- ZZI fixes the set of $|000\rangle$, $|110\rangle$, $|001\rangle$ and $|111\rangle$.
- ZIZ fixes the set of $|000\rangle$, $|101\rangle$, $|010\rangle$ and $|111\rangle$.
- IZZ fixes the set of $|000\rangle$, $|011\rangle$, $|100\rangle$ and $|111\rangle$.

Then, the space that is fixed by $\mathcal{S}$ is the intersection of the above sets. Hence, $\mathcal{S}$ fixes $|000\rangle$ and $|111\rangle$. The space $V_{\mathcal{S}} = \{\alpha|000\rangle + \beta|111\rangle | \alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1\}$ is fixed by $\mathcal{S}$. This group is generated by ZZI and IZZ. Because, $(ZZI)(IZZ) = ZIZ$.

We can study the properties of a group by generators of the group. The generators of $\mathcal{S}$ in Example 4.14 are ZZI and IZZ. Hence, the intersection of the set of quantum states which is fixed only by the generators is enough to construct a stabilizer code.

Proposition 4.15 [14] Let $\mathcal{S}$ be a subgroup of P_n and $V_{\mathcal{S}}$ be a space of quantum states which is fixed by $\mathcal{S}$. We need the following two conditions to have $V_{\mathcal{S}} \neq \emptyset$:

1) $-I$ is not an element of $\mathcal{S}$.
2) $\mathcal{S}$ is an abelian group.

Proof.

1) Assume that $-I$ is an element of $\mathcal{S}$. Let $|\varphi\rangle \in V_{\mathcal{S}}$. Then,

$$-I|\varphi\rangle = -(I|\varphi\rangle) = -(|\varphi\rangle) = -|\varphi\rangle.$$

Moreover, $|\varphi\rangle$ is fixed by $-I$ since $-I$ is an element of $\mathcal{S}$. Hence,

$$-I|\varphi\rangle. = |\varphi\rangle.$$

By the above equations, $|\varphi\rangle$ must be zero. This means that $V_{\mathcal{S}} = \emptyset$.

2) Let S_1 and S_2 be two elements of $\mathcal{S}$. Assume that $\mathcal{S}$ is a nonabelian group. Then, S_1 and S_2 anti-commute. That is, $S_1S_2 = -S_2S_1$. Let $|\varphi\rangle$ be an element of $V_{\mathcal{S}}$. The operator S_1S_2 is also element of $\mathcal{S}$ since $\mathcal{S}$ is a group. Then,

$$S_1S_2|\varphi\rangle = -S_2S_1|\varphi\rangle = -S_2(S_1|\varphi\rangle) = -S_2(|\varphi\rangle) = -(S_2|\varphi\rangle) = -|\varphi\rangle\,.$$

However, $|\varphi\rangle$ must be fixed by S_1S_2 since S_1S_2 is an element of $\mathcal{S}$. It is possible only when $|\varphi\rangle = 0$. Hence, $V_{\mathcal{S}} = \emptyset$.

Lemma 4.16 [14] Let $\mathcal{S}$ be a subgroup of P_n and S_1 and S_2 be two elements of $\mathcal{S}$. The elements S_1 and S_2 commute if and only if the number of different positions without identity operator between S_1 and S_2 is even.

Proof. Let $S_1 = A_1A_2 \dots A_n$ and $S_2 = B_1B_2 \dots B_n$. Assume that the number of different positions between S_1 and S_2 is even. Then,

S_1S_2=$(A_1A_2 \dots A_n)(B_1B_2 \dots B_n)$= $(A_1B_1) \otimes (A_2B_2) \otimes \dots \otimes (A_nB_n)$

If one of A_i and B_i is identity or they are same, then they commute. Otherwise, they anti-commute; that is $S_1S_2 = -S_2S_1$, since elements of $\mathcal{S}$ either commute or anti-commute. Finally, we have a product of even number of (-1)s. We conclude $S_1S_2 =$

$(-1) \dots (-1)$=$(B_1A_1) \otimes (B_2A_2) \otimes \dots \otimes (B_nA_n)$= $(B_1B_2 \dots B_n)(A_1A_2 \dots A_n)$= S_2S_1. Namely, S_1 and S_2 commute.

Similarly, converse is clear.

Example 4.17 Let $S_1 = XXZYIX$ and $S_2 = YXXYZI$. Then,

$$S_1S_2 = (X \otimes X \otimes Z \otimes Y \otimes I \otimes X)(Y \otimes X \otimes X \otimes Y \otimes Z \otimes I)$$

$$= (XY) \otimes (XX) \otimes (ZX) \otimes (YY) \otimes (IZ) \otimes (XI)$$

$$= -(YX) \otimes (XX) \otimes -(XZ) \otimes (YY) \otimes (ZI) \otimes (IX)$$

$$= (-)(-)(Y \otimes X \otimes X \otimes Y \otimes Z \otimes I)(X \otimes X \otimes Z \otimes Y \otimes I \otimes X)$$

$$= (YXXYZI)(XXZYIX) = S_2S_1.$$

In fact, the number of different positions in S_1 and S_2 is two. So, S_1 and S_2 commute by Lemma 4.17

Remark 4.18 Let $\mathcal{S}$ be a subgroup of P_n. Each element S of $\mathcal{S}$ has eigenvalues $+1$ or -1 since $S^2 = I$.

Definition 4.19 Let r be a map from P_n to Z_2^{2n}. An element of P_n is transformed into a vector by using the map. This map is defined as

$$r: P_n \rightarrow Z_2^{2n}$$
$$p \rightarrow v$$

i. If $P \in P_n$ acts on the ith qubit as X, then the ith entry of the vector v is 1.

ii. If $P \in P_n$ acts on the ith qubit as Z, then the $(n+i)$th entry of the vector v is 1.

iii. If $P \in P_n$ acts on the ith qubit as Y, then both the ith and the $(n+i)$th entries of the vector v is 1.

iv. If $P \in P_n$ acts on the ith qubit as I, then the ith entry of the vector v is 0.

Example 4.20 Let $P = XIZYI \in P_5$ for $n = 5$. Then,

$$r(XIZYI) = (1\ 0\ 0\ 1\ 0|0\ 0\ 1\ 1\ 0).$$

The map r is a homomorphism and Ker(r)=$\langle iI \rangle$. The map r leads to a relation between subspaces of Z_2^{2n} and stabilizer groups. The map r can be used to check the commutative property of two elements of P_n.

We know that two elements P_1 and P_2 of Pauli group commute if and only if they have an even number of positions which is different from each other. This condition is equivalent to the following expression:

The elements P_1 and P_2 commute if and only if $r(P_1)A\,r(P_2)^{Tr} \equiv 0 \; mod\; 2$ where A=$\begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}$.

Example 4.21 Let $P_1 = XIY$ and $P_2 = ZIX$ be elements of P_3. Then,

$r(P_1) = (1\;0\;1|0\;0\;1)$, $r(P_2) = (0\;0\;1|1\;0\;0)$ and $A = \begin{pmatrix} 0&0&0&1&0&0\\0&0&0&0&1&0\\0&0&0&0&0&1\\1&0&0&0&0&0\\0&1&0&0&0&0\\0&0&1&0&0&0 \end{pmatrix}$. Also,

$$r(P_1)A\,r(P_2)^{Tr} = (1\;0\;1\;0\;0\;1)\begin{pmatrix} 0&0&0&1&0&0\\0&0&0&0&1&0\\0&0&0&0&0&1\\1&0&0&0&0&0\\0&1&0&0&0&0\\0&0&1&0&0&0 \end{pmatrix}\begin{pmatrix}0\\0\\1\\1\\0\\0\end{pmatrix}$$

$$= (0\;0\;1\;1\;0\;1)\begin{pmatrix}0\\0\\1\\1\\0\\0\end{pmatrix} = 1 + 1 = 2 \equiv 0 \; mod\; 2.$$

Then, P_1 and P_2 commute.

The generators of stabilizer group $\mathcal{S}$ can be described by a check matrix. A check matrix of a stabilizer group is defined as each row of the matrix corresponds to the images of a generator of $\mathcal{S}$ under the map r.

Definition 4.22 Suppose $\mathcal{S}$ is generated by $S_1, S_2, \dots , S_n$. The check matrix of $\mathcal{S}$ is denoted by $H(\mathcal{S})$ and it is defined as:

$$H(\mathcal{S})_i \rightarrow r(S_i)$$

for all i, $i \in \{1,2,\dots,r\}$ where $H(\mathcal{S}) \in Z_2^{r\times 2n}$. Here, $H(\mathcal{S})_i$ denotes the ith row of $H(\mathcal{S})$.

