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

ON t-SPONTANEOUS EMISSION ERROR DESIGNS AND RELATED QUANTUM JUMP CODES

EMRE ERSOY

MSc. THESIS
DEPARTMENT OF MATHEMATICS
PROGRAM OF MATHEMATICS

ADVISER
ASSOC. PROF. EMRE KOLOTOĞLU

ISTANBUL, 2017

REPUBLIC OF TURKEY

YILDIZ TECHNICAL UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

ON *t*-SPONTANEOUS EMISSION ERROR DESIGNS AND RELATED QUANTUM JUMP CODES

A thesis submitted by Emre ERSOY 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. Emre KOLOTOĞLU

Yıldız Technical University

Approved By the Examining Committee

Assoc. Prof. Emre KOLOTOĞLU

Yıldız Technical University ______________________

Assoc. Prof. Fatih DEMİRKALE

Yıldız Technical University ______________________

Assoc. Prof. Sibel ÖZKAN

Gebze Technical University ______________________

ACKNOWLEDGEMENTS

First, I would like to thank my family, especially my father who I most wanted to see my graduation, teaching me how to struggle against difficulties in my life. I also would like to thank my mother and other family members for endless loves and their belief in me.

I am grateful to my advisor Assoc. Prof. Emre KOLOTOĞLU for his support and suggestions. He taught me how to write and read an academic paper. I need to mention that his attention to every detail led my thesis to be completed. The courses; Discrete Mathematics, Group Theory, and Design Theory, I took from him provided a lot of benefits.

I also would like to thank Prof. Bayram Ali ERSOY who inspired me throughout my education life. His support has a big impact on my education. I am grateful to all members of Mathematics department of Yıldız Technical University for the courses that I took throughout my university education. Many thanks to all my friends for their patience, support, and friendship even in my bad days.

Besides my advisor, my sincere thanks also go to member of my thesis committee Assoc. Prof. Fatih DEMİRKALE for the questions that he asked during the seminars. These questions made me to think more and understand the topics. I also would like to thank to Assoc. Prof. Sibel ÖZKAN and all my thesis committee for insightful comments.

Last but not least I dedicate this thesis to my late father who has been my constant source of inspiration. Dear father, this is for you.

May, 2017

Emre ERSOY

TABLE OF CONTENTS

Page

CHAPTER 3

CHAPTER 4

CHAPTER 5

LIST OF SYMBOLS

$\emptyset$	Empty set
$\mathbb{C}$	Set of complex numbers
$\mathbb{Z}$	Set of integers
$\mathbb{Z}_p$	Set of integers in modulo p
$\mathcal{F}_q$	Finite field of order q
$\mathbb{F}$	$\mathcal{F}_2 = \{0, 1\}$
$\mathcal{H}$	Hilbert space
$\bar{\mathcal{D}}$	Complement of $\mathcal{D}$
$\mathcal{D}_a$	Derived design at a
$\mathcal{R}_a$	Residual design at a
π_i	i^{th} parallel class
$\mathfrak{Q}$	Quasi group
$\mathcal{G}$	Automorphism group
Δ	Set of t-orbits
Γ	Set of k-orbits
$\mathcal{T}$	Operator
$\mathcal{P}$	Pauli group
$\mathcal{E}$	Error group
$\mathcal{C}$	Code
$\mathcal{J}$	Jump operator
$\mathbb{W}_k$	Decoherence-free subspace of fixed weight k
$\mathbb{D}(t)$	Decay operator
$\bar{x}$	Conjugate of vector x
$\|x\rangle$	Ket vector
$\langle x\|$	Bra vector
$\|x\rangle^\dagger$	Conjugate transpose of a vector x
$G\|X$	G acts on X
X/B	Set difference
$\mathcal{H}^{\otimes n}$	2^n-dimensional Hilbert space
$\langle\varphi\|\psi\rangle$	Inner product of $\|\psi\rangle$ and $\|\varphi\rangle$
$\|\psi\rangle\langle\varphi\|$	Outer product of $\|\psi\rangle$ and $\|\varphi\rangle$
$A \otimes B$	Tensor product of A and B
$wt(\|x\rangle)$	Hamming weight of x
$span(S)$	Span of S
$supp(x)$	Support of vector x
$S(t, k, v)$	Steiner t-design
$\gcd(a, b)$	Greatest common divisor of a and b

LIST OF ABBREVIATIONS

KM	Kramer-Mesner
LSTS	Large set of Steiner system
STS	Steiner triple system
SQS	Steiner quadruple system
t-SEED	t-spontaneous emission error design

LIST OF FIGURES

Page

LIST OF TABLES

Page

ABSTRACT

ON t-SPONTANEOUS EMISSION ERROR DESIGNS AND RELATED QUANTUM JUMP CODES

Emre ERSOY

Department of Mathematics

MSc. Thesis

Adviser: Assoc. Prof. Emre KOLOTOĞLU

Quantum computers are designed to solve the problems those either cannot be solved or takes long time to solve by classical computers, fastly. One of the most known problems is the factorization problem of integers. Factorization of very large integers cannot be done in a reasonable time even with today's best computers. It is believed that quantum computers will solve the factorization problem within few minutes. Some errors occur in quantum systems while data transfer. In order to correct such errors, quantum error correcting codes have been developed. Combinatorial structures of quantum error correcting codes have been studied and the relation between quantum error correction codes and combinatorial designs has been analyzed by many researchers. In this thesis, the studies in the field of t-*spontaneous emission error design*, shortly t-SEED, are surveyed and written in a more clear and understandable way of exemplification.

In the first chapter, literature review was done. In the second chapter, fundamental definitions and theorems in combinatorial design theory are given with examples. In the third chapter, quantum computing, quantum error correction and quantum jump codes are described. The third chapter also provides some examples of quantum jump codes. In the fourth chapter, the relation between quantum jump codes and combinatorial designs are explained and t-spontaneous emission error designs (t-*SEED*) are introduced.

Key words: quantum jump codes, t-spontaneous emission error designs, t-*SEEDs*, large sets, resolvable designs.

YILDIZ TECHNICAL UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

ÖZET

t-SPONTANE YAYINIM HATA TASARIMLARI VE İLİŞKİLİ KUANTUM ATLAMA KODLARI ÜZERİNE

Emre ERSOY

Matematik Anabilim Dalı

Yüksek Lisans Tezi

Tez Danışmanı: Doç. Dr. Emre KOLOTOĞLU

Kuantum bilgisayarlar günümüzde kullanılan bilgisayarların çözemediği ya da çözümünün uzun sürdüğü problemleri çok kısa sürede çözebilecek şekilde tasarlanmıştır. En bilindik problemlerden biri de çarpanlara ayırma problemidir. Şu an kullanılan en iyi bilgisayarlarla bile çok büyük tam sayıların çarpanlara ayırılması çok uzun zaman alıcı bir problemdir. Kuantum bilgisayarların bu problemi birkaç dakika içerisinde çözebileceği ön görülmektedir. Kuantum bilgisayarlarda veri transferi sırasında bazı hatalar oluşmaktadır. Bu hataların giderilebilmesi için kuantum hata düzelten kodlar geliştirilmiştir. Kuantum hata düzelten kodların kombinatoryel yapıları incelenmiş ve kuantum hata düzelten kodlar ile kombinatoryel tasarımlar arasında bağlantı bulunmuştur. Bu tezde, t-spontane yayınım hata tasarımları alanındaki çalışmalar araştırılmış ve daha anlaşılabilir bir dil ile örneklendirmeler yapılmıştır.

Tezin ilk bölümünde literatür özeti verilmiştir. İkinci bölümde, kombinatoryel tasarım teorisinden temel tanımlar ve teoremler örneklendirilerek verilmiştir. Üçüncü bölümde, kuantum hesaplama, kuantum hata düzeltme ve kuantum atlama kodları tanımlanmıştır. Üçüncü bölümde, bazı kuantum atlama kod örnekleri verilmiştir. Dördüncü bölümde, kuantum atlama kodları ve kombinatoryel tasarımlar arasındaki bağlantı verilmiş ve t-spontane yayınım hata tasarımları tanımlanmıştır.

Anahtar Kelimeler: kuantum atlama kodları, t-spontane yayınım hata tasarımı, büyük kümeler, çözülebilir tasarımlar.

CHAPTER 1

INTRODUCTION

1.1 Literature Review

Combinatorial design theory has its roots in the famous mathematical puzzles (problems) that asked at the end of the eighteenth century. The very first problem was a prize question that published in "Lady's and Gentleman's Diary" asked by W. S. B. Woolhouse in 1844. The question give raise to studies on triple systems. T. P. Kirkman [1] found a solution to this problem in 1847. In the following years, Kirkman [2] posed a question which is known as "Kirkman's schoolgirl problem".

"Fifteen young ladies in a school walk out three abreast for seven days in succession: it is required to arrange them daily so that no two shall walk twice abreast." Kirkman, 1850.

This problem led to studies on resolvable triple systems. Although Kirkman already introduced the triple systems, Steiner [3] was unaware of these works, and reintroduced triple systems in 1853. Even today, after Steiner's works, triple systems are used with the name of Steiner instead of Kirkman. One of the oldest problems in combinatorial design theory which was asked by Jakob Steiner in 1853 was about existence of triple systems. Until 2014, this problem has been studied by many authors [see; 4, 5, 6, 7]. Peter Keevash [8] published a paper on existence of Steiner systems in 2014, and proved the existence of such designs. Another problem is known as "36 officers problem" which is asked by L. P. Euler [9] in 1872.

"Six different regiments have six officers, each one belonging to different ranks. Can these 36 officers be arranged in a square formation so that each row and column contains one officer of each rank and one of each regiment?" Euler, 1872.

To find a solution to this problem many authors studied mutually orthogonal Latin squares. However, Euler conjectured that there was no solution to this problem, and after a century later Gaston Tarry [10, 11] proved the Euler's conjecture in 1901.

Combinatorial design theory gained new research areas at the beginning of nineteenth century, with the discovery of the connection between combinatorial designs and statistical design of experiments. The most known works are [12, 13, 14] by R. A. Fisher and F. Yates. These works led to some new research topics on applications of designs. In the work [14], "balanced incomplete block designs" were introduced and this type of design is still one of the most studied topics in combinatorial design theory.

In 1948, C. E. Shannon [15] published a paper that named "*A mathematical theory of communication*" which led to foundation of information theory. Shannon also proved the existence of codes that correct errors in communication systems. However, Shannon did not give any construction of such codes. In the following years, R. W. Hamming [16] described methods on linear codes. With Hamming's works, combinatorial structures of codes become a new research area. By using the combinatorial designs, new code families can be found. After the realization of the relation between combinatorial designs and codes, each discipline give contributions to other's development. With the establishment of quantum information theory which consist of quantum physics and information theory, some pioneering works have seen. One of the most important papers is Shor's [17] paper named "*Scheme for reducing decoherence in quantum computer memory*". Shor stated that error correction is possible in quantum systems. Shor [17] and Steane [18] gave some constructions on quantum error correcting codes. Many authors [19, 20, 21] used combinatorial designs to construct quantum error correcting codes. In 2001, Alber *et al*. [22] introduced an error correction model which corrects the errors caused by quantum jumps and quantum decay. In the following years, Beth *et al*. [23] proposed a new class of combinatorial designs to construct quantum jump codes. This new class named as t-*spontaneous emission error design*, abbreviated as t-*SEED*. Beth *et al*. [23] gave a general bound on t-*SEED*s. Many authors [24, 25, 26, 27, 28, 29, 30, 31] published papers on existence and non-existence of t-*SEED*s for special parameters.

1.2 Objective of the Thesis

In this thesis, the studies in the field of t-*spontaneous emission error design*, shortly t-$SEED$s, are surveyed and written in a more clear and understandable way of exemplification. The main objective of this thesis, is to describe the relation between quantum jump codes and combinatorial designs. The works done by Alber *et. al*. [22], Beth *et. al.* [23] and Jimbo *et. al.* [24] are source materials of this thesis.

In the second chapter, fundamental definitions and theorems in combinatorial design theory will be given with examples. In the third chapter, quantum computing, quantum error correction and quantum jump codes are described. The third chapter also provides some examples of quantum jump codes. In the fourth chapter, the relation between quantum jump codes and combinatorial designs are explained and t-*SEED*s are introduced.

Another objective of this thesis is to be a useful source for researchers who are willing to learn quantum jump codes and t-*SEED*s. Therefore, we tried to give examples as much as possible for each definition and theorem.

1.3 Hypothesis

The quantum jump error which occurs in quantum systems can be corrected by quantum coding. There is a natural connection between quantum jumps and combinatorial designs. Quantum jump codes can be obtained from some types of combinatorial designs.

CHAPTER 2

INTRODUCTION TO COMBINATORIAL DESIGNS

Design theory is one of the wide areas of discrete mathematics. Design theory can be briefly described as the arrangement of elements of a finite set into subsets which satisfy some prescribed rules. Combinatorial designs have many applications including computer science, experimental designs, genetics, scheduling and more. There are many types of designs which provides solutions to various problems. In this thesis, we will mainly focus on some types of designs that include *t*-designs, Steiner Systems, and large sets of *t*-designs.

In the history of design theory, the most famous problems are about the existence of designs. Recently, many various studies have been done in the field which provides many existence and non-existence results. However, there are still many open problems.

Next definition provides a general definition for a combinatorial design.

Definition 2.1 A pair $(X, \mathfrak{B})$ in which the following two properties are satisfied is called a *combinatorial design*.

1. X is a finite set of elements which is called *points*, and
2. $\mathfrak{B}$ is a multiset of nonempty subsets of X, called *blocks*.

If two nonempty subsets (blocks) in $\mathfrak{B}$ have exactly same elements, they are called *repeated blocks*. That is the reason for using the term multiset instead of the term set. In a multiset, repeated elements are allowed. A design is called *simple design* if there are no repeated blocks in this design.

We now study one of the most studied type of designs, t-designs.

2.1 t - designs

2.1.1 Properties of t-designs

Definition 2.2 Let v, k, λ, and t be positive integers such that $v > k \geq t$. A $t-(v,k,\lambda)$ design is a design $(X, \mathfrak{B})$ such that the following properties are satisfied:

1. $|X| = v$,
2. Each block consists of exactly k points,
3. Every set of t distinct points is contained in precisely λ blocks.

It is clear that a $t-(v,k,\lambda)$ design may have repeated blocks. By the definition, if $\lambda = 1$, there cannot be any repeated blocks in this design. A $t-(v,k,\lambda)$ design is called *simple t-design* if there are no repeated blocks. Construction of simple designs is more difficult than constructing non-simple designs. A *t-design* is said to be *trivial t-design* if we take λ copies of each k-subset of a v-set. Trivial t-design is a $t-\left(v,k,\lambda\binom{v-t}{k-t}\right)$ design, where $k < v$.

Example 2.1 Let $X = \{a,b,c,d,e,f,1,2,3,4,5,6\}$ and

$$\mathfrak{B} = \{\{a,1\},\{b,2\},\{c,3\},\{d,4\},\{e,5\},\{f,6\}\}.$$

Then, $(X,\mathfrak{B})$ is a $1-(12,2,1)$ design.

Example 2.2 Consider a $2-(6,3,2)$ design. Let X and $\mathfrak{B}$ be defined as follows;

$$X = \{0,1,2,3,4,5\},$$

$$\mathfrak{B} = \{\{0,1,2\},\{0,1,3\},\{0,2,4\},\{0,3,5\},\{0,4,5\},\{1,2,5\},\{1,3,4\},\{1,4,5\},\{2,3,4\},\{2,3,5\}\}.$$

It is clear that $(X,\mathfrak{B})$ satisfies all properties of a $2-(6,3,2)$ design and this design is simple since there are no repeated blocks.

From now on, to save space, we write blocks in the form xyz instead of $\{x,y,z\}$.

Example 2.3 Let $X = \{0,1,2,3,4,5\}$ be a set of 6 points. Then $(X,\mathfrak{B})$ is a $2-(6,3,4)$ design with the following blocks.

$$\mathfrak{B} = \left\{\begin{matrix} 012,012,013,013,024,024,035,035,045,045, \\ 125,125,134,134,145,145,234,234,235,235 \end{matrix}\right\}$$

By taking the complement of each block, we again obtain a t-design.

Definition 2.3 Let $\mathcal{D} = (X, \mathfrak{B})$ be a $t-(v,k,\lambda)$ design. Then $C = (X, \mathfrak{B}')$, where $\mathfrak{B}' = \{X/B : B \in \mathfrak{B}\}$ is called the *complement design* of $\mathcal{D}$.

Theorem 2.4 Let $\mathcal{D} = (X, \mathfrak{B})$ be a $t-(v,k,\lambda)$ design and $\overline{\mathcal{D}} = (X, \mathfrak{B}')$ be the complement design of $\mathcal{D}$. Then, $\overline{\mathcal{D}} = (X, \mathfrak{B}')$ is a $t-(v, v-k, \lambda^*)$ where $\lambda^* = \frac{\lambda\binom{v-k}{t}}{\binom{k}{t}}$.

Proof. It is clear that each block of $\overline{\mathcal{D}}$ has exactly $|X| - |B| = v - k$ elements since blocks of $\overline{\mathcal{D}}$ defined by $\mathfrak{B}' = \{X/B : B \in \mathfrak{B}\}$. The number of blocks which does not contain a t-subset of $\mathcal{D}$ is $\frac{\lambda\binom{v-k}{t}}{\binom{k}{t}}$ by the principle of inclusion and exclusion.

Example 2.4 We consider *Example 2.3*. Then, we have the following set of blocks

$$\mathfrak{B}' = \begin{Bmatrix} 345, 345, 245, 245, 135, 135, 124, 124, 123, 123, \\ 034, 034, 025, 025, 023, 023, 015, 015, 014, 014 \end{Bmatrix}.$$

Here, incidentally, the block complement $(X, \mathfrak{B}')$ is again a $2-(6,3,4)$ design.

Example 2.5 Blocks of a $3-(10,4,1)$ design with the point set $X = \{0,1,2,3,4,5,6,7,8,9\}$ are given below.

0128	0136	0145	0179	0237	0246	0259	0349	0358	0478
0567	0689	1234	1257	1269	1359	1378	1467	1489	1568
2356	2389	2458	2479	2678	3457	3468	3679	4569	5789

Theorem 2.5 [32] Let $\mathcal{D} = (X, \mathfrak{B})$ be a $t-(v,k,\lambda)$ design, and $1 \le s \le t$. Then, $\mathcal{D} = (X, \mathfrak{B})$ is also an $s-(v,k,\lambda_s)$ design, where

$$\lambda_s = \frac{\lambda\binom{v-s}{t-s}}{\binom{k-s}{t-s}}.$$

Definition 2.6 Let $\mathcal{D} = (X, \mathfrak{B})$ be a $t-(v,k,\lambda)$ design and let $a \in X$. Then $\mathcal{R}_a = (X/\{a\}, \mathfrak{B}_a)$, where $\mathfrak{B}_a = \{B \in \mathfrak{B} : a \notin B\}$ is called the *residual design* at a.

Theorem 2.7 [32] Let $\mathcal{D} = (X, \mathfrak{B})$ be a $t-(v,k,\lambda)$ design and let $\mathcal{R}_a$ be the residual design at a where $a \in X$. Then $\mathcal{R}_a$ is a $(t-1)-\left(v-1, k, \lambda\frac{v-k}{k-t+1}\right)$ design.

Example 2.6 Let $\mathcal{D} = (X, \mathfrak{B})$ be a $2-(9,3,1)$ design. Let $X = \{0,1,2,3,4,5,6,7,8\}$.

$$\mathfrak{B} = \{012, 034, 056, 078, 135, 147, 168, 238, 246, 257, 367, 458\}.$$

Then, $\mathcal{R}_0 = (X/\{0\}, \mathfrak{B}_0)$ is the residual design at 0 of the design $\mathcal{D} = (X, \mathfrak{B})$ where

$$\mathfrak{B}_0 = \{135, 147, 168, 238, 246, 257, 367, 458\}.$$

Here, $\mathcal{R}_0$ a $1-(8,3,3)$ design.

Definition 2.8 Let $\mathcal{D} = (X, \mathfrak{B})$ be a $t-(v,k,\lambda)$ design and let $a \in X$. Then $\mathcal{D}_a = (X/\{a\}, \mathfrak{B}_a)$, where $\mathfrak{B}_a = \{B/\{a\} : a \in B \in \mathfrak{B}\}$ is called the *derived design* at a.

Theorem 2.9 Let $\mathcal{D} = (X, \mathfrak{B})$ be a $t-(v,k,\lambda)$ design and let $\mathcal{D}_a$ be the derived design at a where $a \in X$. Then $\mathcal{D}_a$ is a $(t-1)-(v-1,k-1,\lambda)$ design.

Proof. Let $\mathfrak{B}(a)$ be the set of blocks of the design $\mathcal{D} = (X, \mathfrak{B})$ that contains a given element a of X. Each $(t-1)$-subset of $X/\{a\}$ occurs with a in exactly λ blocks of $\mathcal{D}$, these blocks being those of $\mathfrak{B}(a)$. Thus, $(X/\{a\}, \mathfrak{B}_a)$, where $\mathfrak{B}_a$ is obtained from the blocks of $\mathfrak{B}(a)$ by removing a, is $(t-1)-(v-1,k-1,\lambda)$ design.

Example 2.7 Let $\mathcal{D} = (X, \mathfrak{B})$ be a $2-(9,3,1)$ design. Let $X = \{0,1,2,3,4,5,6,7,8\}$.

$$\mathfrak{B} = \{012, 034, 056, 078, 135, 147, 168, 238, 246, 257, 367, 458\}.$$

Then $\mathcal{D}_0 = (X/\{0\}, \mathfrak{B}_0)$, is a $1-(8,2,1)$ design, where

$$\mathfrak{B}_0 = \{12, 34, 56, 78\}.$$

Next theorem gives a more general result on derived designs.

Theorem 2.10 Let $(X, \mathfrak{B})$ be a $t-(v,k,\lambda)$ design. Let $D \subseteq X, |D| = i < t$. Then $(X/D, \{B/D : D \subseteq B \subseteq \mathfrak{B}\})$ is a $(t-i)$-$(v-i, k-i, \lambda)$ design.