Example 4.23 $\mathcal{S}= \{III, ZZI, ZIZ, IZZ\}$. The generators of $\mathcal{S}$ are ZZI and IZZ. Then,

$$H(\mathcal{S})_1 \rightarrow r(S_1) = (0\;0\;0\;1\;1\;0),$$

$$H(\mathcal{S})_2 \rightarrow r(S_2) = (0\;0\;0\;0\;1\;1).$$

Thus, $H(\mathcal{S})$=$\begin{pmatrix} H(\mathcal{S})_1 \\ H(\mathcal{S})_2 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$ is the check or control matrix of $\mathcal{S}$.

Example 4.24 Let $s_1 = X_4X_5X_6X_7$, $s_2 = X_2X_3X_6X_7$, $s_3 = X_1X_3X_5X_7$, $s_4 = Z_4Z_5Z_6Z_7$, $s_5 = Z_2Z_3Z_6Z_7$ and $s_6 = Z_4Z_5Z_6Z_7$ be generators of a stabilizer group. It is enough to check the commutativity of generators instead of the full group. So,

$$H(\mathcal{S}) = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix},$$

$$H(\mathcal{S})AH(\mathcal{S})^{Tr} \equiv 0 \; mod \; 2$$

where $A = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$.

Hence, these six generators commute and then the stabilizer group is also commutative. Furthermore, $-I$ is not an element of the stabilizer group. Thus, from Proposition 4.16 a quantum code can be constructed by using this stabilizer group. This code is known as $7-$qubit Steane code with parameters $[\![7,1]\!]$. Here, $k = 1$ and $n = 7$. The number of generators is 6. This shows that $7 - 6 = 1$. It can be generalized as Definition 4.25:

Definition 4.25 Let $s_1, s_2, \ldots, s_r$ be commutative and independent generators of a stabilizer group $\mathcal{S}$. Namely, $\mathcal{S} = \langle s_1, s_2, \ldots, s_r \rangle$ and $-I \notin \mathcal{S}$. The code space $V_{\mathcal{S}}$ which is fixed by $\mathcal{S}$ is called $[\![n, n-r]\!]$ $-$*stabilizer code* and it is denoted by $C(\mathcal{S})$.

Example 4.26 The generators $s_1 = Z_1Z_2$, $s_2 = Z_2Z_3$, $s_3 = Z_4Z_5$, $s_4 = Z_5Z_6$, $s_5 = Z_7Z_8$, $s_6 = Z_8Z_9$, $s_7 = X_1X_2X_3X_4X_5X_6$ and $s_8 = X_4X_5X_6X_7X_8X_9$ generate $[\![9,1]\!]$ $-$Shor code. Here, $n = 9$ and $r = 8$. Hence, $k = 1$.

4.3.2.1 Decoding Procedure in Stabilizer Codes

Let $C(\mathcal{S})$ be a stabilizer code which is fixed by $\mathcal{S}$. For all $|\varphi\rangle \in C(\mathcal{S})$ and for all $s \in \mathcal{S}$, $s|\varphi\rangle = |\varphi\rangle$. This means that a codeword of $C(\mathcal{S})$ is an eigenvector of each element of $\mathcal{S}$ corresponding to the eigenvalue 1.

Let e be an element which does not commute with $\mathcal{S}$. Then, for $s \in \mathcal{S}$, $se = -es$ since elements of P_n commute or anti-commute. Then,

$$s(e|\varphi\rangle) = (se)|\varphi\rangle = (-es)|\varphi\rangle = -e(s|\varphi\rangle) = -e(|\varphi\rangle) = -e|\varphi\rangle.$$

That is, $e|\varphi\rangle$ is an eigenvector of s which has eigenvalue -1. A vector with $+1$ eigenvalue is transformed into a vector with -1 eigenvalue. Errors can be detected by using this transformation.

Example 4.27 Let $C(\mathcal{S}) = \{\alpha|000\rangle + \beta|111\rangle | \alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1\}$. Then, $\mathcal{S} = \{III, Z_1Z_2, Z_2Z_3, Z_1Z_3\}$. It is a 3-qubit flip code. Suppose that error operator X acts on the first qubit. Namely, XII is an error operator. Then, $XII(\alpha|000\rangle + \beta|111\rangle) = \alpha|100\rangle + \beta|011\rangle$. Now, action of each element of $\mathcal{S}$ on the state with error is evaluated:

$$Z_1Z_2(\alpha|000\rangle + \beta|111\rangle) = -(\alpha|000\rangle + \beta|111\rangle),$$

$$Z_2Z_3(\alpha|000\rangle + \beta|111\rangle) = +(\alpha|000\rangle + \beta|111\rangle),$$

$$Z_1Z_3(\alpha|000\rangle + \beta|111\rangle) = -(\alpha|000\rangle + \beta|111\rangle).$$

The operators Z_1Z_2 and Z_2Z_3 change eigenvalues to -1. If Z_2 leads to this change, then Z_2Z_3 also change eigenvalues to -1. If Z_3 leads to a change, then Z_2Z_3 also change eigenvalues to -1. Hence, Z_1 leads to this change of eigenvalue. This means that an error occurs in the first qubit. This error can be corrected by applying operator X to the first qubit. Namely, X_1 is applied on quantum state with error.

So, $X_1(\ \alpha|100\rangle + \beta|011\rangle) = \alpha|000\rangle + \beta|111\rangle$. It is initial quantum state. That is, error is corrected.

Error detection can be also made by using a syndrome table:

Table 4. 1 Syndrome table of Example 4.26

	Z_1Z_2	Z_2Z_3	Z_1Z_3
Error $X_1 = XII$	$-$	$+$	$-$
Error $X_2 = IXI$	$-$	$-$	$+$
Error $X_3 = IIX$	$+$	$-$	$-$

After the syndrome table is constructed, each element of the stabilizer group is applied to the quantum state with an error and then eigenvalues determine the error by using the syndrome table.

Table 4. 2 Syndrome table of Steane code

	$XXXXIII$	$XXIIXXI$	$XIXIXIX$	$ZZZZIII$	$ZZIIZZI$	$ZIZIZIZ$
$IIIIIII$	+	+	+	+	+	+
$XIIIIII$	+	+	+	−	−	−
$IXIIIII$	+	+	+	−	−	+
$IIXIIII$	+	+	+	−	+	−
$IIIXIII$	+	+	+	−	+	+
$IIIIXII$	+	+	+	+	−	−
$IIIIIXI$	+	+	+	+	−	+
$IIIIIIX$	+	+	+	+	+	−
$ZIIIIII$	−	−	−	+	+	+
$IZIIIII$	−	−	−	+	+	+
$IIZIIII$	−	+	−	+	+	+
$IIIZIII$	−	+	+	+	+	+
$IIIIZII$	+	−	−	+	+	+
$IIIIIZI$	+	−	+	+	+	+
$IIIIIIZ$	+	+	−	+	+	+
$YIIIIII$	−	−	−	−	−	−
$IYIIIII$	−	−	−	−	−	+
$IIYIIII$	−	+	−	−	+	−
$IIIYIII$	−	+	+	−	+	+
$IIIIYII$	+	−	−	+	−	−
$IIIIIYI$	+	−	+	+	−	+
$IIIIIIY$	+	+	−	+	+	−

Table 4.2 shows the transformation of eigenvalues when errors of weight 1 occur.

Example 4.28 Let $\mathcal{S}= \langle XXXXIII, XXIIXXI, XIXIXIX, ZZZZIII, ZZIIZZI, ZIZIZIZ\rangle$. The code which is fixed by $\mathcal{S}$ is known as Steane code and the codeword of the code space $C(\mathcal{S}\ )$ as:

$$\frac{\alpha}{\sqrt{8}}(|0000000\rangle + |1111000\rangle + |1100110\rangle + |1010101\rangle|0011110\rangle + |0101101\rangle + |0110011\rangle + |1001011\rangle) + \frac{\beta}{\sqrt{8}}(|0000111\rangle + |1111111\rangle + |1100001\rangle + |1010010\rangle + |0011001\rangle + |0101010\rangle + |0110100\rangle + |1001100\rangle).$$

Assume that an error occurs on the codeword and we have a quantum state as:

$$\frac{\alpha}{\sqrt{8}}(|0010000\rangle + |1101000\rangle + |1110110\rangle + |1000101\rangle + |0001110\rangle + |0111101\rangle + |0100011\rangle + |1011011\rangle) + \frac{\beta}{\sqrt{8}}(|0010111\rangle + |1101111\rangle + |1110001\rangle + |1000010\rangle + |0001001\rangle + |0111010\rangle + |0100100\rangle + |1011100\rangle).$$

When we observe an action of stabilizers on the codeword with error, we obtain eigenvalues $+1, +1, +1, -1, +1$ and -1, respectively. These eigenvalues correspond to error $IIXIIII$ by using Syndrome Table 5.2. If we again apply $IIXIIII$ to the codeword with error, we obtain the original codeword. So,

$$IIXIIII(\frac{\alpha}{\sqrt{8}}(|0010000\rangle + |1101000\rangle + |1110110\rangle + |1000101\rangle + |0001110\rangle + |0111101\rangle + |0100011\rangle + |1011011\rangle) + \frac{\beta}{\sqrt{8}}(|0010111\rangle + |1101111\rangle + |1110001\rangle + |1000010\rangle + |0001001\rangle + |0111010\rangle + |0100100\rangle + |1011100\rangle)).$$

$$= \frac{\alpha}{\sqrt{8}}(|0000000\rangle + |1111000\rangle + |1100110\rangle + |1010101\rangle|0011110\rangle + |0101101\rangle + |0110011\rangle + |1001011\rangle) + \frac{\beta}{\sqrt{8}}(|0000111\rangle + |1111111\rangle + |1100001\rangle + |1010010\rangle + |0011001\rangle + |0101010\rangle + |0110100\rangle + |1001100\rangle).$$

Steane code corrects all errors of weight 1. However, some of errors of weight 2 cannot be corrected by this code.

Errors are divided into three classes in stabilizer codes:

1) The errors which belong to $\mathcal{S}$.
2) The errors which do not commute with $\mathcal{S}$.

3) The errors which commute with $\mathcal{S}$ but they do not belong to $\mathcal{S}$.

Code space $C(\mathcal{S})$ cannot detect the errors in case 3.

- The centralizer of $\mathcal{S}$ in P_n is defined by $Z(\mathcal{S}) = \{P \in P_n | PS = SP, \text{ for all } S \in \mathcal{S}\}$.
- The normalizer of $\mathcal{S}$ in P_n is defined by $N(\mathcal{S}) = \{P \in P_n | P\mathcal{S} = \mathcal{S}P, \text{ for all } S \in \mathcal{S}\}$.

We have already known that $\mathcal{S} \subseteq Z(\mathcal{S}) \subseteq N(\mathcal{S})$.

For any $P \in P_n$ and $S \in \mathcal{S}$,

$$P^{+}SP = \pm P^{+}PS = \pm IS = \pm S.$$

If $-S \in \mathcal{S}$, then $-SS = -I \in \mathcal{S}$. So, this contradicts with $-I \notin \mathcal{S}$. Then, $PP^{+}SP = PS$ implies $SP = PS$. Therefore, $P \in Z(\mathcal{S})$. So, $N(\mathcal{S}) \subseteq Z(\mathcal{S})$. Therefore $Z(\mathcal{S}) = N(\mathcal{S})$ in a stabilizer group $\mathcal{S}$.

The error which commute with $\mathcal{S}$ but do not belong to $\mathcal{S}$ is the elements of $N(\mathcal{S}) - \mathcal{S}$. Hence, the errors in $N(\mathcal{S}) - \mathcal{S}$ cannot be detected.

Example 4.29 Let$\mathcal{S} = \{III, Z_1Z_2, Z_2Z_3, Z_1Z_3\}$ and $C(\mathcal{S}) = \{\alpha|000\rangle + \beta|111\rangle | \alpha, \beta \in \mathbb{C} \text{ and } |\alpha|^2 + |\beta|^2 = 1\}$. Suppose that the error operator is $X_1X_2X_3$.

i. $X_1X_2X_3$ commutes with Z_1Z_2.
ii. $X_1X_2X_3$ commutes with Z_2Z_3.
iii. $X_1X_2X_3$ commutes with Z_1Z_3.

Hence, $X_1X_2X_3$ commutes with $\mathcal{S}$ and it does not belong to $\mathcal{S}$. Thus, $X_1X_2X_3 \in N(\mathcal{S}) - \mathcal{S}$. So, it cannot be detected.

Actually, the action of $X_1X_2X_3$ is as follows:

$$X_1X_2X_3(\alpha|000\rangle + \beta|111\rangle) = \alpha|111\rangle + \beta|000\rangle$$

The error operator does not lead to a change of the eigenvalue.

Definition 4.30 Let A be an operator which belongs to P_n. The number of nonidentity positions is called the *weight of* A and it is denoted by $w(A)$. More formally,

$$w(A) = \{i | A_i \neq I, 1 \leq i \leq n\}$$

where $A = A_1A_2 \dots A_n$.

Example 4.31 For A=$XIZIXX$, $w(A) = 4$. Also, $w(IIZI) = 1$

Definition 4.32 The minimum weight of the errors in P_n which is in $N(\mathcal{S}) - \mathcal{S}$ is called the *minimum distance* of stabilizer code $C(\mathcal{S})$ and it is denoted by d. More formally,

$$d = \{w(P) | P \in N(\mathcal{S}) - \mathcal{S}, P \in P_n\}.$$

Example 4.33 Let $\mathcal{S} = \{III, Z_1Z_2, Z_2Z_3, Z_1Z_3\}$ then $C(\mathcal{S}) = \{\alpha|000\rangle + \beta|111\rangle | \alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1\}$. Here, $n = 3$. The group $\mathcal{S}$ can be generated by Z_1Z_2 and Z_2Z_3. So, there are two generators. Then, $r = 2$ .Therefore, $k = n - r = 3 - 2 = 1$. The operator Z_3 commutes $\mathcal{S}$ and it does not belong to $\mathcal{S}$. So, $Z_3 \in N(\mathcal{S}) - \mathcal{S}$. The operator Z_3 is equivalent to IIZ. The weight of IIZ is 1. Hence, the minimum weight of the elements in $N(\mathcal{S}) - \mathcal{S}$ is 1. Then, $d = 1$. Thus, $C(\mathcal{S})$ is a $[\![3,1,1]\!]$ −stabilizer code.

Definition 4.34 Let $\mathcal{S}$ be a commutative group. Assume that $\mathcal{S}$ is generated by r independent elements and $-I$ does not belong to $\mathcal{S}$. Suppose that the minimum weight of the operators in $N(\mathcal{S}) - \mathcal{S}$ is d. Then, $C(\mathcal{S})$ is called an $[\![n, n-r, d]\!]$ *−stabilizer code.*

Example 4.35 Let $\mathcal{S} = \langle XZZXI, IXZZX, XIXZZ, ZXIXZ\rangle$. The codewords of $C(\mathcal{S})$ which is constructed by stabilizer group $\mathcal{S}$ are defined as:

$$\begin{aligned} |\hat{0}\rangle = {} & |00000\rangle + |10010\rangle + |01001\rangle + |10100\rangle + |01010\rangle - |11011\rangle - |00110\rangle \\ & - |11000\rangle - |11101\rangle - |00011\rangle - |11110\rangle - |01111\rangle - |10001\rangle \\ & - |01100\rangle - |10111\rangle + |00101\rangle, \end{aligned}$$

$$\begin{aligned} |\hat{1}\rangle = {} & |11111\rangle + |01101\rangle + |10110\rangle + |01011\rangle + |10101\rangle - |00100\rangle - |11001\rangle \\ & - |00111\rangle - |00010\rangle - |11100\rangle - |00001\rangle - |10000\rangle - |01110\rangle \\ & - |10011\rangle - |01000\rangle + |11010\rangle. \end{aligned}$$

Here, the number of generators is 4 and the stabilizer group $\mathcal{S}$ is a subgroup of P_5. Hence, $n = 5$ and $n - r = 1$. Moreover, though there is no element of $N(\mathcal{S}) - \mathcal{S}$ such that its weight is smaller than 3, $YZYII$ is an element of $N(\mathcal{S}) - \mathcal{S}$. So, $d = 3$. Therefore, this code is a $[\![5,1,3]\!]$ −code.

Example 4.36 Let $\mathcal{S}$ be a stabilizer group which is generated by the below generators:

$$\begin{array}{lccccccccc}
s_1 = & Z & Z & I & I & I & I & I & I & I \\
s_2 = & Z & I & Z & I & I & I & I & I & I \\
s_3 = & I & I & I & Z & Z & I & I & I & I \\
s_4 = & I & I & I & Z & I & Z & I & I & I \\
s_5 = & I & I & I & I & I & I & Z & Z & I \\
s_6 = & I & I & I & I & I & I & Z & I & Z \\
s_7 = & X & X & X & X & X & X & I & I & I \\
s_8 = & X & X & X & I & I & I & X & X & X
\end{array}$$

Since $n = 9$ and $r = 8, n - r = 1$. We cannot find an element of $N(\mathcal{S}) - \mathcal{S}$ with weight 1 or 2. However, $XXXIIIIII \in N(\mathcal{S}) - \mathcal{S}$. So, $d = 3$. Therefore, $C(\mathcal{S})$ is a $[\![9,1,3]\!]$ −code and it is known as Shor code.