Proof. The proof can be done by using induction on i with the base case proven in the previous theorem.

Example 2.8 It is well known that a $5-(24,8,1)$ design exists (see; [33]). Therefore, from *Theorem 2.10*, there exists a $4-(23,7,1)$ design. There also exist $3-(22,6,1)$ and $2-(21,5,1)$ designs.

Theorem 2.11 Let $(X, \mathfrak{B})$ be a $t-(v,k,\lambda)$ design. Suppose that $P \subseteq X, |P| = p \leq t$. Then there are precisely

$$\lambda_p = \frac{\lambda \binom{v-p}{t-p}}{\binom{k-p}{t-p}}$$

blocks in $\mathfrak{B}$ that contain all points of P.

Proof. Let $\lambda_p(P)$ denote the number of blocks which contains all the points in P. Define a set, say N;

$$N = \{(Y, B) : Y \subseteq X, |Y| = t - p, P \cap Y = \emptyset, B \in \mathfrak{B}, P \cup Y \subseteq B\}.$$

We will compute $|N|$ in two different ways.

Firstly, we can choose a block B in $\lambda_p(P)$ ways such that $P \subseteq B$. For each choice of B, we can choose Y in $\binom{k-p}{t-p}$ ways. Therefore,

$$|N| = \lambda_p(P)\binom{k-p}{t-p}.$$

On the other hand, Y can be chosen in $\binom{v-p}{t-p}$ ways, and for each Y, there are exactly λ blocks B such that $P \cup Y \subseteq B$. Hence,

$$|N| = \lambda\binom{v-p}{t-p}.$$

If we combine these two equations, we have $\lambda_p(P) = \lambda_p$ and $\lambda_p = \frac{\lambda\binom{v-p}{t-p}}{\binom{k-p}{t-p}}$.

Example 2.9 Consider a $5-(24,8,1)$ design. Then we have that $\lambda_0 = 759$, $\lambda_1 = 253$, $\lambda_2 = 77$, $\lambda_3 = 21$, $\lambda_4 = 5$, $and\ \lambda_5 = 1$.

Note that λ_0 indicates the number of blocks, b, in a t-design.

Since λ_p denotes the number of blocks in the p^{th} derived design, λ_p must be an integer. Therefore, this condition is called the necessary condition for the existence of a $t-(v,k,\lambda)$ design.

Theorem 2.12 A $t-(v,k,\lambda)$ design have exactly $b = \lambda\binom{v}{t}/\binom{k}{t}$ blocks.

Proof. Let $(X, \mathfrak{B})$ be a $t-(v,k,\lambda)$ design. Let T denote the t-subsets and B denote the k-subsets of X. We know that $\lambda = |\{B \in \mathfrak{B} : T \subset B\}|$. For any $t-(v,k,\lambda)$ design, if we count the numbers of pairs $(T, B) \in \binom{v}{k} \times \mathfrak{B}$ in two ways; we have $\lambda\binom{v}{t} = |\mathfrak{B}|\binom{k}{t}$.

Example 2.10 Consider a $2-(7,3,1)$ design which is also called the Fano plane. This design has $b = \lambda \binom{v}{t} / \binom{k}{t} = 1 \binom{7}{2} / \binom{3}{2} = 7$ blocks. This design can be shown graphically as in *Figure 1*.

$$X = \{1, 2, 3, 4, 5, 6, 7\},$$

$$\mathfrak{B} = \{123, 145, 167, 246, 257, 347, 356\}.$$

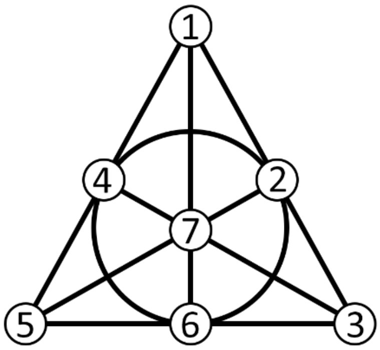


Figure 2. 1 A $2-(7, 3, 1)$ design

Theorem 2.13 [32] Let t, v and k be positive integers such that $t < k < v - t$. There exists a *nontrivial* $t-(v, k, \lambda)$ design for some positive integer λ.

Proof. Let X be a v-set. We consider N-dimensional vector space $\mathbb{Q}^N$ in which the coordinates are indexed by the t-subsets of X where $N = \binom{v}{t}$. We define vectors, say s_A, in $\mathbb{Q}^N$ for each k-subset $A \subseteq X$ in which the entry in the coordinate corresponding to a t-subset $Y \subseteq X$ is equal to 1 if $Y \subseteq A$ and 0 otherwise. Since $t < k < v - t$, there are more of these vectors than the dimension of the space they are in, so, there exists a linear dependence among them. In other words, since we have a set of $\binom{v}{k}$ vectors in a N-dimensional vector space where $N = \binom{v}{t}$, there exist rational numbers α_A $(A \subseteq X, |A| = k)$ such that

$$\sum_{A \subseteq X, |A| = k} \alpha_A s_A = (0, 0, \dots, 0).$$

Let D denote the least common multiple of the denominators of the numbers α_A. Define $\beta_A = D\alpha_A$ for all A. Then we have

$$\sum_{A \subseteq X, |A| = k} \beta_A s_A = (0, 0, \dots, 0).$$

Here, β_A's are all integers. Clearly, at least one of the β_A's is negative. We define $M = min\{\beta_A\}$. Then, $M < 0$. Now, for every $A \subseteq X$, define $\mathfrak{B}$ to be the collection of blocks where, A occurs exactly $\beta_A - M$ times in $\mathfrak{B}$. Since $M = min\{\beta_A\}$, we know that $\beta_A - M \geq 0$ for all A. It is not difficult to see that $(X, \mathfrak{B})$ is a $t - (v, k, \lambda)$ design. We first observe that

$$\sum_{A \subseteq X, |A| = k} s_A = \left(\binom{v-t}{k-t}, \dots, \binom{v-t}{k-t}\right);$$

this follows because, as we already observed, the set of all k-subsets of a v-set is a $t - \left(v, k, \binom{v-t}{k-t}\right)$ design. Now, if we combine above two equations, we have that

$$\sum_{A \subseteq X, |A| = k} (\beta_A - M) s_A = \left(-M\binom{v-t}{k-t}, \dots, -M\binom{v-t}{k-t}\right).$$

This means that every t-set is contained in λ blocks where $\lambda = -M\binom{v-t}{k-t}$. Therefore, $(X, \mathfrak{B})$ is a $t - (v, k, \lambda)$ design with $\lambda = -M\binom{v-t}{k-t}$. Since $(\beta_A - M) = 0$ for at least one A, $(X, \mathfrak{B})$ is nontrivial.

Theorem 2.14 A $1 - (v, k, \lambda)$-design exists if and only if $v\lambda \equiv 0 \ mod \ k$.

Proof. From the *Theorem 2.12*, the number of blocks in a $1 - (v, k, \lambda)$ design is $b = v\lambda/k$. Since b is integer we have $v\lambda \equiv 0 \ mod \ k$. Conversely, suppose that $b = v\lambda/k$ is an integer. We give a method to construct a $1 - (v, k, \lambda)$ design below.

Define $u = \gcd(k, \lambda)$. Then, we have $\lambda = u\lambda'$ and $k = uk'$, where $\gcd(k', \lambda') = 1$. Now, we get $b = {}^{v\lambda}/_{k} = {}^{v\lambda'}/_{k'}$ and $\gcd(k', \lambda') = 1$, so we consider that $v \equiv 0 \ mod \ k'$. Let $v = sk'$, where s is a positive integer. Hence $b = {}^{v\lambda'}/_{k'} = s\lambda'$.

Let X has k' elements. Define $\Upsilon = X \times \mathbb{Z}_s$. Then $|\Upsilon| = v$. Let $A_1, \dots, A_{\lambda'}$ be λ' arbitrary u-subsets of $\mathbb{Z}_s$. For $1 \leq i \leq \lambda'$, define $B_i = X \times A_i$. So, each B_i is a k-subset of Υ. By developing each B_i through $\mathbb{Z}_s$, we have a set of b blocks which contain every point in Υ precisely λ times. Then, we have a $1-(v,k,\lambda)$ design.

Example 2.11 Let the parameters of $1-(v,k,\lambda)$ design be $v=15, k=9$, and $\lambda=6$. Then we have $b=10, s=5, k'=3$, and $\lambda'=2$. Suppose we take $X=\{a,b,c\}$, $A_1=\{1,2,3\}$, and $A_2=\{1,2,4\}$. Then

$$B_1=\{a1,b1,c1,a2,b2,c2,a3,b3,c3\}$$

and

$$B_2=\{a1,b1,c1,a2,b2,c2,a4,b4,c4\}.$$

If we develop the second coordinates of B_1 and B_2 modulo 5 with keeping the first coordinate fixed, we get ten blocks. In the set of ten blocks, each element occurs exactly 6 times. Consequently, we have a $1-(15,9,6)$ design.

2.2 Affine and Projective Planes

In what follows we will call the blocks of a t-design *lines*. If a line contains more than one point, we say that these points are *collinear*. If two lines do not intersect in any point, we say that they are *parallel lines*. Also, if a point p is on the line ℓ, we say ℓ passes through p.

Example 2.12 In *Figure* 2, lines ℓ_1 and ℓ_2 are parallel and points a, b, and c are collinear.

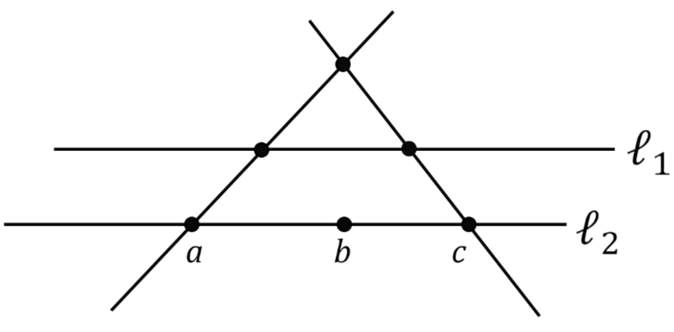


Figure 2. 2 Parallel lines and collinear points

2.2.1 Projective Planes

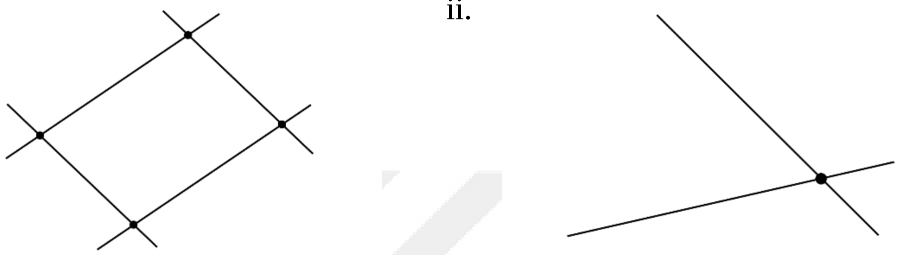
Definition 2.15 A design $(X, \mathfrak{B})$ is called a *projective plane* if the following properties hold.

i. X contains at least one subset of 4 points no 3 of which are collinear,

ii. Each pair of lines intersects in precisely one point, and

iii. Exactly one line passes through any pair of points.

i. ii.



4 points, no 3 of which are collinear. Each pair of lines intersects in one point.

Figure 2. 3 Projective planes

The $2-(7,3,1)$ design is the smallest projective plane which has order 2. It is also known as the *Fano plane*.

Example 2.13 The following pair $(X, \mathfrak{B})$ is a projective plane.

$$X = \{a, b, c, d, e, f, g\},$$

$$\mathfrak{B} = \{abe, acf, adg, bdf, bcg, cde, efg\}.$$

An equivalent definition of a projective plane is given below.

Definition 2.16 A $2-(n^2+n+1, n+1, 1)$ design where $n \geq 2$ is called a *projective plane* of order n.

Example 2.14 A $2-(13,4,1)$ design is a projective plane of order 3.

$$X = \{1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d\},$$

$$\mathfrak{B} = \{123a, 456a, 789a, 147b, 258b, 369b, 159c, 267c, 348c, 168d, 249d, 357d, abcd\}.$$

Theorem 2.17 There exist a projective plane of order q for every prime power $q \geq 2$.

Proof. Let V be a 3-dimensional vector space over the field $\mathcal{F}_q$. Let V_1 be the set of 1-dimensional subspaces of V, and let V_2 be the set of 2-dimensional subspaces of V. Let $X = V_1$. For each $B \in V_2$, define a block $A_B = \{c \in V_1 \mid c \subseteq B\}$, and let $\mathfrak{B} = \{A_B : B \in V_2\}$. Then, $(X, \mathfrak{B})$ is a projective plane of order q.

2.2.2 Affine Planes

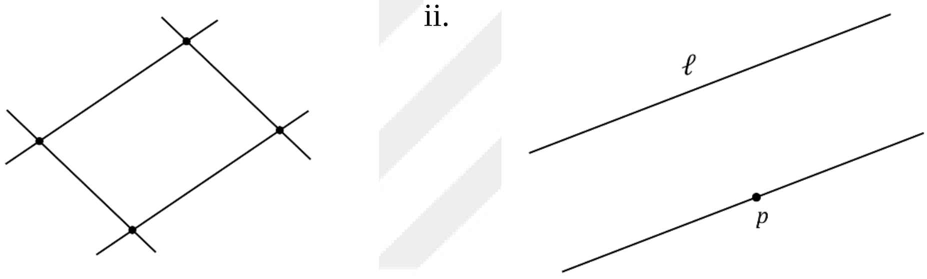
Definition 2.18 A design $(X, \mathfrak{B})$ is called an *affine plane* if the following properties hold.

i. X contains at least one subset of 4 points no 3 of which are collinear,

ii. Given a line ℓ and a point p not on ℓ, there is exactly one line of $\mathfrak{B}$ containing p which is parallel to ℓ, and

iii. Exactly one line passes through any pair of points.

i. ii.



4 points, no 3 of which are collinear. There is exactly one line through p parallel to ℓ

Figure 2. 4 Affine planes

Note. The first condition of the definition guarantees that this plane does not consist of a single line.

Example 2.15 The following pair $(X, \mathfrak{B})$ is an affine plane.

$$X = \{a, b, c, d\},$$

$$\mathfrak{B} = \{ab, ac, ad, cd, bd, bc\}.$$

An equivalent definition of an affine plane is given below.

Definition 2.19 A $2-(n^2, n, 1)$ design where $n \geq 2$ is called an *affine plane* of order n.

Example 2.16 A $2-(9,3,1)$ design is an affine plane of order 3.

$$X = \{1,2,3,4,5,6,7,8,9\},$$

$$\mathfrak{B} = \{123, 456, 789, 147, 258, 369, 168, 249, 357, 159, 267, 348\}.$$

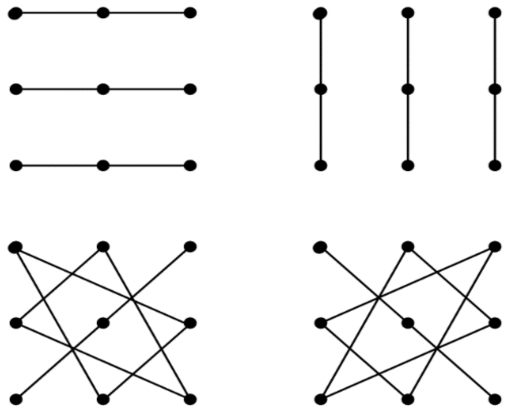


Figure 2. 5 Affine plane of order 3

Theorem 2.20 [32] There exist an affine plane of order q for every prime power $q \geq 2$.

Proof. We first define $P = \mathcal{F}_q \times \mathcal{F}_q$ for any prime q. Then, for any $a, b \in \mathcal{F}_q$, we define a block

$$B_{a,b} = \{(x, y) \in P : y = ax + b\}.$$

For any $c \in \mathcal{F}_q$, define

$$B_{\infty,c} = \{(c, y) : y \in \mathcal{F}_q\}.$$

We now define

$$\mathfrak{B} = \{B_{a,b} : a, b \in \mathcal{F}_q\} \cup \{B_{\infty,c} : c \in \mathcal{F}_q\}.$$

We will show that $(P, \mathfrak{B})$ is a $2 - (q^2, q, 1)$ design (i.e., an affine plane of order q).

Since $P = \mathcal{F}_q \times \mathcal{F}_q$, there are q^2 points in P. It is easy to see that each block contains q points. So, we need to show that each pair of distinct points is contained in exactly one block. Let $(x_1, y_1), (x_2, y_2) \in P$. We have two cases:

1. If $x_1 = x_2$, the pair $\{(x_1, y_1), (x_2, y_2)\}$ is contained in the unique block B_{∞,x_1}.
2. If $x_1 \neq x_2$, we consider the system of equations in $\mathcal{F}_q$:

$$y_1 = ax_1 + b, \tag{2.1}$$

$$y_2 = ax_2 + b. \tag{2.2}$$

We need to show that Equations (2.1) and (2.2) have a unique solution for a and b. If we subtract the second equation from the first one, we have

$$y_1 - y_2 = a(x_1 - x_2). \tag{2.3}$$

We assumed that $x_1 \neq x_2$, so $(x_1 - x_2)$ has a unique multiplicative inverse in $\mathcal{F}_q$, i.e. $(x_1 - x_2)^{-1} \in \mathcal{F}_q$. If we multiply both sides of the previous equation by $(x_1 - x_2)^{-1}$, we get

$$a = (x_1 - x_2)^{-1}(y_1 - y_2).$$

We can substitute a with $(x_1 - x_2)^{-1}(y_1 - y_2)$ in Equation (2.1). Then we obtain

$$y_1 = ax_1 + b = (x_1 - x_2)^{-1}(y_1 - y_2)x_1 + b.$$

From the above equation, we have

$$b = y_1 - (x_1 - x_2)^{-1}(y_1 - y_2)x_1.$$

Hence, $B_{a,b}$ is the unique block that contains the pair $\{(x_1, y_1), (x_2, y_2)\}$.

Consequently, $(P, \mathfrak{B})$ is an affine plane (i.e. a $2 - (q^2, q, 1)$ design).

Example 2.17 We will construct an affine plane of order 3 by using the *Theorem 2.20*.

Let $P = \mathbb{Z}_3 \times \mathbb{Z}_3$. We construct blocks as follows:

$$B_{0,0} = \{(0,0), (1,0), (2,0)\} \qquad B_{2,0} = \{(0,0), (1,2), (2,1)\}$$

$$B_{0,1} = \{(0,1), (1,1), (2,1)\} \qquad B_{2,1} = \{(0,1), (1,0), (2,2)\}$$

$$B_{0,2} = \{(0,2), (1,2), (2,2)\} \qquad B_{2,2} = \{(0,2), (1,1), (2,0)\}$$

$$B_{1,0} = \{(0,0), (1,1), (2,2)\} \qquad B_{\infty,0} = \{(0,0), (0,1), (0,2)\}$$

$$B_{1,1} = \{(0,1), (1,2), (2,0)\} \qquad B_{\infty,1} = \{(1,0), (1,1), (1,2)\}$$

$$B_{1,2} = \{(0,2), (1,0), (2,1)\} \qquad B_{\infty,2} = \{(2,0), (2,1), (2,2)\}.$$

So, $(P, \mathfrak{B})$ is an affine plane of order 3.

Theorem 2.21 Residual of a projective plane of order n is an affine plane of order n.

Proof. Let $\mathcal{D} = (X, \mathfrak{B})$ be a $2-(n^2+n+1, n+1, 1)$ design, i.e. a projective plane of order n, if we consider the residual design on $n+1$ points of this projective plane, we obtain a $2-(n^2, n, 1)$ design, i.e. an affine plane of order n.

2.2.3 Connection Between Affine and Projective Planes

Two designs $\mathcal{D}_1 = (X_1, \mathfrak{B}_1)$ and $\mathcal{D}_2 = (X_2, \mathfrak{B}_2)$ are called block-disjoint if $\mathfrak{B}_1 \cap \mathfrak{B}_2 = \emptyset$. Let $\mathcal{D} = (X, \mathfrak{B})$ be a $\mu - (v, k, \lambda)$ design, and $R = \{(X, \mathfrak{B}_i)\}_{i=1}^{n}$ be a collection of disjoint $t-(v, k, \lambda')$ designs such that $\mathfrak{B} = \bigcup_{i=1}^{n} \mathfrak{B}_i$ we then say that R is a t-resolution of D. A 1-resolvable design is just called a resolvable design.

Example 2.18 Blocks of a resolvable $2-(8,4,3)$ design is given below for the point set $X = \{0,1,2,3,4,5,6,7\}$.

$$\{0,2,3,5\}, \quad \{1,4,6,7\},$$

$$\{0,3,4,6\}, \quad \{2,5,7,1\},$$

$$\{0,4,5,7\}, \quad \{3,6,1,2\},$$

$$\{0,5,6,1\}, \quad \{4,7,2,3\},$$

$$\{0,6,7,2\}, \quad \{5,1,3,4\},$$

$$\{0,7,1,3\}, \quad \{6,2,4,5\},$$

$$\{0,1,2,4\}, \quad \{7,3,5,6\}.$$

Definition 2.22 In a design $(X, \mathfrak{B})$, a set of mutually parallel lines, i.e. a set of disjoint blocks, which partition the points of X is called a *parallel class*.

Example 2.19 Parallel classes of $2-(8,4,3)$ design which is given in *Example 2.18*, are listed below.

$\pi_1 = \{0235, 1467\}$, $\quad \pi_2 = \{0346, 2571\}$, $\quad \pi_3 = \{0457, 3612\}$,

$\pi_4 = \{0561, 4723\}$, $\quad \pi_5 = \{0672, 5134\}$, $\quad \pi_6 = \{0713, 6245\}$,

$\pi_7 = \{0124, 7356\}$.

Example 2.20 In *Example 2.16*, there are 4 parallel classes. These parallel classes of $2-(9,3,1)$ design are given below.

$\pi_1 = \{123, 456, 789\}$, $\pi_2 = \{147, 258, 369\}$,

$\pi_3 = \{159, 267, 348\}$, $\pi_4 = \{168, 249, 357\}$.