4.3.3 Entanglement Assisted Quantum Error Correcting Codes (EAQECC)

There are some methods used to construct quantum codes from classical codes. For instance, we can obtain quantum codes from two linear codes by using cosets. This is called a CSS code. However, the linear codes need to have some additional properties for this method.

By another method, the stabilizer codes are obtained. A stabilizer code is generated by using a stabilizer group. A code fixed by a stabilizer group are called a stabilizer code. But this stabilizer group must be commutative to generate a stabilizer code.

If we do not have a linear code which contains its dual or if the stabilizer group is not commutative, then we can obtain any quantum error correcting code by using another method [18].

Let $\mathcal{S}$ be a group of noncommutative operators which is generated by four operators:

$$\begin{array}{lcccc} s_1 = & Z & X & Z & I \\ s_2 = & Z & Z & I & Z \\ s_3 = & X & Y & X & I \\ s_4 = & X & X & I & X \end{array}$$

i. s_1 does not commute with s_2, s_3 and s_4.

ii. s_2 commutes with s_3 but not s_4.

iii. s_3 and s_4 do not commute.

We can find a different generator set for $\mathcal{S}$. So, $\mathcal{S}$ is transformed into a simpler form $\mathcal{B}$. Error correction conditions can be discussed by using $\mathcal{B}$.

Generator set of $\mathcal{S}$ can be separated to two different subgroup:

i. $\mathcal{S}_I$ is the group of commutative generators in $\mathcal{S}$ and it is called *isotropic* subgroup .

ii. $\mathcal{S}_S$ is the group of noncommutative genarators in $\mathcal{S}$ and it is called *symplectic* subgroup.

Some lemmas are necessary to discuss error correction conditions:

Lemma 4.37 [18] Given arbitrary V, a subgroup in P_n if V has 2^m distinct elements, then there are m independent generators for V:

$\{\bar{Z}_1, \bar{Z}_2, \dots, \bar{Z}_l, \bar{X}_1, \bar{X}_2, \dots, \bar{X}_{m-l}\}$ where $[\bar{Z}_i, \bar{Z}_j] = 0, [\bar{X}_i, \bar{X}_j] = 0\ \forall i, j$; $[\bar{Z}_i, \bar{X}_j] = 0\ \forall i \neq j, \{\bar{Z}_i, \bar{X}_i\} = 0\ \forall i$. Let $V_I = \langle \bar{Z}_{m-l+1}, \bar{Z}_{m-l+2}, \dots, \bar{Z}_l \rangle$ be isotropic group and $V_S = \langle \bar{Z}_1, \bar{Z}_2, \dots, \bar{Z}_{m-l}, \bar{X}_1, \bar{X}_2, \dots, \bar{X}_{m-l} \rangle$ be symplectic group. The group $V = \langle V_I, V_S \rangle$ is a subgroup which is generated by V_I and V_S.

Consider that 4 independent generators for $\mathcal{S}$:

$$\begin{array}{rcccc}
\bar{Z}_1 = & Z & X & Z & I \\
\bar{X}_1 = & Z & Z & I & Z \\
\bar{Z}_2 = & Y & X & X & Z \\
\bar{Z}_3 = & Z & Y & Y & X
\end{array}$$

$S_I = \langle \bar{Z}_2, \bar{Z}_3 \rangle$, $S_I = \langle \bar{Z}_1, \bar{X}_1 \rangle$ and $\mathcal{S} = \langle S_I, S_S \rangle$.

Let $\mathcal{B}$ be a group which is generated by following generators:

$$\begin{array}{rcccc}
Z_1 = & Z & I & I & I \\
X_1 = & X & I & I & I \\
Z_2 = & I & Z & I & I \\
Z_3 = & I & I & Z & I
\end{array}$$

$\mathcal{B}_I = \langle Z_2, Z_3 \rangle$, $S_I = \langle Z_1, X_1 \rangle$ and $\mathcal{B} = \langle \mathcal{B}_I, \mathcal{B}_S \rangle$.

So, $\mathcal{B}$ is isomorphic to $\mathcal{S}$; that is, $\mathcal{B} \cong \mathcal{S}$. We can be related $\mathcal{S}$ with simpler form $\mathcal{B}$.

Lemma 4.38 If $\mathcal{B} \cong \mathcal{S}$, then there exists a unitary operator U such that B= USU^{-1}

$B \in \mathcal{B}$ and $S \in \mathcal{S}$.

According to Lemma 4.38, powers of error correction of $C(\mathcal{B})$ and $C(\mathcal{S})$ are related to unitary transformations.

Next, we will analyze the code space X of C(B).

Since $\mathcal{B}$ is not a commutative group, we cannot make up $C(\mathcal{B})$. But by extending generators, we can construct a new group that is commutative. Qubits of codewords will be embedded to a larger space.

$$\begin{array}{rccccc}
Z'_1 = & Z & I & I & I & Z \\
X'_1 = & X & I & I & I & X \\
Z'_2 = & I & Z & I & I & I \\
Z'_3 = & I & I & Z & I & I
\end{array}$$

Let $|\varphi\rangle^{AB}$ be entangled state shared between Alice and Bob.

Consider that Alice has 4 original qubit and Bob has 1 extra qubit.

$\mathcal{B}_e = \{Z'_1, X'_1, Z'_2, Z'_3\}$ and $C(\mathcal{B}) = \{|\varphi\rangle^{AB}|0\rangle|0\rangle|\varphi\rangle\}$. The vector $|\varphi\rangle$ is arbitrary single qubit. Since entanglement is used, this is called Entanglement Assisted Quantum Error Correction Code (EAQECC).

$[\![n, k; c]\!]$ is parameter of EAQECC. The number of logical qubit is k, physical qubit is n and ebit is c. It may be used as $[\![n, k, d; c]\!]$.

- Number of c ebits equal to number of noncommutative generator pairs in $\mathcal{B}_S$.
- Number of ancilla qubits s equal to number of independent generators in $\mathcal{B}_I$.

Relation between these numbers is that $k = n - c - s$. If any error E anti-commutes with group $\mathcal{B}$, then E can be corrected. We can back error correction properties of original set $\mathcal{S}$ with analysis of $\mathcal{B}$. Just as we made for $\mathcal{B}$, if entangled state can be used, then it can be constructed QECC from noncommutative group $\mathcal{S}$. By adding X and Z extra operators, $\mathcal{S}$ can be transformed into commutative group. Extra qubit belongs to receiver Bob and it is error free.

$$\begin{array}{rccccc} Z'_1 = & Z & X & Z & I & Z \\ X'_1 = & Z & Z & I & X & X \\ Z'_2 = & Y & X & X & Z & I \\ Z'_3 = & Z & Y & Y & X & I \end{array}$$

The set $\mathcal{S}_e$ is generated group by the above generators. Since $\mathcal{B} \cong \mathcal{S}$, by Lemma 4.38 unitary operator U such that $C(\mathcal{S}) = U^{-1}\ (C(\mathcal{B}))U$. The operator U is applied only Alice's entangled qubits. U is called coding operation of EAQECC by $\mathcal{S}$.

Error operator must anti-commutes with $\mathcal{S}$ in that $C(\mathcal{S})$ can correct errors.

Assume that Alice sends a message to Bob via a quantum channel. An error correction process is needed to true transmission of the message. Entangled pairs are used for much more error corrections. Above encoding and decoding process with parameters can be summarized as the following:

- Alice and Bob share a single entangled pair of qubits. $(c = 1)$
- Alice (sender) wants to encode a single qubit $|\varphi\rangle$ to 4 qubits. $(n = 4, k = 1)$

- Alice performs encoding operation U on her original qubit $|\varphi\rangle$, on her half of the entanglement pair and two ancilla qubits. $(s = 2)$
- She transmits them to Bob by noisy quantum channel.
- Bob measures extended generators Z'_1, X'_1, Z'_2 and Z'_3 on the four received qubits and his half of entangled pair.
- Outcome of these 4 measurements gives error syndrome.

If error correction conditions are satisfied, Bob can correct the error and decode $|\varphi\rangle$.

4.3.4 Quantum Codes over Finite Fields

The space $H^n = H \otimes H \dots \otimes H$ is a $2^n -$dimensional Hilbert space where H is a $2-$dimensional Hilbert space. A quantum code of length n is defined as a subspace of $2^n -$dimensional Hilbert space. Hence, a quantum code which encodes k qubits to n qubits is a $2^k -$dimensional subspace of a $2^n -$dimensional Hilbert space and it is denoted by $[\![n,k]\!]$. An element of a quantum code space is called a *codeword.*

Let q be a power of a prime p and let C^q be a $q -$dimensional complex vector space which represents the states of a quantum mechanical system. We use $|u\rangle$ to denote the vectors of a distinguished orthonormal basis of C^q where $u \in F_q$. A quantum error correcting code Q is a k-dimensional subspace of $C^{q^n} = C^q \otimes C^q \otimes \dots \otimes C^q$ where $\otimes$ denotes tensor product.

In order to measure the performance of a code, we need to have an error model. The set ε_n is a basis for the vector space of a complex $q^n x q^n$ matrix which represents a set of the errors. The error operators play an important role on the coding procedure.

More information about the quantum computation can be found in [27].

Definition 4.39: [17] Let a and b be elements of F_q. We define the unitary operators $X(a)$ and $Z(b)$ on C^q by $X(a)|u\rangle = |\alpha + u\rangle$ and $Z(b)|u\rangle = \varepsilon^{Tr(bu)}|u\rangle$ where ε is a primitive pth root of unity as $\varepsilon = e^{2\pi i/p}$ and Tr denotes the trace operation from F_q to F_p.

Definition 4.40: [17] The set $\varepsilon = \{X(a)Z(b)|a, b \in F_q\}$ is a set of error operators. The set ε has the following properties:

i. The identity matrix belongs to ε.

ii. For all $E_1, E_2 \in \varepsilon, E_1E_2 = \lambda E_3$ for some $\lambda \in C$, $E_3 \in \varepsilon$.

iii. $Tr({E_1}^{+}E_2)$= 0 for all $E_1, E_2 \in \varepsilon$.

If a finite set of unitary matrices satisfies these properties, then it is called a *nice error basis*.

CHAPTER 5

QUANTUM CODES OVER EISENSTEIN-JACOBI INTEGERS

In this chapter, we construct quantum codes over EJ-integers. Quantum codes over these integers can be used for coding over two-dimensional signal space [6]. A new minimum weight and a new distance are defined on the quantum code. Error operators play an important role on the error detection and correction procedure. Especially, if a set of the error operators satisfies some certain properties, then it is called a nice error basis. The nice error basis has some advantages during the coding procedure. We illustrate that the set of the error operators which is defined with respect to residue class function μ is a nice error basis. Moreover, the commutative property of the error operators is important in some cases. We prove the commutativity relation between these operators. The construction of a quantum code over EJ-integers and an error basis are explained via examples. These new quantum codes can give codes with new and better parameters.

The set of Eisenstein-Jacobi integers is a subset of the complex numbers such that these integers have a real and rho part [35]. Classical codes over Eisenstein-Jacobi integers are constructed and a distance is defined by Huber in [5]. The Eisenstein-Jacobi integer ring which has a unique factorization is the algebraic integer ring of cyclotomic field $Q(\sqrt{-3})$. The multiplicative group of units in the Eisenstein-Jacobi integer ring which has a unique factorization may be infinite. So, we should study on quotient ring of this ring. Although the factorization of this structure is difficult, an algorithm is given in [6]. Quadrature amplitude modulation (QAM) is both a digital and an analog modulation scheme. QAM signals belong to a type of two-dimensional signal spaces. The signal set can be obtained by factoring the multiplicative group of units in the quotient ring. Also, block codes can be constructed by using the factorization. Therefore, for coding over two-dimensional signal spaces like QAM signals, block codes over these integers; $p = 7, 13, 19, 31, 37, 43, 61, \ldots$, can be useful [6].

Firstly, we will give a formal definition of Eisenstein- Jacobi integers.

Definition 5.1 [35] Eisenstein-Jacobi integers (EJ-integers) are complex numbers defined by $a + \rho . b$ where $a, b \in Z$ and $\rho = \frac{-1+\sqrt{3}i}{2}$. The set of all EJ-integers is denoted by J. If $\alpha = a + \rho . b \in J$, then $\alpha^* = a + \rho^2 . b$ is called the conjugate of α where $\rho^2 + \rho + 1 = 0$. The norm of the element α is defined by $N(\alpha) = a^2 - ab + b^{\,2} = \alpha\alpha^*$. There are six elements whose norms are 1 of the set of EJ-integers. These elements are $1,\ -1,\ \rho,\ -\rho,\ \rho^2$ and $-\rho^2$. In other words, these elements are called the unities of the set. Then, the set $\{1,\ -1,\ \rho,\ -\rho,\ \rho^2,\ -\rho^2\}$ is the unities of the set of EJ-integers.

If any prime p is of the form $p = 6k + 1$ where $k \in Z$, then it can be written as $p = a^2 + 3b^2$ where $a, b \in Z$. We have $\pi\pi^* = p = a^2 + 3b^2$ where $\pi = a + b + \rho . 2b$ and $\pi^* = a + b + \rho^2 . 2b$.

We can define the modulo function as follows:

$$\mu_0 : J \to J_\pi$$

where J is all EJ-integers and J_π is the residue class of J modulo π. This function is defined by

$$\mu_0(a) = a - \left[\frac{a\pi^*}{\pi\pi^*}\right]\pi.$$

The operation of $[.]$ denotes rounding to the closest Einstein-Jacobi integer.

The map $\mu : GF(p) \to J_\pi$ is defined by $\mu(a) = a - \left[\frac{a\pi^*}{\pi\pi^*}\right]\pi$ is a one to one and onto homomorphism. Hence, $GF(p) \cong J_\pi$. The isomorphism leads to a relation between a field with p elements and EJ-integers. When $GF(p)$ is represented as J_π, it provides important advantages for coding as physically meaning like signal constellations [6].

Example 5.2 Let $p = 7$ and $\pi = 3 + \rho . 2$. Then, $J_{3+\rho.2} = \{0, 1, -1, \rho, -\rho, 1 + \rho, -1 - \rho\}$ and we will construct a code over $J_{3+\rho.2}$. Let the generator matrix of code C over $J_{3+\rho.2}$ be $(\ \rho, 1)$. Then, $C = \{(0,0), (\rho, 1), (-\rho, -1), (-\rho - 1, \rho), (\rho + 1, -\rho), (-1, 1 + \rho), (-1, -1 - \rho)\}$.

Example 5.3 Let $p = 19$ and π =5+$\rho.2$. Then,

$J_{5+\rho.2} = \{0,1,-3-2\rho,-2-2\rho,-1-2\rho,\ 3+3\rho,-1+\rho,\ \rho,1+\rho,2+\rho,-2-\rho,-1-\rho,-\rho,\ 1-\rho,-3-3\rho,\ 1+2\rho,\ 2+2\rho,\ 3+3\rho,-1\}$.

$C = \{(0,0,0,0),(1,\rho,-\rho,3+3\rho),(-2-\rho,-1,+2\rho,\rho),(1,0,-1,-1-\rho)\}$ is a code of length 4 over $J_{5+\rho.2}$.

5.1 Error Correction with EJ-Integers

In order to construct a code over $J_{3+\rho.2}$, Huber defined a new distance and a new weight for EJ-integers [5]. Let α_1 and α_2 be elements of J_π and $\alpha = \alpha_2 - \alpha_1$. The element α can be written in several different ways as $\alpha = g_1\varepsilon_1 + g_2\varepsilon_2$ where $\varepsilon_1, \varepsilon_2 \in \{1,-1,\rho,-\rho,1+\rho,-1-\rho\}$.

The weight of α is defined as $w(\alpha) = \min\{|g_1| + |g_2|\}$ in [2]. The distance d between α_1 and α_2 is defined as $d(\alpha_1,\alpha_2) = w(\alpha)$.

Example 5.4 Let $p = 7$ and π =3+$\rho.2$. Assume that $\alpha_1 = 1+\rho$, $\alpha_2 = -1 \in J_{3+\rho.2}$. Let α be the difference between α_1 and α_2. Then, $\alpha = \alpha_2 - \alpha_1 = -2-\rho$. Thus, α can be written in several different ways as $\alpha = -2.1 - 1.\rho$, $\alpha = -1.(1+\rho) - 1.1$, $\alpha = 1.(-1-\rho) - 1.1$, $\alpha = 2.(-1-\rho) + 1.\rho$. Therefore, we obtain $w(-2-\rho) = min\{3,2,2,3\} = 2$, since $w(\alpha) = min\{|g_1| + |g_2|\}$.