These parallel classes form a 1-resolution of a $2-(9,3,1)$ design. It is easy to say that $v \equiv 0\ (mod\ k)$ is the existence condition of a resolvable $t-(v,k,\lambda)$ design.

Theorem 2.23 A resolvable $2-(v,2,1)$ design exists if and only if v is an even integer and $v \geq 4$.

Proof. It is clear that v must be an even integer and $v \geq 4$ since $v \equiv 0\ (mod\ 2)$ in a resolvable $2-(v,2,1)$. To complete the proof, we now give a construction for such v. Let the point set X be $\mathbb{Z}_{v-1} \cup \{\infty\}$. For any $j \in \mathbb{Z}_{v-1}$, we define the parallel classes as follows:

$$\pi_j = \{\{\infty, j\}\} \cup \{\{i + j\ mod\ (v-1), j - i\ mod\ (v-1)\} : 1 \leq i \leq (v-2)/2\}.$$

Any pair of points occurs in precisely one parallel class. Therefore, we have a resolvable $2-(v,2,1)$ design.

Example 2.21 A resolvable $2-(6,2,1)$ design is given with the following parallel classes.

$\pi_0 = \{\infty 0, 14, 23\}$, $\pi_1 = \{\infty 1, 20, 34\}$, $\pi_2 = \{\infty 2, 31, 40\}$,

$\pi_3 = \{\infty 3, 42, 01\}$, $\pi_4 = \{\infty 4, 03, 12\}$.

Remark. Affine planes are resolvable.

Theorem 2.24 There exists a projective plane of order n if and only if there exists an affine plane of order n.

Proof. From the *Theorem 2.21*, the residual design of a projective plane of order n is an affine plane of order n. Conversely, for a given affine plane of order n, we will show how to construct a projective plane of order n from the affine plane of order n. Let $\mathcal{A} = (X, \mathfrak{B})$ be an affine plane of order n. Since affine planes are resolvable, we can define its parallel classes. Let $\pi_1, \pi_2, \ldots, \pi_{n+1}$ be the $n+1$ parallel classes of $\mathcal{A}$. Let $\infty_1, \infty_2, \ldots, \infty_{n+1} \notin X$, define $\Omega = \{\infty_1, \infty_2, \ldots, \infty_{n+1}\}$, and define the point set X' as the union of X and Ω; that is, $X' = X \cup \Omega$. For each $B \in \mathfrak{B}$, define $B' = B \cup \{\infty_i\}$ where $B \in \pi_i$. In other words, we add the point ∞_i to each block in the ith parallel class where $1 \leq i \leq n+1$. Now, define $\mathfrak{B}' = \{B' : B \in \mathfrak{B}\} \cup \{\Omega\}$. We need to show that $(X', \mathfrak{B}')$ is a projective plane of order n. There are n^2 points in an affine plane of order n and $n+1$ points in Ω, then there are total n^2+n+1 points, and each block contains $n+1$ points. Therefore, we only need to show that each pair of points $x, y \in X'$ $(x \neq y)$ is contained in a unique block. If $x, y \in X$, then x and y are contained in a unique block $B \in \mathfrak{B}$, and hence x and y are contained in a unique block in $\mathfrak{B}'$. If $x \in X$ and $y \in \Omega$, say $y = \infty_i$. Then, $\{x, y\} \subseteq B'$ where B is the unique block in π_i which contains x. Finally, if $x = \infty_i$ and $y = \infty_j$, then $\{x, y\} \subseteq \Omega$.

Example 2.22 We will construct a projective plane of order 3 from an affine plane of order 3 by using the technique given in the proof of *Theorem 2.24*. We consider the affine plane of order 3 constructed in *Example 2.17*.

$$B'_{0,0} = \{(0,0),(1,0),(2,0),\infty_0\} \qquad B'_{2,0} = \{(0,0),(1,2),(2,1),\infty_2\}$$

$$B'_{0,1} = \{(0,1),(1,1),(2,1),\infty_0\} \qquad B'_{2,1} = \{(0,1),(1,0),(2,2),\infty_2\}$$

$$B'_{0,2} = \{(0,2),(1,2),(2,2),\infty_0\} \qquad B'_{2,2} = \{(0,2),(1,1),(2,0),\infty_2\}$$

$$B'_{1,0} = \{(0,0),(1,1),(2,2),\infty_1\} \qquad B'_{\infty,0} = \{(0,0),(0,1),(0,2),\infty_3\}$$

$$B'_{1,1} = \{(0,1),(1,2),(2,0),\infty_1\} \qquad B'_{\infty,1} = \{(1,0),(1,1),(1,2),\infty_3\}$$

$$B'_{1,2} = \{(0,2),(1,0),(2,1),\infty_1\} \qquad B'_{\infty,2} = \{(2,0),(2,1),(2,2),\infty_3\}$$

$$\Pi = \{\infty_0, \infty_1, \infty_2, \infty_3\}.$$

2.3 Some Constructions

Until 1983, for $t > 5$, there had not been found any simple t-design. The most common thought was that any simple 6-designs would not exist. In 1983, Magliveras and Leavitt [34] constructed a $6-(33,8,36)$ design which is the first simple 6-design. In the following years, Tierlinck [4] showed that for any t, there exists a simple t-design. In 2014, one of the oldest problems in t-designs is proved by Peter Keevash [8]. He proved the existence of t-designs with the parameters $\lambda = 1$ and $t \geq 2$.

We now give some constructions for t-designs with $\lambda = 1, k = 3$ and $t = 2$. Firstly, we give the definition of Latin squares and quasi groups.

Consider an $n \times n$ array in which each cell of this array contains only one element of the set $X = \{1, 2, \dots, n\}$. If each element of X occurs only once in each column and in each row of the array, then this array called a *Latin square* of order n. We now consider a set $\mathfrak{Q}$ which consist of n elements. $\mathfrak{Q}$ forms a group under " $\circ$ " operation with the following condition.

(i) For any two elements a, b of $\mathfrak{Q}$, the equations $a \circ x = b$ and $y \circ a = b$ have unique solutions.

The pair $(\mathfrak{Q}, \circ)$ is called *Quasigroup* of order n. The similarity between Latin squares and quasigroups can be seen in the next example.

Example 2.23 *(Latin squares and quasigroups)*

(i)

1	2
2	1

a Latin square of order 2

$\circ$	1	2
1	1	2
2	2	1

a quasigroup of order 2

(ii)

1	2	3
3	1	2
2	3	1

a Latin square of order 3

$\circ$	1	2	3
1	1	2	3
2	3	1	2
3	2	3	1

a quasigroup of order 3

A Latin square(quasigroup) is called *commutative* if the cell (i, j) and the cell (j, i) contain the same element for all $1 \leq i, j \leq n$. A latin square is called *idempotent* if the cell (i, i) contain the symbol i for all $1 \leq i \leq n$. A Latin square is called *half-idempotent* of order $2n$ if cells (i, i) and $(n + i, n + i)$ contain the symbol i for $1 \leq i \leq n$.

Example 2.24 *(Commutative, idempotent and half-idempotent Latin squares)*

1	3	2
3	2	1
2	1	3

idempotent and commutative

1	2
2	1

half-idempotent and commutative

1	4	2	5	3
4	2	5	3	1
2	5	3	1	4
5	3	1	4	2
3	1	4	2	5

idempotent and commutative

1	3	2	4
3	2	4	1
2	4	1	3
4	1	3	2

half-idempotent and commutative

The Bose Construction. Let $(\mathfrak{Q}, \circ)$ be an idempotent commutative quasigroup of order $2n + 1$ with $\mathfrak{Q} = \{1, 2, \ldots, 2n + 1\}$ and $X = \mathfrak{Q} \times \mathbb{Z}_3$. Let $\mathfrak{B}$ consist of following types of blocks:

(i) $\{x_0, x_1, x_2\}, x \in \mathfrak{Q}$

(ii) $\{x_i, x_i, (x \circ y)_{i+1}\}, x, y \in \mathfrak{Q}, x \neq y, i \in \mathbb{Z}_3$.

Then $(X, \mathfrak{B})$ forms a $2 - (6n + 3, 3, 1)$ design.

Proof. Firstly, there are $|X| = |\mathfrak{Q}| \times |\mathbb{Z}_3| = (2n + 1)(3) = 6n + 3$. There are $2n + 1$ blocks in (i). For (ii), we can choose x and y in $\binom{2n+1}{2}$ ways and there are 3 blocks for each for each such choice. Therefore, $|\mathfrak{B}| = 2n + 1 + 3\binom{2n+1}{2} = (2n+1)(3n+1)$ which is equal to number of blocks in a $2-(6n+3,3,1)$ design. We now need to show that any pair of two distinct points is contained in one blocks of $\mathfrak{B}$. Let a_j, b_k be the two distinct points in X. If $a = b$ then $\{a_1, a_2, a_3\}$ is the unique block in (i) which contains a_j and b_k. If $j = k$, then $a \neq b$ and moreover $\{a_j, b_j, (a \circ b)_{j+1}\}$ is the unique block in (ii) that contains a_j and b_k. Lastly, let $a \neq b$ and $j \neq k$. Suppose without loss of generality $j = 1$ and $k = 2$. As $(\mathfrak{Q},\circ)$ is quasi group, there exist $p \in \mathfrak{Q}$ such that $a \circ p = b$. As $(\mathfrak{Q},\circ)$ is idempotent and $a \neq b$, then $p \neq a$. Hence, $\{a_1, p_1, (a \circ p)_2 = b_2\}$ is the unique block in (ii) that contains a_1 and b_2. Consequently, $(X, \mathfrak{B})$ forms a $2-(6n+3,3,1)$ design.

Example 2.25 We will construct a $2-(9,3,1)$ design with using the Bose construction. We will use an idempotent commutative quasigroup of order $|X|/3 = 3$. We can use the idempotent commutative quasigroup of order 3 given in the *Example 2.24*.

Let $X = \{1,2,3\} \times \{1,2,3\}$. Then $\mathfrak{B}$ consist of following blocks.

(i) $\{(1,1),(1,2),(1,3)\}, \{(2,1),(2,2),(2,3)\}, \{(3,1),(3,2),(3,3)\}$,

(ii) $i = 1, j = 2$: $\{(1,1),(2,1),(3,2)\}, \{(1,2),(2,2),(3,3)\}, \{(1,3),(2,3),(3,1)\}$,

$i = 1, j = 3$: $\{(1,1),(3,1),(2,2)\}, \{(1,2),(3,2),(2,3)\}, \{(1,3),(3,3),(2,1)\}$,

$i = 2, j = 3$: $\{(2,1),(3,1),(1,2)\}, \{(2,2),(3,2),(1,3)\}, \{(2,3),(3,3),(1,1)\}$.

The Skolem Construction. Let $(\mathfrak{Q},\circ)$ be a half-idempotent commutative quasigroup of order $2n$ with $\mathfrak{Q} = \{1,2,\dots,2n\}$ and $X = \{\infty\} \cup (\mathfrak{Q} \times \mathbb{Z}_3)$. Let $\mathfrak{B}$ consist of following types of blocks:

(i) $\{x_0, x_1, x_2\}$, $1 \leq x \leq n$,

(ii) $\{\infty, (n+x)_i, x_{i+1}\}$, $1 \leq x \leq n$, $i \in \mathbb{Z}_3$,

(iii) $\{x_i, y_i, (x \circ y)_{i+1}\}$, $x, y \in \mathfrak{Q}$, $x \neq y$, $i \in \mathbb{Z}_3$.

Then $(X, \mathfrak{B})$ forms a $2-(6n+1,3,1)$ design.

Proof. The proof is similar to Bose construction's proof.

Example 2.26 We will construct a $2-(7,3,1)$ design with using the Skolem construction. We will use a half-idempotent commutative quasigroup of order $(|X|-1)/3 = 2$. We can use the half-idempotent commutative quasigroup of order 2 given in the *Example 2.24*.

Let $X = \{\infty\} \cup (\{1,2\} \times \{1,2,3\})$. Then $\mathfrak{B}$ consist of following blocks.

(i) $\{(1,1),(1,2),(1,3)\}$,

(ii) $\{\infty,(2,1),(1,2)\},\{\infty,(2,2),(1,3)\},\{\infty,(2,3),(1,1)\}$, and

(iii) $\{(1,1),(2,1),(2,2)\},\{(1,2),(2,2),(2,3)\},\{(1,3),(2,3),(2,1)\}$.

2.4 Steiner Systems

Definition 2.25 A *Steiner system* is a pair $(X,\mathfrak{B})$ in which every t-subset of X is contained in exactly one block in $\mathfrak{B}$.

Steiner systems are special types of $t-(v,k,\lambda)$ designs where $\lambda=1$ and $t\geq 2$. Steiner systems are denoted as $S(t,k,v)$. The most studied and well known Steiner systems are those with $t=2$ and $k=3$. These systems are called *Steiner triple systems* and abbreviated as STS. A STS of order v, denoted as $STS(v)$, is a $2-(v,3,1)$ design. If $t=3$ and $k=4$ in an $S(t,k,v)$, then these systems are called *Steiner quadruple systems* and abbreviated as SQS.

2.4.1 Existence of Steiner Systems

One of the oldest problems in combinatorial design theory which was asked by Jakob Steiner in 1853 was if any nontrivial Steiner system have $t\geq 6$. Until 2014, this problem has been studied by many authors [see; 4, 5, 6, 7]. *Peter Keevash* [8] published a paper on existence of Steiner systems in 2014, and proved the existence of such designs.

Lemma 2.26 (Divisibility Conditions) A Steiner System $S(t,k,v)$ exists only if for every $i\in\{0,1,2,\dots,t-1\}$, $\binom{v-i}{t-i}/\binom{k-i}{t-i}$ is an integer.

Proof. This theorem can be proven with using the same argument proven in *Theorem 2.11* for $\lambda=1$.

Some of the well-known infinite families of Steiner Systems are affine geometries, projective geometries, and spherical geometries. For every prime power q and $n\geq 2$; affine geometries, projective geometries and spherical geometries are $S(2,q,q^n)$, $S(2,q+1,q^n+\cdots+q+1)$, $S(3,q+1,q^n+1)$, respectively.

We now continue with Steiner systems with block size 3, specifically called *Steiner triple systems*.

2.4.2 Steiner Triple Systems

Definition 2.27 A *Steiner triple system* is a design $(X, \mathfrak{B})$, where X is finite set of v points and $\mathfrak{B}$ is a set of 3-element subsets of X, called *triples*, such that each pair of distinct points of X contained in exactly one triple of $\mathfrak{B}$.

Remark. A Steiner triple system of order v is a $2-(v,3,1)$ design.

Example 2.27 The following designs are $S(2,3,3)$, $S(2,3,7)$ and $S(2,3,13)$, respectively.

(i) $X = \{1,2,3\}$, $\mathfrak{B} = \{123\}$,

(ii) $X = \{1,2,3,4,5,6,7\}, \mathfrak{B} = \{124, 235, 346, 457, 561, 672, 713\}$,

(iii) $X = \{1,2,3,4,5,6,7,8,9,0,a,b,c\}$,

$$\mathfrak{B} = \begin{Bmatrix} 012, 034, 056, 078, 09a, 0bc, 135, 147, 168, 19b, 1ac, 239, 245, \\ 26a, 27c, 28b, 36b, 37a, 38c, 46c, 489, 4ab, 57b, 58a, 59c, 679 \end{Bmatrix}.$$

In part (ii) of *Example 2.27*, the Steiner triple system with order 7 can be shown graphically by taking the straight triangle joining $1, 2, 4$ and rotating it once gives another block, $2, 3, 5$ which is the dotted triangle in the *Figure 6*. If we continue this rotation process through 5 times, we obtain all blocks of $\mathfrak{B}$.

Figure 2. 6 Steiner triple system of order 7

Theorem 2.28 A *Steiner triple system*, $STS(v)$, exists if and only if $v \equiv 1, 3 \ (mod\ 6)$.

Proof. Suppose that $STS(v)$ exist. From the *Lemma 2.26 (Divisibility Conditions)*, we know that $\binom{v-i}{t-i} / \binom{k-i}{t-i}$ is an integer for all $i = 0, 1, 2, \dots, t-1$. In a Steiner triple system, we know that $k = 3 \ and \ t = 2$. Therefore, we have,

$$\binom{v-i}{2-i} \bigg/ \binom{3-i}{2-i} \ \ for \ i = 0,1.$$

Hence, for $i = 0$, $\binom{v}{2}/\binom{3}{2} = v(v-1)/3$ and for $i = 1$, $\binom{v-1}{1}/\binom{2}{1} = (v-1)/2$ are integers. Since $(v-1)/2$ is an integer, $v-1$ is even and hence v is odd. Since $v(v-1)/3$ is an integer and v is odd, we get $v \equiv 1\ (mod\ 6)$ or $v \equiv 3\ (mod\ 6)$. To complete proof, we refer the constructions of the $STS(v)$ where v has the form $6n+1$ or $6n+3$. The case when $n = 0$ and $v = 6n+1$, we obtain $v = 1$. In this situation, there is no triple. Therefore, we consider remaining cases. Indeed, in 1847, Kirkman [1] showed that the remaining cases can be constructed. For $v = 6n+1$, see the Skolem construction and for $v = 6n+3$, see the Bose construction given in the *Section 2.3*.

2.4.3 Steiner Quadruple Systems

Definition 2.29 A *Steiner quadruple system* of order v, denoted as $SQS(v)$, is a $3-(v,4,1)$ design.

Example 2.28 Steiner quadruple system of order 8, $S(3,4,8)$;

$$X = \{1,2,3,4,5,6,7,8\}$$

$$\mathfrak{B} = \begin{Bmatrix} 1248, 2358, 3468, 4578, 1568, 2678, 1378, \\ 3567, 1467, 1257, 1236, 2347, 1345, 2456 \end{Bmatrix}.$$

In 1960, H. Hanani [36] determined the necessary conditions for the existence of Steiner quadruple systems.

Theorem 2.30 [36] Steiner quadruple system exist if and only if $v \equiv 2, 4\ (mod\ 6)$.

Theorem 2.31 [37] Every Steiner triple system of order v, where $v \leq 15$, is the derived design of some Steiner quadruple system of order $v+1$.

Most of the known Steiner quadruple systems are derived from 5-designs.

2.5 Large Sets of t-Designs

Definition 2.32 A $t-(v,k,\lambda)$ design is called *complete* if it contains all $\binom{v}{k}$ blocks.

Definition 2.33 A large set $LS[N](t,k,v)$ or $LS_\lambda(t,k,v)$ of $t-(v,k,\lambda)$ designs is a pair $\mathcal{L} = (X, \mathbb{B})$ where $\mathbb{B} = \{\mathfrak{B}_i\}_{i=1}^{N}$ is a partition of all k-subsets of X and each pair $(X, \mathfrak{B}_i)$ is a simple $t-(v,k,\lambda)$ design.

In other words, a large set of t-designs is a t-resolution of the complete design. The number N in the definition of large set which indicates the number of disjoint $t-(v,k,\lambda)$ designs is equal to $N = \binom{v-t}{k-t}/\lambda$. Therefore N is an integer. This condition is necessary condition for the existence of large sets. For a Steiner triple system, it is known that $t = 2$ and $k = 3$. Therefore, if there exists a large set of disjoint Steiner triple systems, N must be $v - 2$. Large set of $STS(v)$ is denoted by $LSTS(v)$. Same argument can be used to show that set of $v - 3$ disjoint Steiner quadruple systems form a large set of Steiner quadruple systems.

Note. Notations $LS[N](t, k, v)$ and $LS_\lambda(t, k, v)$ can be used interchangeable, since N depends on λ.

Example 2.29 Large set of 2-(6,3,2) designs, $LS[2](2,3,6) = (X; \mathfrak{B}_1, \mathfrak{B}_2)$, is given below for the point set $X = \{1, 2, 3, 4, 5, 6\}$.

$$\mathfrak{B}_1 = \{123, 124, 135, 146, 156, 236, 245, 256, 345, 346\}$$

$$\mathfrak{B}_2 = \{125, 126, 134, 136, 145, 234, 235, 246, 356, 456\}.$$

The necessary condition is not always sufficient condition. In 1850, Cayley [38] showed that there are only two disjoint $2 - (7,3,1)$ designs. Therefore, there does not exist $LS(2,3,7)$, although $N = 5$ is an integer for $2 - (7,3,1)$ designs. In the same year, Kirkman showed the existence of an $LSTS(9)$. This design is first nontrivial $LSTS$.

We now give some theorems without proofs, for detailed proofs readers are referred to Tierlinck's papers [4, 39].

Theorem 2.34 [4] For all positive integers N and t, there is an integer v such that an $LS[N](t, t + 1, v)$ exists.

Theorem 2.35 [39] There is a large set of Steiner triple systems of order v where $v \equiv 1, 3\ (mod 6)$ and $v > 7$.

2.6 Automorphisms of Designs

Definition 2.36 Let $(X, \mathfrak{B})$ and $(X', \mathfrak{B}')$ be two $t - (v, k, \lambda)$ designs and let $|X| = |X'|$. $(X, \mathfrak{B})$ and $(X, \mathfrak{B}')$ are called *isomorphic* if there exists a bijection $\varphi : X \to X'$ such that $\mathfrak{B}' = [\{\varphi(x) : x \in B\} : B \in \mathfrak{B}]$.

Example 2.30 The following two pairs $(X, \mathfrak{B})$ and $(X', \mathfrak{B}')$ of $2 - (9,3,1)$ designs are isomorphic if we define a bijection φ as $\varphi(0) = a, \varphi(1) = d, \varphi(2) = h$, $\varphi(3) = c, \varphi(4) = e, \varphi(5) = g, \varphi(6) = k, \varphi(7) = b$ and $\varphi(8) = f$.

$$X = \{0, 1, 2, 3, 4, 5, 6, 7, 8\},$$

$$\mathfrak{B} = \{012, 034, 056, 078, 135, 147, 168, 238, 246, 257, 367, 458\};$$

$$X' = \{a, b, c, d, e, f, g, h, k\},$$

$$\mathfrak{B}' = \{\text{abf}, \text{ace}, \text{adh}, \text{agk}, \text{bck}, \text{bde}, \text{bhg}, \text{chf}, \text{cdg}, \text{dkf}, \text{efg}, \text{ehk}\}.$$

Example 2.31 Let $X = \{1,2,3,4,5,6,7\}$ and $\mathfrak{B} = \{123, 145, 167, 246, 257, 347, 356\}$. Define $\varphi: X \to X$ as $\varphi = (1)(2)(3\ 4)(5\ 6\ 7) \in S_7$. Then $(X, \mathfrak{B})$ and $(X, \mathfrak{B}')$ are isomorphic.