In general, the weight of the vector $u = (u_0, u_1, \dots, u_{n-1}) \in J_\pi$ is defined by $w(u) = \sum_{j=0}^{n-1} w(u_j)$ and the distance between the vectors u and v is defined by $w(v-u)$. The distance satisfies the following properties: $d(u,v) = d(v,u)$, $d(u,v) \geq 0$, if $u = v$ then $d(u,v) = 0$, and $d(u,t) \leq d(u,v) + d(v,t)$. Hence, d defines a metric.

We will construct a one-error-correcting code over J_π of length $n = \frac{p-1}{6}$. Errors can be any value from the set $\{1,-1,\rho,-\rho,1+\rho,-1-\rho\}$. Let $\alpha \in J_\pi$ be a primitive root of order $p-1$. A one-error-correcting code over J_π can be constructed by the following parity-check matrix H:

$$H = \left(\alpha^0, \alpha^1, \dots, \alpha^{\frac{p-1}{6}-1}\right).$$

A codeword c over J_π gives $Hc^T = 0$.

The generator matrix G is given by

$$G = \begin{pmatrix} -\alpha^1 & 1\,0\,\ldots\,0 \\ -\alpha^2 & 0\,1\,\ldots\,0 \\ \vdots & \ddots \\ \alpha^{\frac{p-1}{6}-1} & 0\,0\,\ldots\,1 \end{pmatrix}.$$

A single error which is in $\{1, -1, \rho, -\rho, 1+\rho, -1-\rho\}$ will produce a different syndrome. Next, we will describe the decoding procedure. Let $r = c + e$ be a received vector and we compute syndrome $(s) = Hs^T$. The location of an error which has weight one is given by $l = log_\alpha s \ mod\ n$ and the value of an error is given by $s\alpha^{-l}$.

Example 5.5 Let $p = 13$, $\pi = 3 + \rho.4$ and $\alpha = 1 + 2\rho$. Then,

$$H = (1, 1 + 2\rho), G = (-1 - 2\rho, 1).$$

Assume that the received vector is $r = (2\rho, -\rho)$. Then, we compute the syndrome as $s = Hr^T = -\rho - 1 = \alpha^8$. We can find the position of the error is 0 since $\log_\alpha \alpha^8 = 8$ and 8 is equivalent to 0 modulo 2. The value of the error is that $s\alpha^{-0} = -\rho - 1$. So, $e = (-\rho - 1, 0)$. Then, $c = r - e = (2\rho, -\rho) - (-\rho - 1, 0) = (3\rho + 1, -\rho) = (-\rho - 1, -\rho)$.

These codes can be generalized to the codes of length $n = \frac{p^r - 1}{6}$. Similarly, the parity-check matrix can be defined by

$$H = \left(\alpha^0, \alpha^1, \ldots, \alpha^{\frac{p^r-1}{6}-1}\right)$$

where $\alpha \in J_{\pi^r}$ is an element of order $p^r - 1$. A bijective map from $GF(p^r)$ to J_{π^r} can be defined as $\mu_r: GF(p^r) \to J_{\pi^r}$ where $\mu_r(a) = a - \left[\frac{a(\pi^r)^*}{(\pi^r)(\pi^r)^*}\right]\pi^r$ for all $a \in GF(p^r)$. Hence, $GF(p^r)$ is isomorphic to J_{π^r} since μ_r is a one to one and onto homomorphism.

Let p be a prime such that $p \equiv 1\ (mod\ 6)$. A p-ary quantum code Q of length n and size K is a K-dimensional subspace of a $p^n -$ dimensional Hilbert space. A distinguished orthonormal basis of C^p is denoted by vector $|u\rangle$ where u is an element of J_π. For n-tuple vectors $a = (a_0, a_1, \ldots, a_{n-1})$ and $b = (b_0, b_1, \ldots, b_{n-1}) \in J_\pi^n$, usual inner product on J_π is given by $a \cdot b = \sum_{j=0}^{n-1} a_i b_i$. For $(a|b), (a'|b') \in J_\pi^{2n}$, $(a|b) * (a'|b') = Tr(ba' - b'a)$ where $Tr: J_{\pi^r} \to J_\pi$ is the trace map. The notation $(a|b)$ denotes $2n$-tuple vector which is composed by a and b.

We can define a new weight w and distance d over EJ-integers as follows:

$$wt_J(w) = \left\lceil \frac{\begin{array}{c}[\min\{|g_{0,1}| + |g_{0,2}|\} + \cdots + \min\{|g_{n-1,1}| + |g_{n-1,2}|\} + \\ \min\{|g'_{0,1}| + |g'_{0,2}|\} + \cdots + \min\{|g'_{n-1,1}| + |g'_{n-1,2}|\}]\end{array}}{2} \right\rceil$$

where $w = (a|b) - (a'|b') = (a_j - a'_j|b_j - b'_j) = (w_j|w'_j) \mod \pi$, and $d_J((a|b),(a'|b')) = wt_J(w)$.

Let C be a code over J_π^{2n}. Then, the dual code of C is defined as:

$C^{\perp *} = \{(a|b) \in J_\pi^{2n} \colon (a|b) * (a'|b') = 0 \text{ for all } (a'|b') \in C\}$.

5.2 Error Operators

Definition 5.6: We define unitary operators as $X(a)|u\rangle = |\mu(\alpha + u)\rangle$ and $Z(b)|u\rangle = \varepsilon^{\mu^{-1}(bu)}|u\rangle$ where $a, b \in J_\pi$ and ε is a primitive pth root of unity, and $\mu \colon F_p \to J_\pi$ defined by $\mu(a) = a - \left[\frac{a\pi^*}{p}\right]\pi$.

Hadamard gate is defined as follows:

$H = \frac{1}{\sqrt{p}}(a_{s,t})$ where $a_{s,t} = \varepsilon^{(s-1)(t-1)\,(mod\ p)}$ for $1 \leq s, t \leq p$.

Proposition 5.7: The set $\varepsilon_J = \{X(a)Z(b)|\ a, b \in J_\pi\}$ is a nice error basis on C^q where $q = \pi\pi^*$.

Proof.

i) The operator $X(0)Z(0)$ acts as follow: $X(0)Z(0)|u\rangle = X(0)(\varepsilon^{\mu^{-1}(0)}|u\rangle) = X(0)|u\rangle = |0 + u\rangle = |u\rangle$. Since $X(0)Z(0)|u\rangle = |u\rangle$, $X(0)Z(0)$ is the identity matrix in ε_J.

ii) We have $\varepsilon^{\mu^{-1}(ab)}X(a)Z(b) = Z(b)X(a)$ and this implies that $X(a)Z(b)X(a')Z(b') = \varepsilon^{\mu^{-1}(a'b)}X(a)X(a')Z(b)Z(b')$

$$= \varepsilon^{\mu^{-1}(a'b)}X(a + a')Z(b + b')$$

for all $X(a)Z(b), X(a')Z(b') \in \varepsilon_J$. Since $X(a + a')$ and $Z(b + b')$ are elements of ε_J, the product of any two operators $X(a)Z(b)X(a')Z(b')$ is a scalar multiple of an operator in ε_J.

iii) Let $E_1 = X(a)Z(b)$ and $E_2 = X(a')Z(b')$ be two error operators where $a \neq a'$. The operator ${E_1}^{+}E_2 = Z(-b)Z(a-a')Z(b')$ which implies that the diagonal elements of the matrix ${E_1}^{+}E_2$ are 0. Therefore, $Tr({E_1}^{+}E_2) = 0$ where E_1 and E_2 are different elements of ε_J. Since i), ii) and iii) are satisfied, ε_J is a nice error basis.

Theorem 5.8 Let $X(a)Z(b)$ and $X(a')Z(b')$ be two operators such that $X(a)|u\rangle = |\mu(\alpha+u)\rangle$ and $Z(b)|u\rangle = \varepsilon^{\mu^{-1}(bu)}|u\rangle$. Operators $X(a)Z(b)$ and $X(a')Z(b')$ are commutative if and only if $\mu^{-1}(b'a) - \mu^{-1}(ba') = 0$.

Proof. Since $X(a)|\mathrm{u}\rangle = |\mu(\alpha+u)\rangle \; and \; Z(b)|\mathrm{u}\rangle = \varepsilon^{\mu^{-1}(bu)}|\mathrm{u}\rangle$, we have $\varepsilon^{\mu^{-1}(ab)}X(a)Z(b) = Z(b)X(a)$. Let $X(a)Z(b)$ and $X(a')Z(b')$ be two operators. The product of two error operators is given by

$$X(a)Z(b)X(a')Z(b') = \varepsilon^{\mu^{-1}(ba')}X(a)X(a')Z(b)Z(b'),$$

$$X(a')Z(b')X(a)Z(b) = \varepsilon^{\mu^{-1}(b'a)}X(a')X(a)Z(b')Z(b).$$

We already have $X(a)X(a') = X(a')X(a)$ and $Z(b)Z(b') = Z(b')Z(b)$.