$\mathfrak{B}$	=	{	123,	145,	167,	246,	257,	347,	356	}
			↓	↓	↓	↓	↓	↓	↓	
$\mathfrak{B}'$	=	{	124,	136,	157,	237,	256,	345,	467	}

Definition 2.37 An *automorphism* of a design is an isomorphism of this design with itself.

Example 2.32 Let $X = \{1,2,3,4,5,6,7\}$ and $\mathfrak{B} = \{123, 145, 167, 246, 257, 347, 356\}$. Define $\varphi: X \to X$ as $\varphi = (1)(2)(3)(4\ 5)(6\ 7) \in S_7$.

123	145	167	246	257	347	356
↓	↓	↓	↓	↓	↓	↓
123	145	167	257	246	356	347

Thus, φ is an automorphism of $(X, \mathfrak{B})$.

Note. An automorphism relabels the points of design.

The set of all automorphisms of a design $(X, \mathfrak{B})$ forms a group under the operation of composition of permutations. This group is called the automorphism group of $(X, \mathfrak{B})$. Automorphism group of $(X, \mathfrak{B})$ is denoted by $Aut(X, \mathfrak{B})$.

Definition 2.38 A permutation $\varphi \in S_v$ is called an *automorphism* of a large set $\mathcal{L} = (X, \mathbb{B})$ where $\mathbb{B} = \{\mathfrak{B}_i\}_{i=1}^{N}$, if $\varphi(\mathfrak{B}_i) = \mathfrak{B}_j$ for any $1 \leq i, j \leq N$.

A group $\mathcal{g}$ is called automorphism group of $\mathcal{L}$, if $\varphi(\mathbb{B}) = \mathbb{B}$ holds for all $\varphi \in \mathcal{g}$, that is, if $\varphi(\mathfrak{B}_i) \in \mathbb{B}$ for all $\mathfrak{B}_i \in \mathbb{B}$ and $\varphi \in \mathcal{g}$. A large set with this property is called

$\mathcal{g}$-invariant. If $\varphi(\mathfrak{B}_i) = \mathfrak{B}_i$ holds for all $\mathfrak{B}_i \in \mathbb{B}$ and $\varphi \in \mathcal{g}$, then we say that $\mathcal{L}$ is $[\mathcal{g}]$-invariant.

Definition 2.39 Let G be a group and X be a set. Suppose that $\varphi : G \times X \to X$ satisfies the following conditions. Then φ is called a *group action*.

i. $\varphi(e, x) = x$ for all $x \in X$ and e is the identity element of G,

ii. $\varphi(g, \varphi(h, x)) = \varphi(gh, x)$ for all $x \in X$ and $g, h \in G$.

The group G is said to act on X and this action is denoted by $G|X$. The set X is called a G-set. G permutes the elements of X. If G acts on X, then G also acts on $\binom{X}{t}$ for every t, $2 \le t \le |X|$. The orbit of G, with its automorphism group $\mathcal{g}$, is $\mathcal{g}(G) = \{\varphi(G) : \varphi \in \mathcal{g}\}$. A group action is said to be *transitive* if the set X consists of a single G-orbit. A t-orbit is an orbit of G in its induced action on $\binom{X}{t}$.

Example 2.33 Let $G = \mathbb{Z}_7$ and $X = \mathbb{Z}_7$. G acts on X with the action $\varphi = (0\ 1\ 2\ 3\ 4\ 5\ 6)$. G also acts on $\binom{X}{2}$. Let the set of $2 - orbits$ be denoted as $\Delta = \{\Delta_1, \Delta_2, \Delta_3\}$. Its $2 - orbits$ are listed below.

$$\Delta_1 = \{01, 12, 23, 34, 45, 56, 06\},$$

$$\Delta_2 = \{02, 13, 24, 35, 46, 50, 61\},$$

$$\Delta_3 = \{03, 14, 25, 36, 40, 51, 62\}.$$

The group G also acts on $\binom{X}{3}$. Let the set of $3 - orbits$ be denoted as $\Gamma = \{\Gamma_1, \Gamma_2, \Gamma_3, \Gamma_4, \Gamma_5\}$. Its $3 - orbits$ are listed below.

$$\Gamma_1 = \{012, 123, 234, 345, 456, 560, 601\},$$

$$\Gamma_2 = \{013, 124, 235, 346, 450, 561, 602\},$$

$$\Gamma_3 = \{014, 123, 236, 340, 431, 562, 603\},$$

$$\Gamma_4 = \{015, 126, 230, 341, 452, 563, 604\},$$

$$\Gamma_5 = \{024, 135, 246, 350, 461, 502, 613\}.$$

We now define a matrix $A_{k,t}$ which is called as *Kramer-Mesner matrix*. The matrix $A_{k,t}$ is an $n \times m$ matrix, where n is equal to the number of $k - orbits$ and m is equal to the number of $t - orbits$ of group G. Let Δ denotes the set of $t - orbits$ and Γ denotes the set of $k-orbits$. For $1 \leq j \leq m$, choose any $t-subset$ $\partial_j \in \Delta$. Then, for $1 \leq i \leq n$, the i, j entry of $A_{k,t}$, denoted a_{ij}, is defined as follows:

$$a_{ij} = \left|\left\{A \in \Gamma_i : \partial_j \subseteq A\right\}\right|.$$

Example 2.34 We will construct the Kramer-Mesner matrix $A_{3,2}$ with using the previous example.

$$A_{3,2} = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 2 \\ 1 & 1 & 1 \\ 0 & 2 & 1 \end{pmatrix}.$$

Next theorem provides a simpler way to construct t-designs with specified automorphism.

Theorem 2.40 (Kramer-Mesner Theorem) There exists a $t-(v, k, \lambda)$ design having $\mathcal{g}$ as a subgroup of its automorphism group if and only if there exists a solution $\boldsymbol{z} \in \mathbb{Z}^n$ to the matrix equation

$$\boldsymbol{z} \cdot A_{k,t} = \lambda \boldsymbol{u}_m,$$

where $\boldsymbol{z}$ has nonnegative entries and $\boldsymbol{u}_m$ is the m-dimensional vector which all entries are 1.

Example 2.35 We will construct a 2-(9, 3, 1) design having $\varphi = (0\ 1\ 2\ 3\ 4\ 5)(6\ 7\ 8)$ as automorphism with using Kramer-Mesner theorem. We now compute the $2-orbits$ and $3-orbits$ to construct the matrix $A_{3,2}$. Let $\Gamma = \bigcup_{i=1}^{17} \Gamma_i$ denote the set of $3-orbits$ and $\Delta = \bigcup_{j=1}^{7} \Delta_j$ denote the set of $2-orbits$.

$\Gamma_1 = \{012, 123, 234, 345, 450, 501\}$ $\Gamma_2 = \{013, 124, 235, 340, 451, 502\}$ $\Gamma_3 = \{014, 125, 230, 341, 452, 503\}$

$\Gamma_4 = \{024, 135\}$ $\Gamma_5 = \{016, 127, 238, 346, 457, 508\}$ $\Gamma_6 = \{017, 128, 236, 347, 458, 506\}$

$\Gamma_7 = \{018, 126, 237, 348, 456, 507\}$ $\Gamma_8 = \{026, 137, 248, 356, 407, 518\}$ $\Gamma_9 = \{027, 138, 246, 357, 408, 516\}$

$\Gamma_{10} = \{028, 136, 247, 358, 406, 517\}$ $\Gamma_{11} = \{036, 147, 258\}$ $\Gamma_{12} = \{037, 148, 256\}$

$\Gamma_{13} = \{038, 146, 257\}$ $\Gamma_{14} = \{067, 178, 286, 367, 478, 586\}$ $\Gamma_{15} = \{068, 176, 287, 368, 476, 587\}$

$\Gamma_{16} = \{078, 186, 267, 378, 486, 567\}$ $\Gamma_{17} = \{678\}$

$\Delta_1 = \{01, 12, 23, 34, 45, 50\}$ $\Delta_2 = \{02, 13, 24, 35, 40, 51\}$ $\Delta_3 = \{03, 14, 25\}$

$\Delta_4 = \{06, 17, 28, 36, 47, 58\}$ $\Delta_5 = \{07, 18, 26, 37, 48, 56\}$ $\Delta_6 = \{08, 16, 27, 38, 46, 57\}$

$\Delta_7 = \{67, 78, 86\}$

Now, we compute the matrix $A_{3,2}$.

$$A_{3,2} = \begin{pmatrix} 2 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 2 & 0 & 0 & 0 & 0 \\ 1 & 1 & 2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 2 \\ 0 & 0 & 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 1 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Since $\lambda = 1$ and $\boldsymbol{u}_7 = (1, 1, 1, 1, 1, 1, 1)$, we search for an integral solution $\boldsymbol{z}$ which satisfies the equation $\boldsymbol{z} \cdot A_{\mathbf{3},2} = (1, 1, 1, 1, 1, 1, 1)$. One solution is that $\boldsymbol{z} = (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$. We can find all solutions, but there is exactly one $2 - (9, 3, 1)$ design up to isomorphism. Therefore, finding one solution is enough in this example. If we combine the four $3 - orbits$ (i.e. the union of $\Gamma_4, \Gamma_5, \Gamma_{12}$, and Γ_{17}), we have a $2 - (9, 3, 1)$. Then;

$$\mathfrak{B} = \{\Gamma_4, \Gamma_5, \Gamma_{12}, \Gamma_{17}\} = \{024, 135, 016, 127, 238, 346, 457, 508, 037, 148, 256, 678\}.$$

Finding nonnegative solutions to the Kramer-Mesner matrix equation have exponential complexity with known algorithms. Nonetheless, this method to finding designs which have specified automorphisms has been very useful in practice in discovering previously unknown designs.

Theorem 2.41 [40] A $\mathcal{G}$ -invariant large set $LS[N](t, k, v)$ exists if and only if there exist a matrix $\boldsymbol{z} \in \{0, 1\}^{1\times n}$, satisfying the following matrix equation:

$$\boldsymbol{z} \cdot A_{k,t} = \lambda \boldsymbol{u}_m$$

where $\boldsymbol{u}_m$ is the m-dimensional vector which all entries are 1.

S. S. Magliveras and C. A. Cusack [40] generalized the Kramer-Mesner theorem for the existence of large sets of t-designs.

Theorem 2.42 [40] A $[\mathcal{g}]$-invariant large set $LS[N](t,k,v)$ exists if and only if there exist a matrix $\boldsymbol{z} \in \{0,1\}^{n \times N}$, with constant row sum 1, satisfying the matrix equation:

$$\boldsymbol{z} \cdot A_{k,t} = \lambda(j, \dots, j) = \begin{pmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{pmatrix}.$$

The large sets that are known to exist are listed below. For more details of large sets, the reader should check [40, 41, 42, 43, 44, 45, 46, 47, 48].

(i) An $LS_1(2,3,v)$ exists for all admissible parameters of $v \neq 7$. [43, 44, 45, 46]

(ii) An $LS_1(2,4,13)$ exists. [41]

(iii) An $LS_1(2,4,16)$ exists. [47]

(iv) An $LS_2(3,4,13)$ exists. [42]

(v) An $LS_{60}(4,5,60v+4)$ exists for $\gcd(v,60) = 1,2$. [48]

(vi) No $LS_1(3,4,v)$ is known. (*Large set of SQS*) [53]

(vii) An $LS_3(3,4,v)$ exists for $v \equiv 0,6 \ (mod\ 12)$. [49]

(viii) An $LS_6(3,4,v)$ exists for $v \equiv 9 \ (mod\ 12)$. [49]

(ix) An $LS_{12}(3,4,v)$ exists for $v \equiv 3 \ (mod\ 12)$. [49]

(x) The number of disjoint designs in $LS_\lambda(t,t+1,v)$ is $N = \frac{v-t}{\lambda}$.

CHAPTER 3

QUANTUM JUMP CODES

Quantum computation is placed in the intersection of the fields quantum physics, computer science, and information theory. In this thesis, we mainly consider mathematical concept of quantum computation. By interaction with the environment, some errors occur in quantum systems. We focus on the errors caused by spontaneous emission, specifically quantum jumps.

In 1995, Shor [50] has shown that error correction in quantum systems is possible. In the quantum information theory, big developments took place in the late twentieth century after Shor's pioneering work. After six years of developments, Alber *et al*. [22] introduced an error correction model which corrects the errors caused by quantum jumps.

We now continue with the basics of quantum computing and quantum coding theory.

3.1 Basics of Quantum Computing

Classical computers use binary digits (*bits*) to code and encode data. Any bit represents one information which has two possibilities as mathematically 0 or 1. In the quantum systems, the basic unit of quantum information is *quantum bit* (*qubit*).

In quantum computations, mathematically, we are working on a finite dimensional vector space over complex numbers. We can consider Hilbert vector space, since in a Hilbert space Hermitian inner product is defined. We will denote a Hilbert space by $\mathcal{H}$. Therefore, quantum codes can be defined on a finite dimensional Hilbert space $\mathcal{H}$. Hence, in a quantum system, a qubit can be modeled as a 2-dimensional vector space. Any quantum code of length n is a subspace of a Hilbert space of length 2^n.

We now give some fundamental definitions from linear algebra and then we will introduce the Dirac notation.

Any vector x is a linear combination of vectors $s_1, s_2, \dots, s_n$ if there exist complex numbers $\alpha_1, \alpha_2, \dots, \alpha_n$ such that $x = \alpha_1 s_1 + \alpha_2 s_2 + \cdots + \alpha_n s_n$. We consider a set of vectors S. This vector set generates a complex vector space V if we can write all elements of V as linear combination of vectors in S. In other words, for all $x \in V$, x can be written as $x = \alpha_1 s_1 + \alpha_2 s_2 + \cdots + \alpha_n s_n$ for some $s_i \in S$ and $\alpha_i \in \mathbb{C}$. For a given S, the subspace of all linear combinations of vectors in S is called the *span* of S and it is denoted by $span(S)$. A set of vectors B is called a *basis* for a vector space V if we can write uniquely all elements of V as a linear combination of vectors in B. In a 2-dimensional vector space, any pair of vectors that are not multiples of each other form a basis.

Quantum states are represented by *Dirac* (*bra-ket*) notation. A *ket* vector, a quantum state of a single particle, is a 2-dimensional vector in $\mathcal{H}$ and represented by $|x\rangle$. A quantum state $|x\rangle$ is a column vector. The Hilbert space $\mathcal{H}$ of dimension 1 is the set of complex numbers. Elements of the Hilbert space of dimension 2 are the 2×1 column vectors where the entries are complex numbers. We can find a basis for a finite dimensional vector space. Hence, for $\binom{\alpha}{\beta} \in \mathcal{H}$, $\binom{\alpha}{\beta} = \alpha\binom{1}{0} + \beta\binom{0}{1}$ holds where $\alpha, \beta \in \mathbb{C}$. So, the vectors $\binom{1}{0}$ and $\binom{0}{1}$ is a basis for the two-dimensional Hilbert space. As in the classical computers, there are two pure states in the quantum systems. In a quantum system, $|0\rangle$ and $|1\rangle$ are called pure states. Pure states have matrix representations; $|0\rangle = \binom{1}{0}$ and $|1\rangle = \binom{0}{1}$. So, $\{|0\rangle, |1\rangle\}$ is a basis for the two-dimensional Hilbert space. Hence, the two-dimensional Hilbert space is $\mathcal{H} = \{\alpha|0\rangle + \beta|1\rangle : \alpha, \beta \in \mathbb{C}\}$. From now on, $|x\rangle$ represents a vector in $\mathcal{H}$. Any state $|x\rangle$ can be written as a linear combination of pure states, that is; $|x\rangle = \alpha|0\rangle + \beta|1\rangle$ for $\alpha, \beta \in \mathbb{C}$. This situation is called as *quantum superposition*. The main advantage of quantum computers over classical computer is superposition, that is, while bits can have only values 0 and 1, qubits have not only the values $|0\rangle$ and $|1\rangle$ but also any linear combination of the values $|0\rangle$ and $|1\rangle$, $\alpha|0\rangle + \beta|1\rangle$, where $\alpha, \beta \in \mathbb{C}$ such that $|\alpha|^2 + |\beta|^2 = 1$. We use measurements to get information about the state, since we cannot know the initial state. Indeed, the condition $|\alpha|^2 + |\beta|^2 = 1$ comes from a basic probability computation. After the measurement, the probability to have $|0\rangle$ as a measurement result is $|\alpha|^2$, and the probability to have $|1\rangle$ as a measurement result is $|\beta|^2$. Since the sum of the probabilities equal to 1, we have the condition $|\alpha|^2 + |\beta|^2 = 1$. Geometrically, this condition is equal to normalizing a state to length one. Since we are working on a Hilbert space over the complex numbers, each vector has a complex conjugate. The conjugate transpose of a vector x is denoted by $x^\dagger$. Now we define *bra* vector which is denoted by $\langle x|$ in Dirac notation as the complex conjugate transpose of the $|x\rangle$, i.e.

$$\langle x| = |x\rangle^\dagger.$$

A state $\langle x|$ is a row vector. For instance, if $|x\rangle = \begin{pmatrix} 1 \\ 1+i \end{pmatrix}$, then $\langle x| = (1 \quad 1-i)$.

We now define an inner product of two vectors which is a way to multiply vectors.

Let $\mathbb{F} = \{0, 1\}$ and define $|x_1\rangle = \sum_{y\in\mathbb{F}^n} c_y\,|y\rangle$ and $|x_2\rangle = \sum_{y\in\mathbb{F}^n} d_y\,|y\rangle$ where $c_y, d_y \in \mathbb{C}$.

Definition 3.1 A complex function $\langle x_2|x_1\rangle = \sum_{y\in\mathbb{F}^n} \bar{c_y} d_y \in \mathbb{C}$ is called a *Hermitian inner product* of $|x_1\rangle$ and $|x_2\rangle$ on a vector space V if the following properties are satisfied for $x_1, x_2, x_3 \in V$ and $a, b \in \mathbb{C}$.

(i) Positive definiteness: $\langle x|x\rangle \geq 0$, and $\langle x|x\rangle = 0$ implies $x = 0$,

(ii) Conjugate symmetry: $\langle x_2|x_1\rangle = \overline{\langle x_1|x_2\rangle}$, and

(iii) Linearity: $(a\langle x_2| + b\langle x_3|)|x_1\rangle = a\langle x_2|x_1\rangle + b\langle x_3|x_1\rangle$,

where $\overline{\langle x_1|x_2\rangle}$ stands for the complex conjugate of $\langle x_1|x_2\rangle$.

The vector pair $|x_1\rangle$ and $|x_2\rangle$ is called *orthogonal* if $\langle x_1|x_2\rangle = 0$.The *norm* or length of a vector is defined as $\left||x\rangle\right| = \sqrt{\langle x|x\rangle}$. If all elements of a vector set are of length one and orthogonal to each other, then we say that this vector set is *orthonormal*. In other words, a set of vectors $B = \{|x_1\rangle, |x_2\rangle, \dots, |x_n\rangle\}$ is called orthonormal if for all i, j, $\langle x_i|x_j\rangle = \delta_{ij}$, where

$$\delta_{ij} = \begin{cases} 1 & if\ i = j \\ 0 & otherwise. \end{cases}$$

In order to define an n-qubit state, we now define Kronecker product.

Definition 3.2 Let A be an $n \times m$ matrix and B be a $p \times q$ matrix. The *Kronecker product* $A \otimes B$ is the $mp \times nq$ matrix which is defined as follows:

$$A \otimes B = \begin{pmatrix} a_{11}(B) & \cdots & a_{1n}(B) \\ \vdots & \ddots & \vdots \\ a_{m1}(B) & \cdots & a_{mn}(B) \end{pmatrix}.$$

Example 3.1 Let $A = \begin{pmatrix} i & 2 \\ 0 & 3 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 2 & 4 \\ 6 & 8i & 10 \end{pmatrix}$.

$$A \otimes B = \begin{pmatrix} i & 2 \\ 0 & 3 \end{pmatrix} \otimes \begin{pmatrix} 0 & 2 & 4 \\ 6 & 8i & 10 \end{pmatrix} = \begin{pmatrix} i\cdot 0 & i\cdot 2 & i\cdot 4 & 2\cdot 0 & 2\cdot 2 & 2\cdot 4 \\ i\cdot 6 & i\cdot 8i & i\cdot 10 & 2\cdot 6 & 2\cdot 8i & 2\cdot 10 \\ 0\cdot 0 & 0\cdot 2 & 0\cdot 4 & 3\cdot 0 & 3\cdot 2 & 3\cdot 4 \\ 0\cdot 6 & 0\cdot 8i & 0\cdot 10 & 3\cdot 6 & 3\cdot 8i & 3\cdot 10 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 2i & 4i & 0 & 4 & 8 \\ 6i & -8 & 10i & 12 & 16i & 20 \\ 0 & 0 & 0 & 0 & 6 & 12 \\ 0 & 0 & 0 & 18 & 24i & 30 \end{pmatrix}.$$

The Kronecker product of A and B, $A \otimes B$, is called *Tensor product* of A and B if A and B are linear transformations.

We now define a quantum system which consists of n-qubits. The joint state of n-qubits is defined as follow:

$$|x\rangle = |x_1 x_2 \dots x_n\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle,$$

where $\otimes$ denotes the tensor product and $x_i \in \{0,1\}$. Here, from the definition of tensor product, it is easy to see that $|x\rangle$ is a 2^n-dimensional vector in $\mathcal{H}^{\otimes n}$.

In general, for the vectors $|\varphi\rangle$ and $|\phi\rangle$, the following notations are equal.

$$|\varphi\rangle \otimes |\phi\rangle = |\varphi\rangle|\phi\rangle = |\varphi\phi\rangle$$

Let $\mathbb{F} = \{0,1\}$ and $\mathbb{F}^n = \underbrace{\mathbb{F}\times\mathbb{F}\times\cdots\times\mathbb{F}}_{n\ times}$. Then, any vector $x = (x_1, x_2, \dots, x_n)$ in $\mathbb{F}^n$, $|x\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle$ is pure state for n-qubits system. There are 2^n vectors in $\{|x\rangle : x \in \mathbb{F}^n\}$. These vectors form an orthonormal basis of $\mathcal{H}^{\otimes n}$.

Therefore, any state of n-qubit system can be represented by

$$|\varphi\rangle = \sum_{x\in\mathbb{F}^n} \alpha_x |x\rangle,$$

where $\sum_{x\in\mathbb{F}^n} |\alpha_x|^2 = 1, \alpha_x \in \mathbb{C}$.

Note. In the quantum information theory, the scalar multiple of a state $|x\rangle$, $\alpha_x|x\rangle$ ($\alpha_x \neq 0$), is identified as the same state $|x\rangle$. Therefore, without loss of generality, we will assume that $\langle x|x\rangle = 1$.

The Hamming weight of a state $|x\rangle$ is defined as the number of non-zero positions in x and denoted by $wt(|x\rangle)$.

Example 3.2 *(Hamming weight)*

$$wt(|11010\rangle) = 3 \qquad wt(|011101001101\rangle) = 7$$

$$wt(|0000\rangle) = 0 \qquad wt(|1\rangle) = 1$$

Example 3.3 *(Examples of inner product)*

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

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

Example 3.4 *(Examples of n-qubit systems)*

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix}^T$$

$$|01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \end{pmatrix}^T$$

$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \end{pmatrix}^T$$

$$|11\rangle = |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 \end{pmatrix}^T$$

$$|001\rangle = |0\rangle \otimes |0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}^T$$

$$|101\rangle = |1\rangle \otimes |0\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}^T$$

$$|111\rangle = |1\rangle \otimes |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}^T$$

By extending the above example, we can generalize the tensor product of the vectors $|0\rangle$ and $|1\rangle$.

$$|0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle \otimes |0\rangle = \left|\underbrace{00\cdots 00}_{n}\right\rangle = (\underbrace{1 \quad 0 \quad 0 \quad \cdots \quad 0 \quad 0}_{2^n})^T,$$

$$|0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle \otimes |1\rangle = \left|\underbrace{00\cdots 01}_{n}\right\rangle = (\underbrace{0 \quad 1 \quad 0 \quad \cdots \quad 0 \quad 0}_{2^n})^T,$$

$$|0\rangle \otimes |0\rangle \otimes \cdots \otimes |1\rangle \otimes |0\rangle = \left|\underbrace{00\cdots 10}_{n}\right\rangle = (\underbrace{0 \quad 0 \quad 1 \quad \cdots \quad 0 \quad 0}_{2^n})^T,$$

$$\vdots$$

$$|1\rangle \otimes |1\rangle \otimes \cdots \otimes |1\rangle \otimes |0\rangle = \left|\underbrace{11\cdots 10}_{n}\right\rangle = (\underbrace{0 \quad 0 \quad 0 \quad \cdots \quad 1 \quad 0}_{2^n})^T,$$

$$|1\rangle \otimes |1\rangle \otimes \cdots \otimes |1\rangle \otimes |1\rangle = \left|\underbrace{11\cdots 11}_{n}\right\rangle = (\underbrace{0 \quad 0 \quad 0 \quad \cdots \quad 0 \quad 1}_{2^n})^T.$$

We now consider a Hilbert space of dimension 2^n where $n \geq 2$. Let $n = 2$. Then the elements of the Hilbert space of dimension 4 are the 4×1 column vectors. So, any element x of $\mathcal{H}$ has the form

$$x = \begin{pmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{pmatrix}$$

where $a_{00}, a_{01}, a_{10}, a_{11} \in \mathbb{C}$. Each vector x can be written as follows,

$$x = \begin{pmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{pmatrix} = a_{00}\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + a_{01}\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + a_{10}\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + a_{11}\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

It is shown that; $|00\rangle = (1 \quad 0 \quad 0 \quad 0)^T$, $|01\rangle = (0 \quad 1 \quad 0 \quad 0)^T$, $|10\rangle = (0 \quad 0 \quad 1 \quad 0)^T$, $|11\rangle = (0 \quad 0 \quad 0 \quad 1)^T$. So, $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ is a basis for the Hilbert space of dimension 2^2. Hence,

$$\mathcal{H} = \{a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle : a_{00}, a_{01}, a_{10}, a_{11} \in \mathbb{C}\}.$$

We now give a generalization for $n \geq 1$. If we consider any $n \geq 1$, it is easy to see that $\left|\underbrace{10\cdots 00}_{n}\right\rangle, \left|\underbrace{01\cdots 00}_{n}\right\rangle, \ldots, \left|\underbrace{00\cdots 10}_{n}\right\rangle, \left|\underbrace{00\cdots 01}_{n}\right\rangle$ is a basis for the 2^n-dimensional Hilbert space.

Definition 3.3 Let $\mathcal{H}$ be a 2^n-dimensional Hilbert space and $B = \{|b_i\rangle\}$ be a basis for $\mathcal{H}$. $B = \{|b_i\rangle\}$ is called an orthonormal basis for $\mathcal{H}$, if for any $|b_i\rangle, |b_j\rangle \in \mathcal{H}$, $\langle b_i|b_j\rangle = \delta_{ij}$ holds where

$$\delta_{ij} = \begin{cases} 1 & if\ i = j \\ 0 & otherwise. \end{cases}$$

Example 3.5 The set $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ forms an orthonormal basis for 2^2-dimensional Hilbert space, since

$$\langle 00|00\rangle = \langle 01|01\rangle = \langle 10|10\rangle = \langle 11|11\rangle = 1,$$

$$\langle 00|01\rangle = \langle 00|10\rangle = \langle 00|11\rangle = 0,$$

$$\langle 01|00\rangle = \langle 01|10\rangle = \langle 01|11\rangle = 0,$$

$$\langle 10|00\rangle = \langle 10|01\rangle = \langle 10|11\rangle = 0,$$

$$\langle 11|00\rangle = \langle 11|01\rangle = \langle 11|10\rangle = 0.$$

Theorem 3.4 Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be two Hilbert spaces of dimension 2^n and 2^m, respectively. Let $B_1 = \{|b_i\rangle\}_{i\in\{1,2,\dots,2^n\}}$ and $B_2 = \{|d_j\rangle\}_{j\in\{1,2,\dots,2^m\}}$ be bases for $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively. Then, the followings hold.

(i) Tensor product of $\mathcal{H}_1$ and $\mathcal{H}_2$, $\mathcal{H}_1 \otimes \mathcal{H}_2$, is a 2^{n+m}-dimensional vector space.

(ii) $\{|b_i\rangle \otimes |d_j\rangle\}_{i\in\{1,2,\dots,2^n\}, j\in\{1,2,\dots,2^m\}}$ is an orthonormal basis for the vector space $\mathcal{H}_1 \otimes \mathcal{H}_2$.

3.1.1 State Transition in Quantum Systems

In this thesis, with the quantum state transition, we will mean a mapping from the state space of a quantum system to itself, that is, a mapping from $\mathcal{H}$ to $\mathcal{H}$. In a quantum system, a state transition is represented by an operator. This operator must be linear, so that, a state goes to the superposition of their images. For an operator $\mathcal{T}$ and any n-qubit state $|\varphi\rangle$, linearity means that;

$$\mathcal{T}|\varphi\rangle = \mathcal{T}(\alpha_1|x_1\rangle + \alpha_2|x_2\rangle + \cdots \alpha_n|x_n\rangle) = \alpha_1\mathcal{T}|x_1\rangle + \alpha_2\mathcal{T}|x_2\rangle + \cdots + \alpha_n\mathcal{T}|x_n\rangle.$$

Any linear operator in a finite dimensional vector space has a matrix representation.

Example 3.6 Let $\mathcal{H}$ be a two-dimensional Hilbert space. Define a linear transformation $\mathcal{T}$ as follows,

$$\mathcal{T} : \mathcal{H} \to \mathcal{H}$$

$$\mathcal{T}(\alpha|0\rangle + \beta|1\rangle) = \beta|0\rangle + \alpha|1\rangle.$$

Since each linear operator in a finite dimensional vector space has a matrix representation, the corresponding matrix to operator $\mathcal{T}$ is $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Therefore, we will use linear operators which act on the qubits. Since each qubit is represented by 2×1 matrices, we will use linear operators of the form 2×2 matrices. An operator $\mathcal{T}$ is called *unitary* if $\mathcal{T}^\dagger\mathcal{T} = \mathrm{I}$ holds where I is the identity matrix. Mathematically, quantum computations are made by applying unitary operators.

Example 3.7 The matrices $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ are unitary matrices.

During the computation or data transfer, by interaction with the environment some errors occur in the quantum system. Therefore, we need error correction to communicate even if there is an error. In classical systems, there is a basic error correction model where the information is copied and sent several times in different channels so that error is detected and corrected by controlling copied data. By copying data, we mean that if we have a state $x = 011$ we copy x and we have 011011. So, for instance, if we send 011011 and get 001011 as output, by checking second copy of data we can easily see that the second bit had a bit flip error. However, unlike the classical systems, *no-cloning theorem* says that we cannot perfectly copy the information in quantum systems.

Theorem 3.5 (*No-cloning Theorem*) [51] There is no unitary operator U that can code the state $|\varphi\rangle$ as $|\varphi\rangle \otimes |\varphi\rangle$.

Proof. Let U be the unitary operator that can code the state $|\varphi\rangle$ as $|\varphi\rangle \otimes |\varphi\rangle$. Let the state $|\phi\rangle$ be different than the state $|\varphi\rangle$. Then,

$$U|\varphi\rangle = |\varphi\rangle|\varphi\rangle,$$

$$U|\phi\rangle = |\phi\rangle|\phi\rangle,$$

$$U(|\varphi\rangle + |\phi\rangle) = (|\varphi\rangle + |\phi\rangle)(|\varphi\rangle + |\phi\rangle).$$

Since quantum operators are linear, we have

$$U(|\varphi\rangle + |\phi\rangle) = U(|\varphi\rangle) + U(|\phi\rangle) = |\varphi\rangle|\varphi\rangle + |\phi\rangle|\phi\rangle.$$

However, in general,

$$(|\varphi\rangle + |\phi\rangle)(|\varphi\rangle + |\phi\rangle) \neq |\varphi\rangle|\varphi\rangle + |\phi\rangle|\phi\rangle.$$

So, we have a contradiction. Therefore, there is no such a quantum operator U.

Errors are also defined as operators. Any error for a single qubit can be expressed as a linear combination of the following matrices

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

These four matrices are called *Pauli matrices*. We define the set $\mathcal{P} = \{\pm I, \pm iI, \pm\sigma_x, \pm i\sigma_x, \pm\sigma_y, \pm i\sigma_y, \pm\sigma_z, \pm i\sigma_z\}$. This set forms a non-Abelian group, called the *Pauli group*. To correct errors in a quantum system, we will use (inverse) unitary operators.

Example 3.8 Let $\begin{pmatrix} a \\ b \end{pmatrix}$ be a matrix representation of an arbitrary state $|\varphi\rangle = a|0\rangle + b|1\rangle$. We will see what Pauli matrices do to the state $|\varphi\rangle$.

$$I|\varphi\rangle = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix} \qquad \sigma_x|\varphi\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} b \\ a \end{pmatrix}$$

$$\sigma_y|\varphi\rangle = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = i\begin{pmatrix} -b \\ a \end{pmatrix} \qquad \sigma_z|\varphi\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a \\ -b \end{pmatrix}$$

The error σ_x is also called a *bit flip error* and the error σ_z is called a *phase error*. Between these error operators the following relations are known.

$$\sigma_x{}^2 = \sigma_y{}^2 = \sigma_z{}^2 = I,$$

$$\sigma_x\sigma_z = -\sigma_z\sigma_x,$$

$$\sigma_y = i\sigma_x\sigma_z.$$

In particular,

$$I|0\rangle = |0\rangle, \qquad \sigma_x|0\rangle = |1\rangle, \qquad \sigma_y|0\rangle = i|1\rangle, \qquad \sigma_z|0\rangle = |0\rangle,$$

$$I|1\rangle = |1\rangle, \qquad \sigma_x|1\rangle = |0\rangle, \qquad \sigma_y|1\rangle = -i|1\rangle, \qquad \sigma_z|1\rangle = -|1\rangle.$$

As in the classical systems, if an error occurs twice in a qubit, this state stays invariant. Therefore, we can correct errors by applying the same Pauli operators to a qubit if we can find the position of errors and the errors that occurred. We use the notation E_i to indicate any error E which acts to the ith qubit of an n-qubit state where $i \leq n$.

Example 3.9 Let $|\varphi\rangle = (\alpha|110\rangle + \beta|001\rangle)$. If a bit flip error occurs in the first qubit, i.e. σ_{x_1}, then we have,

$$\sigma_{x_1}|\varphi\rangle = \sigma_{x_1}(\alpha|110\rangle + \beta|001\rangle) = (\alpha|010\rangle + \beta|101\rangle).$$

If we apply σ_{x_1} again, we have the initial state $|\varphi\rangle$.

$$\sigma_{x_1}(\alpha|010\rangle + \beta|101\rangle) = (\alpha|110\rangle + \beta|001\rangle) = |\varphi\rangle.$$

3.1.2 Quantum Error Correcting Codes

As mentioned before, any error can be expressed as a linear combination of Pauli matrices. Therefore, any error in an n-qubit system can be expressed as linear combinations of elements of Pauli group. We define the set of all errors that occur in the quantum system as $\mathcal{E}$. Since $\mathcal{P}$ is a group, then $\mathcal{E}$ also forms a group. The group $\mathcal{E}$ is called the *error group*.

$$\mathcal{E} = \{p_1 \otimes p_2 \otimes \cdots \otimes p_n : \ p_i \in \mathcal{P}\}.$$

There are 4^n elements in tensor product of n-error operator since there are 4 Pauli matrices. As $\mathcal{P}$ forms a group with the m multiple of the elements of $\mathcal{P}$ where $m \in \{-1, 1, i, -i\}$, then the result of the tensor product of n-error operator is also m multiple of 4^n elements. Therefore, $|\mathcal{E}| = 4 \cdot 4^n$.

A subspace $\mathcal{C}$ of $\mathcal{H}^{\otimes n}$ is called an $\mathcal{E}$-error correcting quantum code, if we can recover the original state $|c\rangle$ by using the information of $E|c\rangle$, for any element $|c\rangle$ in $\mathcal{C}$ and E in $\mathcal{E}$. More formal definition is given by the next theorem of Knill and Laflamme [52].

Theorem 3.6 [52] A subspace $\mathcal{C} \leq \mathcal{H}^{\otimes n}$ with orthonormal basis $\{|c_i\rangle : i = 1, 2, \dots, m\}$ is a *quantum $\mathcal{E}$-error correcting code* for the set of error operators $\mathcal{E} = \{E_i : i = 1, 2, \dots, p\}$ if and only if the following holds:

$$\langle c_i | E_k^\dagger E_l | c_j \rangle = \delta_{ij} \mu_{E_k, E_l}, \quad \text{for any } i, j, \text{and } E_k, E_l \in \mathcal{E}. \tag{3.1}$$

where

$$\delta_{ij} = \begin{cases} 1, & if\ i = j, \\ 0, & if\ i \neq j. \end{cases}$$

and μ_{E_k,E_l} is a nonnegative constant depending only on E_k and E_l.

Example 3.10 For a 2-qubit quantum system, let $\mathcal{E} = \{ I = I \otimes I, E = \sigma_x \otimes I\}$ and let $\mathcal{C} = \langle |01\rangle, |10\rangle \rangle$.

$$\langle 01|E^{\dagger}E|01\rangle = \langle 11||11\rangle = (0 \quad 0 \quad 0 \quad 1)\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = 1,$$

$$\langle 10|E^{\dagger}E|10\rangle = \langle 00||00\rangle = (1 \quad 0 \quad 0 \quad 0)\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = 1,$$

$$\langle 01|E^{\dagger}E|10\rangle = \langle 11||00\rangle = (0 \quad 0 \quad 0 \quad 1)\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = 0,$$

$$\langle 10|E^{\dagger}E|01\rangle = \langle 00||11\rangle = (0 \quad 0 \quad 1 \quad 0)\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = 0,$$

$$\langle 10|I^{\dagger}E|01\rangle = \langle 10|E^{\dagger}I|01\rangle = \langle 01|I^{\dagger}E|10\rangle = \langle 01|E^{\dagger}I|10\rangle = 0,$$

$$\langle 01|I^{\dagger}E|01\rangle = \langle 01|E^{\dagger}I|01\rangle = \langle 10|I^{\dagger}E|10\rangle = \langle 10|E^{\dagger}I|10\rangle = 0.$$

In the last line, although $i = j$ the result is 0, that means $\mu_{E,I}$ is 0. Thus, by Knill-Laflamme Theorem, $\mathcal{C}$ is an *$\mathcal{E}$-error correcting quantum code*. Here, the code space is spanned by $|01\rangle$ and $|10\rangle$ and the error space is spanned by $|11\rangle$ and $|00\rangle$ since $E|01\rangle = |11\rangle$ and $E|10\rangle = |00\rangle$.

3.2 Quantum Jump Codes

In a quantum system, various errors occur due to unavoidable interaction with the environment. One type of the errors in quantum system occur due to spontaneous emission by energy loss in quantum systems. There are two types of errors which is caused by spontaneous emission. These errors are known as quantum decay and quantum jump. In 2001, Alber *et al*. [22] introduced quantum jump codes which correct errors due to quantum jumps.

3.2.1 Quantum Decay

A quantum decay operator $\mathbb{D}(t)$ is represented by $\mathbb{D}(t) = e^{-\frac{\kappa t}{2}|1\rangle\langle 1|}$ where t represents time variable and κ represents decay rate. If we consider the Taylor series of e^x, we can fully understand what a decay operator does to the any quantum state.

Firstly, let $\alpha = -\frac{\kappa t}{2}$ and $B = |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$. It is easy to see that all powers of B are equal to B, that is, $B = B^i$ for any positive integer i. Then, $\mathbb{D}(t) = e^{\alpha B}$. Now, consider the Taylor series of $e^{\alpha B}$.

$$e^{\alpha B} = \sum_{n=0}^{\infty} \frac{(\alpha B)^n}{n!} = I + \alpha B + \frac{(\alpha B)^2}{2!} + \frac{(\alpha B)^3}{3!} + \frac{(\alpha B)^4}{4!} + \cdots$$

If we add and subtract B to the above series, we get

$$e^{\alpha B} = \sum_{n=0}^{\infty} \frac{(\alpha B)^n}{n!} = I - B + B + \alpha B + \frac{\alpha^2 B}{2!} + \frac{\alpha^3 B}{3!} + \frac{\alpha^4 B}{4!} + \cdots$$

Now, grouping B in right side of equation gives

$$e^{\alpha B} = \sum_{n=0}^{\infty} \frac{(\alpha B)^n}{n!} = (I - B) + B\left(1 + \alpha + \frac{\alpha^2}{2!} + \frac{\alpha^3}{3!} + \frac{\alpha^4}{4!} + \cdots\right) = (I - B) + Be^{\alpha}.$$

Since $(I - B) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, we have

$$e^{\alpha B} = e^{-\frac{\kappa t}{2}|1\rangle\langle 1|} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + e^{-\frac{\kappa t}{2}} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Definition 3.7 A *quantum decay operator* $\mathbb{D}(t)$ is defined by

$$\mathbb{D}(t) = e^{-\frac{\kappa t}{2}|1\rangle\langle 1|} = e^{-\frac{\kappa t}{2}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + e^{-\frac{\kappa t}{2}} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

where t represents time variable and κ represents decay rate.

If we apply decay operator to a qubit $|x\rangle$, where x is either 0 or 1, we have

$$\mathbb{D}(t)|x\rangle = \left(e^{-\frac{\kappa t}{2}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}}\right)|x\rangle = e^{-x\frac{\kappa t}{2}}|x\rangle.$$

We consider the case where spontaneous decay occurs with the same decay rate to each qubit. We now define the decay operator for n-qubit systems. Let $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}^n$ and $\mathbb{D}_V(t) = \underbrace{\mathbb{D}(t) \otimes \mathbb{D}(t) \otimes \cdots \otimes \mathbb{D}(t)}_{n\ times} = \mathbb{D}(t)^{\otimes n}$. Then,

$$\mathbb{D}_V(t)|x\rangle = \mathbb{D}(t)|x_1\rangle \otimes \mathbb{D}(t)|x_2\rangle \otimes \cdots \otimes \mathbb{D}(t)|x_n\rangle = e^{-wt(x)\frac{\kappa t}{2}}|x\rangle$$

holds, where $wt(x)$ stands for the Hamming weight of x.

Example 3.11 *(Decay operator for a single qubit)*

$$\mathbb{D}(t)|0\rangle = \left(\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} + e^{-\frac{\kappa t}{2}}\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}\right)\begin{pmatrix}1\\ 0\end{pmatrix} = \begin{pmatrix}1\\ 0\end{pmatrix} + \begin{pmatrix}0\\ 0\end{pmatrix} = \begin{pmatrix}1\\ 0\end{pmatrix} = |0\rangle,$$

$$\mathbb{D}(t)|1\rangle = \left(\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} + e^{-\frac{\kappa t}{2}}\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}\right)\begin{pmatrix}0\\ 1\end{pmatrix} = \begin{pmatrix}0\\ 0\end{pmatrix} + e^{-\frac{\kappa t}{2}}\begin{pmatrix}0\\ 1\end{pmatrix} = e^{-\frac{\kappa t}{2}}\begin{pmatrix}1\\ 0\end{pmatrix} = e^{-\frac{\kappa t}{2}}|1\rangle.$$

Example 3.12 Let $n = 3$ and $|\varphi\rangle = \alpha_1|100\rangle + \alpha_2|010\rangle + \alpha_3|001\rangle$.

$$\mathbb{D}_V(t)|\varphi\rangle = \alpha_1 e^{-\frac{\kappa t}{2}}|100\rangle + \alpha_2 e^{-\frac{\kappa t}{2}}|010\rangle + \alpha_3 e^{-\frac{\kappa t}{2}}|001\rangle = e^{-\frac{\kappa t}{2}}|\varphi\rangle = |\varphi\rangle.$$

Example 3.13 Let $n = 3$ and $|\varphi\rangle = \alpha_1|001\rangle + \alpha_2|011\rangle + \alpha_3|111\rangle$.

$$\mathbb{D}_V(t)|\varphi\rangle = \alpha_1 e^{-\frac{\kappa t}{2}}|001\rangle + \alpha_2 e^{-\kappa t}|011\rangle + \alpha_3 e^{-3\frac{\kappa t}{2}}|111\rangle.$$

From the above examples, it is clear that if a state $|\varphi\rangle$ has a fixed weight, then the state $|\varphi\rangle$ is invariant under decay operator since any scalar multiple of a state is defined as the same state.