If $X(a)Z(b)$ and $X(a')Z(b')$ commute, we obtain $\varepsilon^{\mu^{-1}(ba')} = \varepsilon^{\mu^{-1}(b'a)}$. This implies that $\mu^{-1}(b'a) - \mu^{-1}(ba') = 0$.

Conversely, if $\mu^{-1}(b'a) - \mu^{-1}(a'b) = 0$, then $\mu^{-1}(b'a) = \mu^{-1}(a'b)$ which implies $\varepsilon^{\mu^{-1}(ba')} = \varepsilon^{\mu^{-1}(b'a)}$. Since $X(a)Z(b)X(a')Z(b') = \varepsilon^{\mu^{-1}(ba')}X(a)X(a')Z(b)Z(b')$ and $X(a')Z(b')X(a)Z(b) = \varepsilon^{\mu^{-1}(b'a)}Z(b)Z(b')X(a)X(a')$, we obtain $X(a)Z(b)X(a')Z(b') = X(a')Z(b')X(a)Z(b)$. This shows that these operators are commutative.

Example 5.9 Let $p = 13$, $\pi = 3 + \rho.4$ and the map $\mu(a) = a - \left[\frac{a\pi^*}{\pi\pi^*}\right]\pi$. We can find the following images of F_{13} under the map:

$\mu(0) = 0,\ \mu(1) = 1,\ \mu(2) = 2,\ \mu(3) = -\rho - 1,\quad \mu(4) = -\rho,\ \mu(5) = 2\rho,\ \mu(6) = 1 + 2\rho$, $\mu(7) = -2\rho - 1$, $\mu(8) = -2\rho,\ \mu(9) = \rho$,$\mu(10) = 1 + \rho,\ \mu(11) = -2, \mu(12) = -1$. Then, $J_{3+\rho.4} = \{\, 0, 1, 2\,,\ -\rho - 1, -\rho, 2\rho, 1 + 2\rho, -2\rho, 1\,, -2\rho, \rho, 1 + \rho, -2, -1\,\}$.

The error basis can be found by the method below:

$X(0)_{i,j} = \delta_{\mu(i),\mu(j)}$, $X(1) = \delta_{\mu(i+1),\mu(j)}$, $X(2) = \delta_{\mu(i+2),\mu(j)}$, $X(-\rho - 1) = \delta_{\mu(i+3),\mu(j)}$, $X(-\rho) = \delta_{\mu(i+4),\mu(j)}$, $X(2\rho) = \delta_{\mu(i+5),\mu(j)}$, $X(1 + 2\rho) = \delta_{\mu(i+6),\mu(j)}$, $X(-1 - 2\rho) = \delta_{\mu(i+7),\mu(j)}$, $X(-2\rho) = \delta_{\mu(i+8),\mu(j)}$, $X(\rho) = \delta_{\mu(i+9),\mu(j)}$, $X(1 + \rho) = \delta_{\mu(i+10),\mu(j)}$, $X(-2) = \delta_{\mu(i+11),\mu(j)}$, $X(-1) = \delta_{\mu(i+12),\mu(j)}$.

For example, $X(-\rho) = \begin{pmatrix} 0&0&0&0&1&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&1&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&1&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&1&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&1&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&1 \\ 1&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0&0&0&0&0&0 \end{pmatrix}$.

We define a distinguished orthonormal basis for $p = 13$ as follows:

$|0\rangle = (1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0)^t$,

$|\rho\rangle = (0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0)^t$,

$|-\rho\rangle = (0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0)^t$,

$|2\rangle = (0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0)^t$,

$|-2\rangle = (0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0)^t$,

$|-1 - 2\rho\rangle = (0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0)^t$,

$|1 + 2\rho\rangle = (0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0)^t$,

$|2\rho\rangle = (0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0)^t$,

$|-2\rho\rangle = (0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0)^t$,

$|-1\rangle = (0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0)^t$,

$|1\rangle = (0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1)\ ^t$,

$|\rho + 1\rangle = (0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0)^t$,

$|-\rho - 1\rangle = (0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0)^t$.

For instance, if an error acts on a vector: $X(\rho)|-\rho\rangle = |\mu(\rho - \rho)\rangle = |0\rangle$. Then,

$$Z(-1-\rho)|1\rangle = \varepsilon^{\mu^{-1}(-1-\rho)}|1\rangle = \varepsilon^{3}|1\rangle.$$

Suppose that we have a quantum state $|\varphi\rangle = |(2 \otimes (-3-\rho 4) \otimes -1 \otimes (1-\rho))\rangle$. Here, φ is a vector of length 4. If any error E occured in the third position, then error vector is $IIEI$. The action of the $X(2-\rho)$ is that $X(2-\rho)|-1\rangle = |\mu((2-\rho)-1)\rangle = |\mu((2-\rho)-1)\rangle = |1-\rho\rangle$. So, error vector is (0,0, $1-\rho$,0). Therefore, corrupted state becomes $|(2 \otimes (-3-\rho 4) \otimes (1-\rho) \otimes (1-\rho))\rangle$ if the error $IIX_{2-\rho}I$ occurred.

Theorem 5.10 [5] Let C_1 and C_2 be two classical linear codes over J_π with the parameters $[n, k_1, d_{J_1}]$ and $[n, k_2, d_{J_2}]$ such that $C_1 \subseteq C_2$. Then, there exists an $[[n, k_1 - k_2\ ,\ d_J\ ]]$ quantum code with the minimum distance $d_J = min\{d_{J_1}, {d_{J_2}}^{\perp}\}$, where d_{J_1} denotes the new minimum distance of the code C_1 over J_π and ${d_{J_2}}^{\perp}$ denotes the new minimum distance of the dual code ${C_2}^{\perp}$ of the code C_2 over J_π.

Proof. Let $|a + C_2\rangle = \frac{1}{\sqrt{|C_2|}}\sum_{b\in C_2}|a \oplus_2 b\rangle$ where $\oplus_2$ is addition modulo 2. If $a - a' \in C_2$ where $a, a' \in C_1$, then $|a + C_2\rangle = |a' + C_2\rangle$. Also, if a and a' belong to distinct cosets of C_2, then there do not exist $b, b' \in C_2$ such that $a + b = a' + b'$ and so $|a + C_2\rangle$ and $|a' + C_2\rangle$ are orthonormal.

The quantum CSS code which is defined by C_1, C_2 is spanned by $|a + C_2\rangle$ for all $a \in C_1$. The number of cosets of C_2 in C_1 is $\frac{|C_1|}{|C_2|}$. Hence, the dimension of the CSS code is $\frac{|C_1|}{|C_2|} = \frac{2^{k_1}}{2^{k_2}} = 2^{k_1-k_2}$. So, the quantum CSS code which is defined by C_1 and C_2 is an $[n, k_1 - k_2]$-code.

In order to detect and correct quantum errors, we can use the classical error correcting properties of C_1 and ${C_2}^{\perp}$. An n bit vector ε_1 describes bit flip errors such that there are 1s where bit flips occurred and there are 0s elsewhere. An n bit vector ε_2 describes phase flip errors such that there are 1s where phase flips occurred and there are 0s elsewhere. Let $|a + C_2\rangle$ be the initial state. If some errors occurred, then the corrupted state is:

$$\frac{1}{\sqrt{|C_2|}}\sum_{b\in C_2}(-1)^{(a+b)\varepsilon_2}|a + b + \varepsilon_1\rangle.$$

To detect the location of bit flips, we introduce ancilla qubits. Since $(a + b) \in C_1$ is annihilated by matrix H_1, $|a + b + \varepsilon_1\rangle|0\rangle$ to $|a + b + \varepsilon_1\rangle|H_1(a + b + \varepsilon_1)\rangle = |a + b + \varepsilon_1\rangle|H_1\varepsilon_1\rangle$ where H_1 is parity-check matrix of C_1 . Then, we obtain

$$\frac{1}{\sqrt{|C_2|}}\sum_{b\in C_2}(-1)^{(a+b)\varepsilon_2}|a+b+\varepsilon_1\rangle\,|H_1\varepsilon_1\rangle.$$

The detection procedure is completed by measuring ancilla qubits, then

$$\frac{1}{\sqrt{|C_2|}}\sum_{b\in C_2}(-1)^{(a+b)\varepsilon_2}|a+b+\varepsilon_1\rangle.$$

Since C_1 can correct up to t errors, if we know the error syndrome $H_1\varepsilon_1$, we can conclude the error ε_1. So, the error correction abilities of linear codes C_1 and C_2 are related to the quantum codes which are obtained by these linear codes. The complete proof is given in [4] and [5]. The quantum code which is constructed by using linear codes C_1 and C_2 is known as the CSS code.