3.2.2 Quantum Jumps

We can demonstrate qubits as two level atoms. So, the pure states $|0\rangle$ and $|1\rangle$ can be thought as two energy levels where $|0\rangle$ is the ground state and $|1\rangle$ is the induced state. By losing energy, the state $|1\rangle$ spontaneously decay into the ground state. This process is called quantum jump. We now define the quantum jump operator mathematically.

We first define the operator A as follows:

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

Definition 3.8 The *quantum jump operator*, $\mathcal{J}$, for a single qubit is defined as follows

$$\mathcal{J}|x\rangle = \begin{cases} A|x\rangle, & \text{if } \langle x|A^\dagger A|x\rangle \neq 0,\\ |x\rangle, & \text{if } \langle x|A^\dagger A|x\rangle = 0.\end{cases}$$

Let $|x\rangle = a|0\rangle + b|1\rangle$. Hence, we have

$$\mathcal{J}(a|0\rangle + b|1\rangle) = \begin{cases} b|0\rangle, & \text{if } b \neq 0, \\ |0\rangle, & \text{if } b = 0. \end{cases}$$

Example 3.14 *(Jump operator for a single qubit)*

$$\mathcal{J}|1\rangle = |0\rangle \qquad\qquad \mathcal{J}|0\rangle = |0\rangle$$

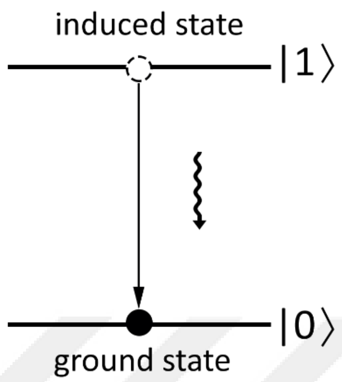


Figure 3. 1 Spontaneous Decay

From the definition of quantum jump operator, if the original state is $|0\rangle$, then a quantum jump cannot occur.

If we consider n-qubit system, a jump operator which acts on the ith position is given by

$$\mathcal{J}_i = I \otimes I \otimes \cdots \otimes I \otimes \mathcal{J} \otimes I \otimes \cdots I \otimes I \otimes.$$

Physically, by continuously monitoring the system we can know where the quantum jump occurred. Indeed, monitoring the system has side effects on the quantum system. Even if no quantum jump occurs, the original state can be changed due to monitoring the system. However, in this thesis we will ignore this situation.

Example 3.15 *(Jump operator for n-qubit system)*

$$\mathcal{J}_1(|01\rangle) = |01\rangle \qquad\qquad \mathcal{J}_3(|1001\rangle) = |1001\rangle$$

$$\mathcal{J}_2(|1101\rangle) = |1001\rangle \qquad\qquad \mathcal{J}_5(|011010\rangle) = |011000\rangle$$

We now consider n-qubit quantum systems to which multiple jump operators are applied. Let the set of jump operators $\mathcal{J}_{i_1}, \mathcal{J}_{i_2}, \ldots, \mathcal{J}_{i_{s-1}}, \mathcal{J}_{i_s}$ be applied to the quantum state $|x\rangle$ where $i_k \leq n$. Let $E = (i_1, i_2, \ldots, i_s)$ be an ordered s-tuple and $V = \{1,2, \ldots, n\}$. Then,

$$\mathcal{J}_E = \mathcal{J}_{i_s}\mathcal{J}_{i_{s-1}} \cdots \mathcal{J}_{i_2}\mathcal{J}_{i_1}.$$

Example 3.16 *(Multiple jump operators)*

$$\mathcal{J}_3\mathcal{J}_1(|111\rangle) = \mathcal{J}_3(|011\rangle) = |010\rangle$$

$$\mathcal{J}_4\mathcal{J}_3\mathcal{J}_1(|1011011\rangle) = \mathcal{J}_4\mathcal{J}_3(|0011011\rangle) = \mathcal{J}_4|0001011\rangle = |0000011\rangle$$

Now consider the state $|\varphi\rangle = \sum_{i=1}^{n} \alpha_i |x_i\rangle$ where $x_i \in \mathbb{F}^n$ and $\alpha_i \in \mathbb{C}$. We apply jump operators to the state $|\varphi\rangle$. Let $E = (i_1, i_2, \ldots, i_s)$ be the error positions. For the nonzero coefficients α_i of x_i, applying jump operator $\mathcal{J}_{i_j}$ to x_{i_j} results two different cases. Let X be the set of x_{i_j}'s whose the i_jth position is 1, where $i \in E$. If $|X| \geq 1$, then jump operator deletes the all data except the elements of X, and for the elements of X quantum jump occurs, that is, flips 1's in the ith position to 0 in $x_i \in X$. Otherwise, if $|X| = 0$, quantum jump cannot occur, that is, state stay invariant under jump operator.

For a better understanding, we give an example.

Example 3.17 *(Multiple jump operators)*

(i) $\mathcal{J}_2\mathcal{J}_1(|1111\rangle + |0011\rangle) = \mathcal{J}_2(|0111\rangle) = |0011\rangle$

(ii) $\mathcal{J}_4\mathcal{J}_2(|1100\rangle + |0110\rangle) = \mathcal{J}_4(|1000\rangle + |0010\rangle) = |1000\rangle + |0010\rangle$

In the part (i) of the above example, if we apply the jump operator $\mathcal{J}_1$ to $(|1111\rangle + |0111\rangle)$, the jump occurs in $|1111\rangle$ and we get $|0111\rangle$, and the jump deletes $|0011\rangle$. In the part (ii), applying $\mathcal{J}_2$ gives $|1000\rangle + |0010\rangle$. Now if we apply $\mathcal{J}_4$ to this state, jump cannot occur or cannot delete the data.

Example 3.18 *(Multiple jump operators)*

(a) $\mathcal{J}_2\mathcal{J}_1(|100\rangle + |011\rangle) = |000\rangle$ (b) $\mathcal{J}_2\mathcal{J}_1(|010\rangle + |101\rangle) = |001\rangle$

(c) $\mathcal{J}_1\mathcal{J}_2(|100\rangle + |011\rangle) = |011\rangle$ (d) $\mathcal{J}_1\mathcal{J}_2(|010\rangle + |101\rangle) = |000\rangle$

Jump operators mostly are not commutative, as we can see in the above example. For instance, in *Example 3.18* (b), $\mathcal{J}_2$ does not change the state. So, the question comes to mind, what if we delete the jump operators which does not change the state. If we delete these operators, we have a subsequence of jump operators $\mathcal{J}_{E_\varphi} = \mathcal{J}_{i_{j_r}} \cdots \mathcal{J}_{i_{j_1}}$ where $E_\varphi = \left(i_{j_1}, \ldots, i_{j_r}\right) \subset E$. Hence, for the state $|\varphi\rangle = \sum_{x\in\mathbb{F}^n} \alpha_x |x\rangle$, we have

$$\mathcal{J}_{E_\varphi}|\varphi\rangle = \mathcal{J}_E|\varphi\rangle.$$

Define support of a vector $x = (x_1, x_2, \ldots, x_n)$, $supp(x)$, as follows

$$supp(x) = \{i : x_i \neq 0\}.$$

Therefore, for the state $|\varphi\rangle = \sum_{x \in \mathbb{F}^n} \alpha_x |x\rangle$ there are x's such that $\alpha_x \neq 0$ and $supp(x) \subset E$. Furthermore, operators in $\mathcal{J}_{E_\varphi}$ are commutative.

Hence, for a state $|\varphi\rangle$, we consider the jump operators which are commutative when we apply to $|\varphi\rangle$. So, define a subset E of V where E consist of the positions of commutative jump operators with respect to $|\varphi\rangle$. Then, multiple jump operators are denoted by

$$\mathcal{J}_E = \otimes_{i=1}^{n} A_i, \quad A_i = \begin{cases} I & \text{if } i \notin E, \\ \mathcal{J} & \text{if } i \in E. \end{cases}$$

Quantum decay and quantum jump process is given by

$$\mathbb{D}_V(t_s) \cdot \mathcal{J}_{i_s} \cdot \mathbb{D}_V(t_{s-1}) \cdot \mathcal{J}_{i_{s-1}} \cdot \cdots \cdot \mathbb{D}_V(t_1) \cdot \mathcal{J}_{i_1} \cdot \mathbb{D}_V(t_0).$$

Therefore, state is changed by decay operator between quantum jumps. That is, there is a close connection between decay and jump operators.

3.2.3 Decoherence-free Subspace for Decay Operator

So far, we have discussed quantum jump and quantum decay errors and so finding an error model which corrects quantum jump and quantum decay errors is the main problem. If we can find an error-free space caused by quantum decay operator, then we only need to correct quantum jump errors. That is equivalent to applying passive error correction to quantum decay. Therefore, we will find a subspace that any arbitrary quantum state is invariant under decay operator. Note that any multiple of a state is identified as the same state.

Definition 3.9 A subspace $\mathbb{W}$ is said to be *decoherence-free subspace* if $\mathbb{D}_V(t)|\varphi\rangle = \alpha|\varphi\rangle$ holds where $|\varphi\rangle \in \mathbb{W}$ and α is a nonzero constant number.

Example 3.19 Let $\mathbb{W} = \{|\varphi\rangle, |\psi\rangle\}$ and $|\varphi\rangle = \alpha_1|100\rangle + \alpha_2|010\rangle$, $|\psi\rangle = \beta_1|001\rangle + \beta_2|010\rangle$. If we apply decay operator to states, we have

$$\mathbb{D}_V(t)|\varphi\rangle = \alpha_1 e^{-\frac{\kappa t}{2}}|100\rangle + \alpha_2 e^{-\frac{\kappa t}{2}}|010\rangle = e^{-\frac{\kappa t}{2}}|\varphi\rangle,$$

$$\mathbb{D}_V(t)|\psi\rangle = \beta_1 e^{-\frac{\kappa t}{2}}|001\rangle + \beta_2 e^{-\frac{\kappa t}{2}}|010\rangle = e^{-\frac{\kappa t}{2}}|\psi\rangle.$$

Thus, $\mathbb{W}$ is a decoherence-free subspace since the states $|\varphi\rangle$ and $|\psi\rangle$ are invariant under decay operator.

Example 3.20 Consider the subspace $\mathbb{W} = \{|\varphi\rangle, |\psi\rangle\}$ where $|\varphi\rangle = \alpha_1|101\rangle + \alpha_2|010\rangle$ and $|\psi\rangle = \beta_1|001\rangle + \beta_2|110\rangle$. Applying the decay operator to the states gives

$$\mathbb{D}_V(t)|\varphi\rangle = \alpha_1 e^{-\kappa t}|101\rangle + \alpha_2 e^{-\frac{\kappa t}{2}}|010\rangle \neq |\varphi\rangle,$$

$$\mathbb{D}_V(t)|\psi\rangle = \beta_1 e^{-\frac{\kappa t}{2}}|001\rangle + \beta_2 e^{-\kappa t}|110\rangle \neq |\psi\rangle.$$

So, $\mathbb{W}$ is not a decoherence-free subspace under decay operator.

As we can see in above examples, the necessary condition to be decoherence-free subspace is that for $|\varphi\rangle = \sum_{i=1}^{n} \alpha_i |x_i\rangle$ where $x_i \in \mathbb{F}^n$ and $\alpha_i \in \mathbb{C}$, for any $|x_i\rangle$ which has a nonzero coefficient α_i must have fixed weight.

We now give some notation. Let $\mathbb{F}_k^n$ denotes the vectors in $\mathbb{F}^n$ which has the fixed weight k. The subspace $\mathbb{W}_k$ denotes a subspace which is spanned by vectors in $\mathbb{F}_k^n$. That is,

$$\mathbb{F}_k^n = \{x \in \mathbb{F}^n : wt(x) = k\},$$

$$\mathbb{W}_k = \langle\, |x\rangle : x \in \mathbb{F}_k^n \rangle.$$

Lemma 3.10 [24] The subspace $\mathbb{W}$ is a decoherence-free subspace with respect to quantum decay operator $\mathbb{D}_V(t)$ if and only if $\mathbb{W}$ is a subspace of $\mathbb{W}_k$ where k is arbitrary fixed weight.

Proof. Let $|\varphi\rangle = \sum_{x\in\mathbb{F}^n} \alpha_x |x\rangle \in \mathbb{W}$. We have,

$$\begin{aligned}\mathbb{D}_V(t)|\varphi\rangle &= \sum_{x\in\mathbb{F}^n} \alpha_x^{(i)} \mathbb{D}_V(t)|x\rangle \\ &= \sum_{x\in\mathbb{F}^n} \alpha_x^{(i)} e^{-wt(x)\frac{\kappa t}{2}}|x\rangle \\ &= \sum_{k=0}^{n} \sum_{x\in\mathbb{F}_k^n} \alpha_x^{(i)} e^{-\frac{k\kappa t}{2}}|x\rangle.\end{aligned}$$

$\mathbb{D}_V(t)|\varphi\rangle = \delta|\varphi\rangle$ holds for any t and constant δ, if the weight k is constant, and that proves the lemma.

Thus, if we want to construct a jump code $\mathcal{C}$, then it must be contained in a subspace of $\mathbb{W}_k$ for some k. Hence, if we apply quantum jump operator to any state $|c\rangle \in \mathbb{W}_k$, we have $\mathcal{J}_E|c\rangle \in \mathbb{W}_{k'}$ where $k' \leq k$. That is because, a jump operator may decrease the Hamming weight of code.

3.2.4 Quantum Jump Codes

In this subsection, the definition of a jump code will be given. In the previous subsection, it is said that an e-error correcting quantum jump code $\mathcal{C}$ must be a subspace of $\mathbb{W}_k$. So, we will consider the error operators $\mathcal{E}$ which has the form

$$\mathcal{E} = \{\mathcal{J}_E : E \text{ is a } s - \text{list of elements in } V, s \leq e\}.$$

As it is mentioned, we observe that quantum system is continuously monitored. So that, the positions of quantum jumps are known. Let the error positions be $E = (i_1, i_2, \dots, i_s)$. Since we know the error positions by monitoring the system, Knill-Laflamme theorem can be simplified as

$$\langle c_i|\mathcal{J}_E^\dagger \mathcal{J}_E|c_j\rangle = \delta_{ij}\mu_E, \quad \text{for any } i \neq j, \text{and } \mathcal{J}_E \in \mathcal{E}$$

where μ_E is a nonzero constant which depends on E.

Now, we can define an e-error correcting quantum jump code.

An e-error correcting quantum jump code $\mathcal{C}$, denoted by $(n, m, e)_k$ *jump code*, is a subspace of $\mathbb{W}_k$ which satisfies the Knill-Laflamme Theorem. In the definition, n indicates n-qubit system, m is the dimension of the code $\mathcal{C}$, e indicates the number of errors and k is the fixed weight of the code.

Theorem 3.11 [23] For a jump code $\mathcal{C} = (n, m, e)_k$, any s-jump error, where $0 \leq s \leq e$ can be corrected.

Let $x|_E = (x_{\ell_1}, x_{\ell_2}, \dots, x_{\ell_s})$ where $x = (x_1, x_2, \dots, x_n) \in \mathbb{F}^n$ and $E = \{\ell_1, \ell_2, \dots, \ell_s\}$.

Lemma 3.12 [24] Let the code $\mathcal{C}$ be an $(n, m, e)_k$ jump code. Then for any E, where $|E| = s \leq e$, and for any $y \in \mathbb{F}^s$ the following conditions hold:

(i) $\mathcal{J}_E|c_i\rangle = |c_i\rangle$ implies that $\alpha_x^{(i)} = 0$ for any $x \in \mathbb{F}_k^n$ such that $x|_E = (1,1, \dots, 1)$.

(ii) For an orthonormal basis $\{|c_i\rangle : i = 1, \dots, m\}$, if $\mathcal{J}_E|c_i\rangle = |c_i\rangle$ holds for some i , then $\mathcal{J}_E|c_j\rangle = |c_j\rangle$ holds for any $j = 1, \dots, m$.

Proof. (i) is clear, because if $\alpha_x^{(i)} \neq 0$ then the state would not stay invariant under jump operator. (ii) holds, because if $\mathcal{J}_E|c_i\rangle \neq |c_i\rangle$ then $\langle c_i|\mathcal{J}_E^\dagger\mathcal{J}_E|c_j\rangle < \langle c_i|c_j\rangle = 1$.

3.2.5 Examples of e-error Correcting Quantum Jump Codes

In this subsection, we will construct some e-error correcting jump codes.

3.2.5.1 A 1-error Correcting Quantum Jump Code of Length Four

We will construct a 1-error correcting quantum jump code of length four. Now let $\mathcal{C}$ be a 1-error correcting quantum jump code. As we proved, any code word will have a constant weight.

A code word $|c\rangle$ is represented by

$$|c\rangle = \sum_{x\in\mathbb{F}_k^n} \alpha_x|x\rangle$$

for a constant weight k where $0 \leq k \leq n$.

Since $n = 4$, we have $0 \leq k \leq 4$. So, for the fixed weight k there are 5 possibilities $0, 1, 2, 3, 4$.

We now define an orthonormal basis c_i of the code $\mathcal{C}$ as follows

$$\left\{c_i = \sum_{x\in\mathbb{F}_k^n} \alpha_x{}^{(i)}|x\rangle : i = 1, 2, \dots, m\right\}.$$

As $\langle c_i|c_j\rangle = \delta_{ij}$, the following holds for any i and j, and for a constant k where $0 \leq k \leq 4$.

$$\sum_{x\in\mathbb{F}_k^4} \overline{\alpha_x}^{(i)}\alpha_x{}^{(j)} = \delta_{ij}. \tag{3.2}$$

Here, $\overline{\alpha_x}^{(i)}$ denotes the complex conjugate of $\alpha_x{}^{(i)}$.

We now define a matrix P_ℓ as a 4×4 diagonal matrix in which all diagonal entries are 1 except for the ℓ-th entry is 0.

Example 3.21 *(P_ℓ matrices)*

$$P_1 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad P_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$P_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad P_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Example 3.22 Let $x = (1 \quad 1 \quad 0 \quad 1)^T$

$$P_1 x = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \qquad P_2 x = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix},$$

$$P_3 x = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \qquad P_4 x = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

As we can see, the matrix P_ℓ and jump operator $\mathcal{J}_\ell$ are similar when we apply to the state $|x\rangle \in \mathbb{F}^4$ if the position ℓ of $|x\rangle$ is 1, i.e. $x_\ell = 1$. Therefore,

$$\mathcal{J}_\ell |c_i\rangle = \sum_{x \in \mathbb{F}_k^4} \alpha_x{}^{(i)} \mathcal{J}_\ell |x\rangle = \sum_{x \in \mathbb{F}_k^4, x_\ell = 1} \alpha_x{}^{(i)} |P_\ell x\rangle.$$

Hence, the following holds for any i, j and $\ell \in V$ where $V = \{1, 2, \dots, n\}$ and $\kappa_{k,\ell,1}$ is a nonzero constant which depends on k and ℓ.

$$\langle c_i | \mathcal{J}_\ell^\dagger \mathcal{J}_\ell | c_j \rangle = \sum_{x \in \mathbb{F}_k^4, x_\ell = 1} \overline{\alpha_x}^{(i)} \alpha_x{}^{(j)} = \delta_{ij} \kappa_{k,\ell,1} \tag{3.3}$$

We can rewrite Equations (3.2) and (3.3) as follows

$$\sum_{x \in \mathbb{F}_k^4, x_\ell = 1} \overline{\alpha_x}^{(i)} \alpha_x{}^{(j)} = \delta_{ij} \kappa_{k,\ell,1} \tag{3.4}$$

$$\sum_{x \in \mathbb{F}_k^4, x_\ell = 0} \overline{\alpha_x}^{(i)} \alpha_x{}^{(j)} = \delta_{ij} \kappa_{k,\ell,0} \tag{3.5}$$

for any i, j and ℓ. We will find the fixed weight k with using the above two equations.

Now, let $k = 0$. Then, $c_i = \alpha_{0000}{}^{(i)}|0000\rangle$ and $c_j = \alpha_{0000}{}^{(j)}|0000\rangle$.

$$\sum_{x \in \mathbb{F}_0^4, x_\ell = 0} \overline{\alpha_x}^{(i)} \alpha_x{}^{(j)} = \delta_{ij} \kappa_{0,\ell,0}.$$

Since we have at least two orthonormal basis c_i and c_j, we can evaluate above equation for $i \neq j$. Then we have,

$$\overline{\alpha_{0000}}^{(i)} \alpha_{0000}{}^{(j)} = 0.$$

That means, $\overline{\alpha_{0000}}^{(i)}$ or $\alpha_{0000}{}^{(j)}$ is equal to 0. However, if one the components is 0, then there is no such c_i or c_j. Here, we get a contradiction. So, k must be different than 0.

Let $k = 4$. We use similar arguments as in the case $k = 0$. If $k = 4$, then $c_i = \alpha_{1111}{}^{(i)}|1111\rangle$ and $c_j = \alpha_{1111}{}^{(j)}|1111\rangle$.

$$\sum_{x \in \mathbb{F}_4^4, x_\ell = 1} \overline{\alpha_x}^{(i)} \alpha_x{}^{(j)} = \delta_{ij} \kappa_{4,\ell,1}.$$

For the basis c_i and c_j, we will evaluate above equation for $i \neq j$. Then, we have

$$\overline{\alpha_{1111}}^{(i)} \alpha_{1111}{}^{(j)} = 0.$$

Here, $\overline{\alpha_{1111}}^{(i)}$ or $\alpha_{1111}{}^{(j)}$ must be equal 0. But, if $\overline{\alpha_{1111}}^{(i)}$ or $\alpha_{1111}{}^{(j)}$ is equal to 0, then c_i or c_j does not exist. This contradicts with our assumption that we have at least two basis. Hence, $k \neq 4$. Now, we have three possibilities, that is $k \in \{1,2,3\}$.

We consider the case when $k = 1$. Then we have following basis

$$c_i = \alpha_{0001}{}^{(i)}|0001\rangle + \alpha_{0010}{}^{(i)}|0010\rangle + \alpha_{0100}{}^{(i)}|0100\rangle + \alpha_{1000}{}^{(i)}|1000\rangle,$$

$$c_j = \alpha_{0001}{}^{(j)}|0001\rangle + \alpha_{0010}{}^{(j)}|0010\rangle + \alpha_{0100}{}^{(j)}|0100\rangle + \alpha_{1000}{}^{(j)}|1000\rangle.$$

From Equation (3.4),

$$\sum_{x \in \mathbb{F}_1^4, x_\ell = 1} \overline{\alpha_x}^{(i)} \alpha_x{}^{(j)} = \delta_{ij} \kappa_{1,\ell,1}. \tag{3.6}$$

Let $\ell = 1$ in Equation (3.6). Hence, we have

$$\sum_{x \in \mathbb{F}_1^4, x_1 = 1} \overline{\alpha_x}^{(i)} \alpha_x{}^{(j)} = \delta_{ij} \kappa_{1,1,1}.$$

For $i = j$,

$$\overline{\alpha_{1000}}^{(i)} \alpha_{1000}{}^{(i)} = \kappa_{1,1,1}.$$

Since $\kappa_{1,1,1}$ is a nonzero constant, $\alpha_{1000}{}^{(i)} = \alpha_{1000}{}^{(j)} \neq 0$. For the cases $\ell = 2, 3, 4$, we have the following equations

$$\overline{\alpha_{0100}}^{(i)} \alpha_{0100}{}^{(i)} = \kappa_{1,2,1},$$

$$\overline{\alpha_{0010}}^{(i)} \alpha_{0010}{}^{(i)} = \kappa_{1,3,1},$$

$$\overline{\alpha_{0001}}^{(i)} \alpha_{0001}{}^{(i)} = \kappa_{1,4,1}.$$

As $\kappa_{1,\ell,1}$ is a nonzero constant, $\alpha_{0100}{}^{(i)}, \alpha_{0010}{}^{(i)}$ and $\alpha_{0001}{}^{(i)}$ are not equal to 0 for any i.

For $i \neq j$ in Equation (3.6), we have

$$\overline{\alpha_{0001}}^{(i)} \alpha_{0001}{}^{(j)} + \overline{\alpha_{0010}}^{(i)} \alpha_{0010}{}^{(j)} + \overline{\alpha_{0100}}^{(i)} \alpha_{0100}{}^{(j)} + \overline{\alpha_{1000}}^{(i)} \alpha_{1000}{}^{(j)} = 0 \quad (3.7)$$

Let $i \neq j$ and evaluate Equation (3.6) for $\ell = 1, 2, 3, 4$.

$$\overline{\alpha_{1000}}^{(i)} \alpha_{1000}{}^{(j)} = 0, \qquad \overline{\alpha_{0100}}^{(i)} \alpha_{0100}{}^{(j)} = 0,$$

$$\overline{\alpha_{0010}}^{(i)} \alpha_{0010}{}^{(j)} = 0, \qquad \overline{\alpha_{0001}}^{(i)} \alpha_{0001}{}^{(j)} = 0.$$

That is a contradiction since $\alpha_{1000}{}^{(i)}$, $\alpha_{0100}{}^{(i)}, \alpha_{0010}{}^{(i)}$, $\alpha_{0001}{}^{(i)}, \alpha_{1000}{}^{(j)}$, $\alpha_{0100}{}^{(j)}$, $\alpha_{0010}{}^{(j)}$, and $\alpha_{0001}{}^{(j)}$ are not equal to 0. Therefore, $k \neq 1$.

We now consider the weight $k = 3$. Then we have following basis

$$c_i = \alpha_{0111}{}^{(i)}|0111\rangle + \alpha_{1011}{}^{(i)}|1011\rangle + \alpha_{1101}{}^{(i)}|1101\rangle + \alpha_{1110}{}^{(i)}|1110\rangle,$$

$$c_j = \alpha_{0111}{}^{(j)}|0111\rangle + \alpha_{1011}{}^{(j)}|1011\rangle + \alpha_{1101}{}^{(j)}|1101\rangle + \alpha_{1110}{}^{(j)}|1110\rangle.$$

From Equation (3.5),

$$\sum_{x \in \mathbb{F}_3^4, x_\ell = 0} \overline{\alpha_x}^{(i)} \alpha_x{}^{(j)} = \delta_{ij} \kappa_{3,\ell,0} \quad (3.8)$$

Let $\ell = 1$ in Equation (3.8). Hence, we have

$$\sum_{x\in\mathbb{F}_3^4, x_1=0} \overline{\alpha_x}^{(i)} \alpha_x{}^{(j)} = \delta_{ij}\kappa_{3,1,0}.$$

For $i = j$,

$$\overline{\alpha_{0111}}^{(i)} \alpha_{0111}{}^{(i)} = \kappa_{3,1,0}.$$

Since $\kappa_{3,1,0}$ is a nonzero constant, $\alpha_{0111}{}^{(i)} = \alpha_{0111}{}^{(j)} \neq 0$. For the cases $\ell = 2, 3, 4$, we have the following equations

$$\overline{\alpha_{1011}}^{(i)} \alpha_{1011}{}^{(i)} = \kappa_{3,2,0},$$

$$\overline{\alpha_{1101}}^{(i)} \alpha_{1101}{}^{(i)} = \kappa_{3,3,0},$$

$$\overline{\alpha_{1110}}^{(i)} \alpha_{1110}{}^{(i)} = \kappa_{3,4,0}.$$

As $\kappa_{3,\ell,0}$ is a nonzero constant, $\alpha_{1011}{}^{(i)}$, $\alpha_{1101}{}^{(i)}$, and $\alpha_{1110}{}^{(i)}$ are not equal to 0 for any i.

For $i \neq j$ in Equation (3.8), we have

$$\overline{\alpha_{0111}}^{(i)} \alpha_{0111}{}^{(j)} + \overline{\alpha_{1011}}^{(i)} \alpha_{1011}{}^{(j)} + \overline{\alpha_{1101}}^{(i)} \alpha_{1101}{}^{(j)} + \overline{\alpha_{1110}}^{(i)} \alpha_{1110}{}^{(j)} = 0. \quad (3.9)$$

Let $i \neq j$ and evaluate Equation (3.8) for $\ell = 1, 2, 3, 4$.

$$\overline{\alpha_{0111}}^{(i)} \alpha_{0111}{}^{(j)} = 0, \qquad \overline{\alpha_{1011}}^{(i)} \alpha_{1011}{}^{(j)} = 0,$$

$$\overline{\alpha_{1101}}^{(i)} \alpha_{1101}{}^{(j)} = 0, \qquad \overline{\alpha_{1110}}^{(i)} \alpha_{1110}{}^{(j)} = 0.$$

That is the contradiction since $\alpha_{0111}{}^{(i)}$, $\alpha_{1011}{}^{(i)}$, $\alpha_{1101}{}^{(i)}$, $\alpha_{1110}{}^{(i)}$, $\alpha_{0111}{}^{(j)}$, $\alpha_{1011}{}^{(j)}$, $\alpha_{1101}{}^{(j)}$ and $\alpha_{1110}{}^{(j)}$ are not equal to 0. Therefore, $k \neq 3$.

Hence, if there exist such a jump code, then the only possible weight k is equal to 2. That means that the decoherence-free subspace $\mathbb{W}_k$ have the weight 2, i.e. $\mathbb{W}_2$. Now, we consider the case when $k = 2$.

Therefore, for a code word $|c\rangle = \sum_{x\in\mathbb{F}_k^4} \alpha_x |x\rangle$,

$$\alpha_{0000}{}^{(i)} = 0, \qquad \alpha_{0001}{}^{(i)} = \alpha_{0010}{}^{(i)} = \alpha_{0100}{}^{(i)} = \alpha_{1000}{}^{(i)} = 0,$$

$$\alpha_{1111}{}^{(i)} = 0, \qquad \alpha_{1110}{}^{(i)} = \alpha_{1101}{}^{(i)} = \alpha_{1011}{}^{(i)} = \alpha_{0111}{}^{(i)} = 0.$$

Let $k = 2$, then we have following basis,

$$c_i = \alpha_{0011}{}^{(i)}|0011\rangle + \alpha_{0101}{}^{(i)}|0101\rangle + \alpha_{0110}{}^{(i)}|0110\rangle + \alpha_{1001}{}^{(i)}|1001\rangle + \alpha_{1010}{}^{(i)}|1010\rangle + \alpha_{1100}{}^{(i)}|1100\rangle,$$

$$c_j = \alpha_{0011}{}^{(j)}|0011\rangle + \alpha_{0101}{}^{(j)}|0101\rangle + \alpha_{0110}{}^{(j)}|0110\rangle + \alpha_{1001}{}^{(j)}|1001\rangle + \alpha_{1010}{}^{(j)}|1010\rangle + \alpha_{1100}{}^{(j)}|1100\rangle.$$

We obtain the following equations from Equations (3.4) and (3.5) for any i and j,

$$\overline{\alpha_{1100}}^{(i)}\alpha_{1100}{}^{(j)} + \overline{\alpha_{1010}}^{(i)}\alpha_{1010}{}^{(j)} + \overline{\alpha_{1001}}^{(i)}\alpha_{1001}{}^{(j)} = \delta_{ij}\kappa_{2,1,1}, \tag{3.10}$$

$$\overline{\alpha_{1100}}^{(i)}\alpha_{1100}{}^{(j)} + \overline{\alpha_{0110}}^{(i)}\alpha_{0110}{}^{(j)} + \overline{\alpha_{0101}}^{(i)}\alpha_{0101}{}^{(j)} = \delta_{ij}\kappa_{2,2,1}, \tag{3.11}$$

$$\overline{\alpha_{1010}}^{(i)}\alpha_{1010}{}^{(j)} + \overline{\alpha_{0110}}^{(i)}\alpha_{0110}{}^{(j)} + \overline{\alpha_{0011}}^{(i)}\alpha_{0011}{}^{(j)} = \delta_{ij}\kappa_{2,3,1}, \tag{3.12}$$

$$\overline{\alpha_{1001}}^{(i)}\alpha_{1001}{}^{(j)} + \overline{\alpha_{0101}}^{(i)}\alpha_{0101}{}^{(j)} + \overline{\alpha_{0011}}^{(i)}\alpha_{0011}{}^{(j)} = \delta_{ij}\kappa_{2,4,1}, \tag{3.13}$$

$$\overline{\alpha_{0011}}^{(i)}\alpha_{0011}{}^{(j)} + \overline{\alpha_{0101}}^{(i)}\alpha_{0101}{}^{(j)} + \overline{\alpha_{0110}}^{(i)}\alpha_{0110}{}^{(j)} = \delta_{ij}\kappa_{2,1,0}, \tag{3.14}$$

$$\overline{\alpha_{0011}}^{(i)}\alpha_{0011}{}^{(j)} + \overline{\alpha_{1001}}^{(i)}\alpha_{1001}{}^{(j)} + \overline{\alpha_{1010}}^{(i)}\alpha_{1010}{}^{(j)} = \delta_{ij}\kappa_{2,2,0}, \tag{3.15}$$

$$\overline{\alpha_{0101}}^{(i)}\alpha_{0101}{}^{(j)} + \overline{\alpha_{1001}}^{(i)}\alpha_{1001}{}^{(j)} + \overline{\alpha_{1100}}^{(i)}\alpha_{1100}{}^{(j)} = \delta_{ij}\kappa_{2,3,0}, \tag{3.16}$$

$$\overline{\alpha_{0110}}^{(i)}\alpha_{0110}{}^{(j)} + \overline{\alpha_{1010}}^{(i)}\alpha_{1010}{}^{(j)} + \overline{\alpha_{1100}}^{(i)}\alpha_{1100}{}^{(j)} = \delta_{ij}\kappa_{2,4,0}. \tag{3.17}$$

We now solve these equations for $i = j$ and $i \neq j$.

First, let $i \neq j$. Then, from Equations (3.10) and (3.15) we have,

$$\overline{\alpha_{1100}}^{(i)}\alpha_{1100}{}^{(j)} = \overline{\alpha_{0011}}^{(i)}\alpha_{0011}{}^{(j)}. \tag{3.18}$$

From Equations (3.10) and (3.16) we have,

$$\overline{\alpha_{1010}}^{(i)}\alpha_{1010}{}^{(j)} = \overline{\alpha_{0101}}^{(i)}\alpha_{0101}{}^{(j)}. \tag{3.19}$$

From Equations (3.10) and (3.17) we have,

$$\overline{\alpha_{1001}}^{(i)}\alpha_{1001}{}^{(j)} = \overline{\alpha_{0110}}^{(i)}\alpha_{0110}{}^{(j)}. \tag{3.20}$$

From Equations (3.10), (3.15), (3.16) and (3.17) we have,

$$\overline{\alpha_{1100}}^{(i)}\alpha_{1100}{}^{(j)} + \overline{\alpha_{1010}}^{(i)}\alpha_{1010}{}^{(j)} + \overline{\alpha_{1001}}^{(i)}\alpha_{1001}{}^{(j)} = 0.$$

Now, let $i = j$. Then, from Equations (3.10) and (3.15) we have,

$$\left|\alpha_{1100}{}^{(i)}\right| = \left|\alpha_{0011}{}^{(i)}\right| = \mathbb{c}_1{}^{(i)}. \quad (3.21)$$

From Equations (3.10) and (3.16) we have,

$$\left|\alpha_{1010}{}^{(i)}\right| = \left|\alpha_{0101}{}^{(i)}\right| = \mathbb{c}_2{}^{(i)}. \quad (3.22)$$

From Equations (3.10) and (3.17) we have,

$$\left|\alpha_{1001}{}^{(i)}\right| = \left|\alpha_{0110}{}^{(i)}\right| = \mathbb{c}_3{}^{(i)}. \quad (3.23)$$

From Equations (3.10), (3.15), (3.16) and (3.17) we have,

$$\mathbb{c}_1{}^{(i)^2} + \mathbb{c}_2{}^{(i)^2} + \mathbb{c}_3{}^{(i)^2} = \tau$$

where $\mathbb{c}_1{}^{(i)}, \mathbb{c}_2{}^{(i)}, \mathbb{c}_3{}^{(i)}$ and τ are constant numbers.

In particular, to maximize the dimension of the jump code, let $\alpha_{1100}{}^{(i)} = \alpha_{0011}{}^{(i)}$ in Equation (3.18), $\alpha_{1010}{}^{(i)} = \alpha_{0101}{}^{(i)}$ in Equation (3.19), $\alpha_{1001}{}^{(i)} = \alpha_{0110}{}^{(i)}$ in Equation (3.20) for any i and let $\alpha_{1100}{}^{(i)} = \alpha_{0011}{}^{(i)} = 1$ for $i = 1$, $\alpha_{1010}{}^{(i)} = \alpha_{0101}{}^{(i)}$ for $i = 2$, $\alpha_{1001}{}^{(i)} = \alpha_{0110}{}^{(i)}$ for $i = 3$ otherwise all coefficients are 0. Then,

$$|c_1\rangle = \frac{1}{\sqrt{2}}(|1100\rangle + |0011\rangle),$$

$$|c_2\rangle = \frac{1}{\sqrt{2}}(|1010\rangle + |0101\rangle),$$

$$|c_3\rangle = \frac{1}{\sqrt{2}}(|1001\rangle + |0110\rangle)$$

is an example of a 1-error correcting quantum jump code of length 4 with the normalizing constant $\frac{1}{\sqrt{2}}$, i.e. $(4, 3, 1)_2$ jump code.

3.2.5.2 A 1-error Correcting Quantum Jump Code of Length Six

We now consider an example of 1-error correcting jump code C of length six. For some constant weight k, $0 \le k \le 6$, any code word $|c\rangle$ can be represented by

$$|c\rangle = \sum_{x\in\mathbb{F}_k^6} \alpha_x |x\rangle.$$

We define an orthonormal basis of $\mathcal{C}$ as follows,

$$\left\{c_i = \sum_{x\in\mathbb{F}_k^6} \alpha_x{}^{(i)} |x\rangle : i = 1, 2, \dots, m\right\}.$$

A $(6, 5, 1)_2$ jump code is given with the following orthonormal bases

$$|c_1\rangle = \frac{1}{\sqrt{3}}(|110000\rangle + |001001\rangle + |000110\rangle),$$

$$|c_2\rangle = \frac{1}{\sqrt{3}}(|101000\rangle + |010100\rangle + |000011\rangle),$$

$$|c_3\rangle = \frac{1}{\sqrt{3}}(|100100\rangle + |001010\rangle + |010001\rangle),$$

$$|c_4\rangle = \frac{1}{\sqrt{3}}(|100010\rangle + |011000\rangle + |000101\rangle),$$

$$|c_5\rangle = \frac{1}{\sqrt{3}}(|100001\rangle + |001100\rangle + |010010\rangle).$$

Actually, these orthonormal bases form a $(6, 5, 1)_2$ jump code because Knill-Laflamme Theorem holds for any orthonormal basis and the jump code is a subspace of $\mathbb{W}_2$.

3.2.5.3 A 2-error Correcting Quantum Jump Code of Length Six

Let an orthonormal basis of a 2-error correcting jump code of length six is given by

$$\left\{c_i = \sum_{x\in\mathbb{F}_k^6} \alpha_x{}^{(i)} |x\rangle : i = 1, 2, \dots, m\right\}.$$

Let $E = \{\ell_1, \ell_2\}$ where ℓ_1 and ℓ_2 denotes the positions of quantum jump errors. We define P_E matrix as a 6×6 diagonal matrix in which the all diagonal entries are 1 except for the positions ℓ_1 and ℓ_2 being 0.

If there are some x such that $supp(x) \supset E$ and $\alpha_x{}^{(i)} \neq 0$, we have

$$\mathcal{J}_E|c_i\rangle = \sum_{x\in\mathbb{F}_k^6} \alpha_x{}^{(i)} \mathcal{J}_E|x\rangle = \sum_{x\in\mathbb{F}_k^6, x_\ell = 1 \text{ for } \ell\in E} \alpha_x{}^{(i)} |P_\ell x\rangle.$$

Therefore,

$$\langle c_i|\mathcal{J}_E^\dagger \mathcal{J}_E|c_j\rangle = \sum_{x\in\mathbb{F}_k^6, x_\ell=1 \text{ for } \ell\in E} \overline{\alpha_x}^{(i)} \alpha_x{}^{(j)} = \delta_{ij}\kappa_E \tag{3.24}$$

where κ_E is a nonzero constant which depends on E.

From Equation (3.24), we can find that the decoherence-free subspace $\mathbb{W}_k$ is $\mathbb{W}_3$. Hence, $\overline{\alpha_x}^{(i)} = 0$ for any x which have weight $k = 0, 1, 2, 4, 5, 6$.

Then, we have a $(6, 2, 2)_3$ jump code with the following orthonormal basis

$$|c_1\rangle = \frac{1}{\sqrt{10}}(|111000\rangle + |101100\rangle + |100110\rangle + |100011\rangle + |110001\rangle + |011010\rangle + |001101\rangle + |010110\rangle + |001011\rangle + |010101\rangle),$$

$$|c_2\rangle = \frac{1}{\sqrt{10}}(|000111\rangle + |010011\rangle + |011001\rangle + |011100\rangle + |001110\rangle + |100101\rangle + |110010\rangle + |101001\rangle + |110100\rangle + |101010\rangle).$$

Equation (3.24) holds for any $E \subset V$ where $|E| \leq 2$.

In particular; let $E = \{3, 4\}$. Then, we have

$$\mathcal{J}_E|c_1\rangle = \frac{1}{\sqrt{10}}(|100000\rangle + |000001\rangle),$$

$$\mathcal{J}_E|c_2\rangle = \frac{1}{\sqrt{10}}(|010000\rangle + |000010\rangle).$$

Here, for $i \in \{1\ 2\}$, $\langle c_i|\mathcal{J}_E{}^\dagger \mathcal{J}_E|c_i\rangle = \frac{1}{5}$ and $\langle c_1|\mathcal{J}_E{}^\dagger \mathcal{J}_E|c_2\rangle = \langle c_2|\mathcal{J}_E{}^\dagger \mathcal{J}_E|c_1\rangle = 0$ holds. Changing the elements of E where $|E| = 2$, does not change that $\mathcal{J}_E|c_i\rangle$ have two vectors in the basis.

Let $E = \{1\}$. Then, we have

$$\mathcal{J}_E|c_1\rangle = \frac{1}{\sqrt{10}}(|011000\rangle + |001100\rangle + |000110\rangle + |000011\rangle + |010001\rangle),$$

$$\mathcal{J}_E|c_2\rangle = \frac{1}{\sqrt{10}}(|000101\rangle + |010010\rangle + |001001\rangle + |010100\rangle + |001010\rangle).$$

Here, for $i \in \{1, 2\}$, $\langle c_i|\mathcal{J}_E{}^\dagger \mathcal{J}_E|c_i\rangle = \frac{1}{2}$ and $\langle c_1|\mathcal{J}_E{}^\dagger \mathcal{J}_E|c_2\rangle = \langle c_2|\mathcal{J}_E{}^\dagger \mathcal{J}_E|c_1\rangle = 0$ holds. Also, same as the above example where $|E| = 2$, we can see that if $|E| = 1$ then $\mathcal{J}_E|c_i\rangle$ have five vectors in the basis.

If $E = \emptyset$, then we have

$$\mathcal{J}_E|c_1\rangle = |c_1\rangle, \qquad \mathcal{J}_E|c_2\rangle = |c_2\rangle.$$

Computing $\langle c_i|\mathcal{J}_E{}^{\dagger}\mathcal{J}_E|c_i\rangle$ gives 1 as the result.