Example 5.11 Let $\pi = 9 + \rho.4$ and let $c_1(x) = (x + 3 + \rho4)(x + 2 + \rho4) = x^2 - \rho x + \rho3 + 3$ be the generator polynomial of the code C_1 over $J_{9+\rho.4}$ and $c_2(x) = (x + \rho2 - 1)(x + \rho - 1) = x^2 + (\rho3 - 2)x - \rho5 - 1$ be the generator polynomial of the code C_2 over $J_{9+\rho.4}$. The code C_1 which is generated by $c_1(x)$ is a $[4,2,4]$ $-$code and the code C_2 which is generated by $c_2(x)$ is a $[4,2,6]$ $-$code. So, we can obtain a quantum code with respect to the new distance with parameters $[\![4,0,4]\!]_{9+\rho.4}$ by using CSS code construction of C_1 and C_2.

A table of more generator polynomials is given by Huber in [5].

CHAPTER 6

CONCLUSION

In this thesis, we introduced coding theory. We gave historical view of classical and quantum coding theory.

We gave some preliminaries about algebraic coding theory and we stated some definitions about error correcting codes by illustrating these with examples.

We introduced mathematical concepts of quantum mechanics. Also, we explained algebraic properties of quantum vectors and showed principals of quantum theory.

Moreover, we conducted a literature research about quantum error correcting codes. We explained some types of quantum codes with details and we illustrated these codes with examples. Furthermore, we gave error detection and correction conditions. Also, we mentioned about relation between classical and quantum codes.

We gave the definition of Eisenstein-Jacobi integers and we showed that there is an isomorphism between the set of these integers and a finite field. This isomorphism provides a construction of quantum codes over Eisenstein-Jacobi integers. We defined a new distance for this new class of quantum codes, and we described error bases, matrices and operators of them. Also, we proved the commutative property of error operators with respect to this new distance. Obtaining these codes can lead an answer for the existence question for some new parameters.

Another class of quantum codes can be researched in the future. Finding a new code with better parameters is always an open problem.

REFERENCES

[1] Shannon, C. E. (1948). A mathematical theory of communication, bell System technical Journal 27: 379-423 and 623–656. Mathematical Reviews (MathSciNet): MR10, 133e.

[2] Ingarden, R. S. (1976). Quantum information theory. Reports on Mathematical Physics, 10(1): 43-72.

[3] Benioff, P. (1980). The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. Journal of statistical physics, 22(5): 563-591.

[4] Deutsch, D. (1985, July). Quantum theory, the Church-Turing principle and the universal quantum computer. In Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences 400(1818): 97-117.

[5] Huber K., (1994)" Codes over Eisenstein-Jacobi integers," Contemporary Mathematics 168: 165-165.

[6] Dong, X. D., Soh, C. B., Gunawan, E., and Tang, L. Z. (1998). Groups of algebraic integers used for coding QAM signals. IEEE Transactions on Information Theory, 44(5): 1848-1860.

[7] W. Shor, P., (1995). "Scheme for reducing decoherence in quantum computer memory", Physc. Review A, 52:R2493-R2496.

[8] Andrew, S. (1996). "Multiple-partical interference and quantum error correction", Proc. Roy. Soc. Lond., A452:2551-2577.

[9] Calderbank, A. R. and W. Shor, P., (1996). "Good Quantum Error Correcting Codes Exist", Physc. Review A, 54:1098-1105.

[10] Andrew, S., (1996). "Simple Quantum Error Correcting Codes", Physc. Review A, 54:4741-4751.

[11] Knill, E., Laflamme, R., Ashikhmin, A., Barnum, H., Viola, L., and Zurek, W. H. (2002). Introduction to quantum error correction. arXiv preprint quant-ph/0207170.

[12] Majek.P., (2005). Quantum Error Correcting Codes. PhD Thesis, Bratislava.

[13] Danniel, G. (1997). Stabilizer Codes and Quantum Error Correction, Ph. D. Thesis, California Institute of Technology, California.

[14] Calderbank, A. R., Rains, E. N., W. Shor, P. and Sloane, N. S., (1998). "Quantum Error Correction via Codes Over $GF(4)$", IEEE Trans. Infor. Theory, 44:1369- 1387.

[15] Li, R. and Li, X., (2004). “Binary Consruction of Quantum Codes of Minimum Distance Three and Four”, IEEE Trans. Infor. Theory, 50:1331-1336.

[16] Ashikhmin, A. and Knill, E., (2001). Nonbinary quantum stabilizer codes. IEEE Transactions on Information Theory, 47(7): 3065-3072.

[17] Ketkar, A., Klappenecker, A., Kumar, S. and Sarvepelli, P.K., (2006). “Nonbinary Stabilizer Codes Over Finite Field”, IEEE Trans. Infor. Theory, 52:4892-4914.

[18] Brun, T., Devetak, I. and Hsieh, M. H., (2006). Correcting quantum errors with entanglement. Science, 314(5798): 436-439.

[19] Qian, J., and Zhang, L., (2015). Entanglement-assisted quantum codes from arbitrary binary linear codes. Designs, Codes and Cryptography, 77(1): 193-202.

[20] Shin, J., Heo, J. and Brun, T. A., (2011). Entanglement-assisted codeword stabilized quantum codes. Physical Review A, 84(6): 062321.

[21] Wilde, M. M. (2008)., Quantum coding with entanglement. arXiv preprint arXiv:0806.4214.

[22] Aly, S. A. and Klappenecker, A. (2008, July). Subsystem code constructions. In Information Theory, 2008. ISIT 2008. IEEE International Symposium on (pp. 369-373). IEEE.

[23] Ling, S. and Xıng, C., (2004). A First Course In Coding Theory, Cambridge University Press, New York.

[24] Huffman, W. C. and Pless, V., (2003). Fundamental of Error Correcting Codes, First Edition, Cambridge University Press, New York.

[25] Roman, S., (1992). Coding and information theory (Vol. 134). Springer Science & Business Media.

[26] Bennett, C. H. and Shor, P. W. (1998). Quantum information theory. IEEE transactions on information theory, 44(6): 2724-2742.

[27] A. Nielsen and L. Chuang, I., (2008). Quantum Computation and Quantum Information, First Edition, The Press Syndicate of the University of Cambridge, Cambridge.

[28] Kaye, P., Laflamme, R. and Mosca, M., (2007). An Introduction to Quantum Computing, Oxford University Press, New York.

[29] Djordjevic, I., (2012). Quantum information processing and quantum error correction: an engineering approach. Academic press.

[30] Rieffel, E. G. and Polak, W. H., (2011). Quantum computing: A gentle introduction. MIT Press.

[31] Mermin, N. D., (2007). Quantum computer science: an introduction. Cambridge University Press.

[32] Desurvire, E., (2009). Classical and quantum information theory: an introduction for the telecom scientist. Cambridge University Press.

[33] Diósi, L., (2011). A short course in quantum information theory: an approach from theoretical physics (Vol. 827). Springer.

[34] McMahon, D., (2007). Quantum computing explained. John Wiley & Sons.

[35] Hardy, G. H., & Wright, E. M. (1979). An introduction to the theory of numbers. Oxford University Press.

[36] Einstein, A., Podolsky, B., and Rosen, N. (1935). Can quantum-mechanical description of physical reality be considered complete?. Physical review, 47(10): 777.

[37] Gisin, N., & Bechmann-Pasquinucci, H. (1998). Bell inequality, Bell states and maximally entangled states for n qubits. Physics Letters A, 246(1-2): 1-6.

[38] Sanpera, A., Bruß, D., and Lewenstein, M. (2001). Schmidt-number witnesses and bound entanglement. Physical Review A, 63(5): 050301.

CURRICULUM VITAE

PERSONAL INFORMATION

Name Surname: Eda YILDIZ

Date of birth and place: 01/01/1994 İSTANBUL

Foreign Language: English

E-mail: edayildiz_93@hotmail.com

EDUCATION

Degree	Department	School/University	Date of Garaduation
Bachelor	Mathematics	Yildiz Technical University	2015
High School	Science	Rami Atatürk High School	2011

WORK EXPERIENCE

Year	Institution	Enrollment
2017	Yildiz Technical University	Research Assistant

PUBLISHMENTS

Conference Papers

1- Yildiz,E., Demirkale F., (2017). Quantum Codes over Eisenstein-Jacobi Integers, Seventh International Conference on Modeling, Simulation and Applied Optimization, American University of Sharjah, Sharjah, United Arab Emirates, IEEE Xplore.