For this example, we can generalize the inner product $\langle c_i|\mathcal{J}_E{}^{\dagger}\mathcal{J}_E|c_j\rangle$ as follows

$$\langle c_i|\mathcal{J}_E{}^{\dagger}\mathcal{J}_E|c_j\rangle = \begin{cases} \frac{1}{5}, & if\ i = j\ and\ |E| = 2, \\ \frac{1}{2}, & if\ i = j\ and\ |E| = 1, \\ 1, & if\ i = j\ and\ E = \emptyset, \\ 0, & if\ i \neq j. \end{cases} \tag{3.25}$$

CHAPTER 4

t-SPONTANEOUS EMISSION ERROR DESIGN

In this chapter, we will show that e-error correcting jump codes and t-designs have a very close connection. As mentioned before quantum jump code is a type of quantum error correcting codes. Alber *et al*. [22] introduced quantum jump codes in 2001. In the following years, Beth *et al*. [23] proposed a new class of combinatorial designs to construct quantum jump codes. This new class named as *t-spontaneous emission error design*, abbreviated as *t-SEED*.

4.1 A t-SEED and a Jump Code

We defined an n-qubit ket vector $|c\rangle$ as a superposition of vectors in $\mathbb{F}^n$, that is, $|c\rangle = \sum_{x\in\mathbb{F}^n} {\alpha_x}^{(i)}|x\rangle$. Here, the coefficients ${\alpha_x}^{(i)}$ of $|c\rangle$ are elements of complex numbers. If we restrict the values of ${\alpha_x}^{(i)}$ to α and 0, where α is a normalizing constant, we can see that the combinatorial structure of quantum jump codes are very similar to combinatorial designs.

Any ket vector $|c\rangle$ is represented by $|c\rangle = \sum_{x\in\mathbb{F}^n} \alpha_x|x\rangle$. We define support of a vector $x = (x_1, x_2, \dots, x_n) \in \mathbb{F}^n$ as $B = supp(x) = \{i : x_i = 1\}$.

To see the combinatorial structure of quantum jump codes, we identify the states as follows;

$$|c_i\rangle = \left|\mathfrak{B}^{(i)}\right\rangle = \frac{1}{\sqrt{|\mathfrak{B}^{(i)}|}} \sum_{B\in\mathfrak{B}^{(i)}} |B\rangle$$

where $\mathfrak{B}^{(i)} = \left\{supp(x) : {\alpha_x}^{(i)} \neq 0\right\}$.

These orthonormal states c_i's span an e-error correcting quantum jump code $\mathcal{C} = (n, m, e)_k$. Let E be the sets of quantum jump positions where $|E| \leq e$. Then for all sets $\mathcal{B}^{(i)}$ the following multiplicity condition holds:

$$\frac{\left|\left\{B \in \mathfrak{B}^{(i)} : E \subseteq B\right\}\right|}{|\mathfrak{B}^{(i)}|} = \lambda_E.$$

If the sets $\mathcal{B}^{(i)}$ are all disjoint then above condition corresponds to Knill-Laflamme Theorem with the condition $i \neq j$. To obtain the case $i = j$, we define $\mathcal{J}_E^{\dagger}\mathcal{J}_E = \sum_{B \supseteq E} |x\rangle\langle x|$. Then $\langle c_i|\mathcal{J}_E{}^{\dagger}\mathcal{J}_E|c_i\rangle$ equals to λ_E. For a better understanding, the reader can check Equation (3.25) in the example of 1-error correcting quantum jump code of length six.

Here, since any quantum jump code has a fixed weight k, we are interested with the k-subsets of an n-set.

We continue with the definition of t-spontaneous emission error design.

Definition 4.1 A system $\left(V;\, \mathfrak{B}^{(1)}, \dots, \mathfrak{B}^{(m)}\right)$ is called a *t-spontaneous emission error design*, shortly $t-(n,k;m)$-*SEED* where $|V| = n$, if the following properties holds

(i) $|B| = k$ holds for any $B \in \mathfrak{B}^{(i)}$,

(ii) For any $\mathfrak{B}^{(i)}$ and $\mathfrak{B}^{(j)}$,where $i \neq j$, $\mathfrak{B}^{(i)} \cap \mathfrak{B}^{(j)} = \emptyset$,

(iii) $\frac{\left|\left\{B \in \mathcal{B}^{(i)} : E \subseteq B\right\}\right|}{|\mathcal{B}^{(i)}|} = \frac{\lambda_i(T)}{|\mathcal{B}^{(i)}|} = \lambda_E$ holds for $E \subset V$, $|E| \leq t$, where λ_E is a constant depending on only E not i.

Indeed, Condition (i) represents the fixed weight k of a jump code. Second condition is equal to the orthogonality of basis of quantum jump code. Condition (iii) is the multiplicity condition as mentioned before. The parameter m is called the dimension of t-*SEED*.

Example 4.1 Let $V = \{1,2,3,4,5,6\}$ and $k = 3$. A $2-(6,3;2)$-*SEED* is given as follows.

$$\mathfrak{B}^{(1)} = \{123, 134, 145, 156, 126, 246, 235, 346, 246, 356\},$$

$$\mathfrak{B}^{(2)} = \{124, 135, 146, 125, 136, 234, 345, 456, 256, 236\}.$$

Here, $|B| = 3$ holds for any $B \in \left\{\mathfrak{B}^{(1)}, \mathfrak{B}^{(2)}\right\}$ and $\mathfrak{B}^{(1)} \cap \mathfrak{B}^{(2)} = \emptyset$. For Condition (iii), $\lambda_E = \frac{1}{5}$ and $\lambda_i(T) = 2$.

Indeed, this $2-(6,3;2)$-*SEED* is the $(6,2,2)_3$ jump code constructed in previous chapter. A $(6,2,2)_3$ jump code is given with the following orthonormal basis

$$|c_1\rangle = \frac{1}{\sqrt{10}}(|111000\rangle + |101100\rangle + |100110\rangle + |100011\rangle + |110001\rangle + |011010\rangle + |001101\rangle + |010110\rangle + |001011\rangle + |010101\rangle),$$

$$|c_2\rangle = \frac{1}{\sqrt{10}}(|000111\rangle + |010011\rangle + |011001\rangle + |011100\rangle + |001110\rangle + |100101\rangle + |110010\rangle + |101001\rangle + |110100\rangle + |101010\rangle).$$

By the above example, we can easily see the connection between t-*SEED*s and quantum jump codes. By taking blocks of $\mathfrak{B}^{(i)}$'s as the supports of vectors in $|c_i\rangle$, we can construct the quantum jump code. Also, this t-*SEED* is the large set of $2-(6,3,2)$ designs given in the *Example 2.29*.

Example 4.2 Let $V = \{1,2,3,4,5,6,7,8,9\}$ and $k = 3$. A $2-(9,3;3)$-*SEED* is given as follows.

$$\mathfrak{B}^{(1)} = \{123, 456, 789, 168, 249, 357, 159, 267, 348\},$$

$$\mathfrak{B}^{(2)} = \{135, 279, 468, 189, 234, 567, 126, 378, 459\},$$

$$\mathfrak{B}^{(3)} = \{138, 246, 579, 129, 345, 678, 156, 237, 489\}.$$

In this example, each $\mathfrak{B}^{(i)}$ is a $2-(9,3,1)$ design. Here, the corresponding jump code $(9,3,2)_3$ is given with the following basis.

$$|c_1\rangle = \frac{1}{3}(|111000000\rangle + |000111000\rangle + |000000111\rangle + |100001010\rangle + |010100001\rangle + |001010100\rangle + |100010001\rangle + |010001100\rangle + |001100010\rangle),$$

$$|c_2\rangle = \frac{1}{3}(|101010000\rangle + |010000101\rangle + |000101010\rangle + |100000011\rangle + |011100000\rangle + |000011100\rangle + |110001000\rangle + |001000110\rangle + |000110001\rangle),$$

$$|c_3\rangle = \frac{1}{3}(|101000010\rangle + |010101000\rangle + |000010101\rangle + |110000001\rangle + |001110000\rangle + |000001110\rangle + |100011000\rangle + |011000100\rangle + |000100011\rangle).$$

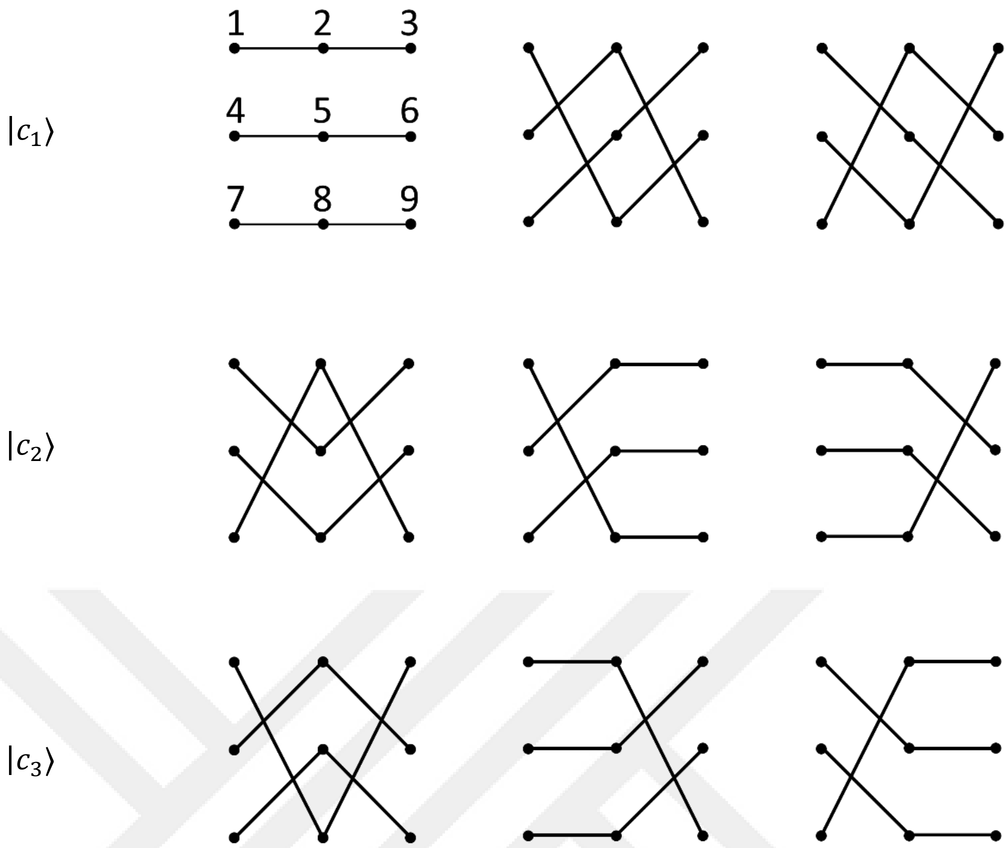


Figure 4. 1 A $2-(9,3;\ 3)$-*SEED*

Example 4.3 Let $V_1 = \{0,1,2,3\}$, $V_2 = \{a,b,c,d\}$ and $V = V_1 \cup V_2$. Then $\left(V;\ \mathfrak{B}^{(1)}, \mathfrak{B}^{(2)}, \mathfrak{B}^{(3)}\right)$ is a $3-(8,4;3)$-*SEED* where

$$\mathfrak{B}^{(1)} = \{01ab, 01cd, 23ab, 23cd, 02ac, 02bd, 13ac, 13bd, 03ad, 03bc, 12ad, 12bc\},$$

$$\mathfrak{B}^{(2)} = \{01ac, 01bd, 23ac, 23bd, 02ad, 02bc, 13ad, 13bc, 03ab, 03cd, 12ab, 12cd\},$$

$$\mathfrak{B}^{(3)} = \{01ad, 01bc, 23ad, 23bc, 02ab, 02cd, 13ab, 13cd, 03ac, 03bd, 12ac, 12bd\}.$$

Here, each $\mathfrak{B}^{(i)}$ is a Steiner quadruple system of order 8, and they are all disjoint.

Example 4.4 Any $t-(n,k,\lambda)$ design is a $t-(n,k;1)$-*SEED*. Since in a $t-(n,k,\lambda)$ design the block size is k and the multiplicity condition for a t-*SEED*, $\lambda_i(T) = \lambda_E$, holds.

Lemma 4.2 Let $\left(V, \mathfrak{B}^{(i)}\right)$ be a $t-(v,k,\lambda_i)$ design for every $1 \le i \le m$. If $\mathfrak{B}^{(i)} \cap \mathfrak{B}^{(j)} = \emptyset$ for all $1 \le i < j \le m$, then $\left\{\left(V, \mathfrak{B}^{(i)}\right) : 1 \le i \le m\right\}$ forms a $t-(v,k;m)$-*SEED*.

Proof. For any $E \subseteq X$, $|E| = t$, and $1 \le i \le m$, we have

$$\lambda_E = \frac{\left|\left\{B \in \mathfrak{B}^{(i)} \ : \ E \subseteq B\right\}\right|}{|\mathfrak{B}^{(i)}|} = \frac{\lambda_i}{\lambda_i \binom{v}{t}/\binom{k}{t}} = \frac{\binom{k}{t}}{\binom{v}{t}}.$$

So λ_E is a constant depending on the parameters t, k, and v. In the same way, by *Theorem 2.5*, we know that any t-design can be regarded as an i-design for $1 \leq i \leq t-1$, and we also know that λ_E is also a constant which depends on only the size of E for any $E \subseteq X$, $|E| = i < t$. Since all m designs are disjoint, they form a $t-(v,k;\ m)$-*SEED*.

Example 4.5 A $2-(7,3;3)$-*SEED*, $\left(V;\ \mathfrak{B}^{(1)}, \mathfrak{B}^{(2)}, \mathfrak{B}^{(3)}\right)$, is given below.

$$\mathfrak{B}^{(1)} = \{013, 124, 235, 346, 045, 156, 026\},$$

$$\mathfrak{B}^{(2)} = \{023, 134, 245, 356, 046, 015, 126\},$$

$$\mathfrak{B}^{(3)} = \left\{\begin{matrix} 024, 135, 246, 035, 146, 025, 136, 012, 123, 234, \\ 345, 456, 056, 016, 014, 125, 236, 034, 145, 256, 036 \end{matrix}\right\}.$$

Here, $\mathfrak{B}^{(1)}$ and $\mathfrak{B}^{(2)}$ are two $2-(7,3,1)$ designs, and $\mathfrak{B}^{(3)}$ is a $2-(7,3,3)$ design. Also, $\mathfrak{B}^{(i)} \cap \mathfrak{B}^{(j)} = \emptyset$ holds for any $i, j \in \{1,2,3\}$. In *Section 2.5*, it is stated that there exist only two disjoint $2-(7,3,1)$ designs. We can see that, $\binom{v}{k}/\left\{\mathfrak{B}^{(1)} \cup \mathfrak{B}^{(2)}\right\}$ forms a $2-(7,3,3)$ design. This $2-(7,3;3)$-*SEED* corresponds to a $(7,3,2)_3$ jump code.

Note. [53] There is no $2-(7,3;m)$-*SEED* for any $m \geq 4$.

Corollary 4.3 If there exist m mutually disjoint simple $t-(n,k,\lambda)$ designs, then there exists a $t-(n,k;m)$-$SEED$.

Some results are given in *Table 2 (Section 4.2)* for *Corollary 4.3*.

If m is equal to the parameter N in large set notation, $t-(n,k;m)$-$SEED$ is equal to large set of $t-(n,k,\lambda)$ designs.

Example 4.6 A $2-(9,3;7)$-*SEED*, $\left(V; \mathfrak{B}^{(1)}, \dots, \mathfrak{B}^{(7)}\right)$, is given by

$$\mathfrak{B}^{(1)} = \{123, 147, 258, 369, 159, 267, 348, 168, 249, 357, 456, 789\},$$

$$\mathfrak{B}^{(2)} = \{124, 235, 136, 157, 268, 349, 189, 279, 378, 458, 569, 467\},$$

$$\mathfrak{B}^{(3)} = \{125, 236, 134, 169, 247, 358, 178, 289, 379, 459, 567, 468\},$$

$$\mathfrak{B}^{(4)} = \{126, 234, 135, 148, 259, 367, 179, 278, 389, 457, 568, 469\},$$

$$\mathfrak{B}^{(5)} = \{127, 238, 139, 146, 245, 356, 158, 269, 347, 489, 579, 678\},$$

$$\mathfrak{B}^{(6)} = \{128, 239, 137, 149, 257, 368, 156, 246, 345, 478, 589, 679\},$$

$$\mathfrak{B}^{(7)} = \{129, 237, 138, 145, 256, 345, 167, 248, 359, 479, 578, 689\}.$$

Here, indeed, each $\mathfrak{B}^{(i)}$ corresponds to a $2-(9,3,1)$ design and $\mathfrak{B}^{(i)} \cap \mathfrak{B}^{(j)} = \emptyset$ for any $i, j \in \{1,2,3,4,5,6,7\}$. This $2-(9,3;7)$-*SEED* is equivalent to a large set of 7 disjoint $2-(9,3,1)$ designs since all $\mathfrak{B}^{(i)}$ are disjoint and $N = \binom{v-t}{k-t}/\lambda = \binom{9-2}{3-2} = 7$ in large set notation. These designs can be constructed by using the methods given in *Theorem 2.40* and *Theorem 2.41*, with automorphism $\varphi = (123)(456)(789)$.

By using this $2-(9,3;7)$-*SEED*, we can construct a $(9,7,2)_3$ jump code. Two of the basis of this jump code is given below. Other five basis can be found by using $\mathfrak{B}^{(2)}, \mathfrak{B}^{(3)}, \mathfrak{B}^{(4)}, \mathfrak{B}^{(5)}, \mathfrak{B}^{(6)}$.

$$|c_1\rangle = \frac{1}{\sqrt{12}}(|111000000\rangle + |100100100\rangle + |010010010\rangle + |001001001\rangle + |100010001\rangle + |010001100\rangle + |001100010\rangle + |100001010\rangle + |010100001\rangle + |001010100\rangle + |000111000\rangle + |000000111\rangle),$$

$$\vdots$$

$$|c_7\rangle = \frac{1}{\sqrt{12}}(|110000001\rangle + |011000100\rangle + |101000010\rangle + |100110000\rangle + |010011000\rangle + |001110000\rangle + |100001100\rangle + |010100010\rangle + |001010001\rangle + |000100101\rangle + |000010110\rangle + |000001011\rangle).$$

Lemma 4.4 Let $(V, \mathfrak{B}_i)$, $1 \le i \le m$, be m simple $t-(n,k,\lambda)$ designs. If $\mathfrak{B}_i \cap \mathfrak{B}_j = \mathcal{A}$ for $1 \le i, j \le m$ and $i \ne j$, then there exists a $t-(n,k;m)$-$SEED$.

Proof. Let $\mathfrak{B}_i{}' = \mathfrak{B}_i \backslash \mathcal{A}$ for $1 \le i \le m$. We will show that $(V; \mathfrak{B}_1{}', \dots, \mathfrak{B}_m{}')$ is a $t-(n,k;m)$-$SEED$. For the first condition, $|B| = k$ holds for any $B \in \mathfrak{B}_i{}'$. For any $\mathfrak{B}_i{}'$ and $\mathfrak{B}_j{}'$, where $i \ne j$, $\mathfrak{B}_i{}' \cap \mathfrak{B}_j{}' = \emptyset$ holds. We now check the multiplicity condition, that is, $\frac{|\{B \in \mathfrak{B}_i{}' : E \subseteq B\}|}{|\mathfrak{B}_i{}'|} = \frac{\lambda_i(T)}{|\mathfrak{B}_i{}'|} = \lambda_E$ must be a constant for any choice of $E \subseteq V$ with $|E| = t$. Let $|E| = t$ and $|\mathcal{A}| = p$. If $E \nsubseteq A \in \mathcal{A}$, then $\frac{|\{B \in \mathfrak{B}_i{}' : E \subseteq B\}|}{|\mathfrak{B}_i{}'|} = \frac{\lambda}{\lambda\binom{v}{t}/\binom{k}{t} - p} = \lambda_E$ is a constant since E is contained in exactly λ blocks in B. If $E \subseteq A \in \mathcal{A}$, let $|\{A \in \mathcal{A} : E \subseteq A\}| = r$. Then, for any choice of $E \subseteq V$ with $|E| = t$, $\frac{|\{B \in \mathfrak{B}_i{}' : E \subseteq B\}|}{|\mathfrak{B}_i{}'|} = \frac{|\{B \in \mathfrak{B}_i : E \subseteq B\} / \{A \in \mathcal{A} : E \subseteq A\}|}{|\mathfrak{B}_i{}'|} = \frac{\lambda - r}{\lambda\binom{v}{t}/\binom{k}{t} - p}$ is a constant since E is contained in exactly λ blocks in $\mathfrak{B}_i$ and E is contained in exactly r blocks in $\mathcal{A}$. Therefore, $(V;\ \mathfrak{B}_1', \dots, \mathfrak{B}_m')$ forms a $t-(n,k;m)$-*SEED*.

The following lemma is an analogue of derived design of a t-design given in *Chapter 2*.

Lemma 4.5 [53] If $\left(V;\ \mathfrak{B}^{(1)}, \dots, \mathfrak{B}^{(m)}\right)$ is a $t-(n,k;m)$-*SEED*, then for any $p \in V$, $\left(V\backslash\{p\};\ \mathfrak{B}^{(1)'}, \dots, \mathfrak{B}^{(m)'}\right)$ is a $(t-1)-(n-1,k-1;m)$-*SEED*, where $\mathfrak{B}^{(i)'} = \left\{B\backslash\{p\} : p \in B \in \mathfrak{B}^{(i)}\right\}$.

Example 4.7 A large set $LS_\lambda(t,k,v)$ is an example of a $t-\left(v,k;\ \binom{v-t}{k-t}/\lambda\right)$-*SEED*.

Indeed, the parameter λ_E is the same as the ratio of occurrence of a particular subset T in each design $\mathfrak{B}^{(i)}$. Here, it can be seen that the conditions of a large set of a t-designs are more restrictive than the conditions of a t-*SEED*. Because, λ_E depends on the choice of T, but for a large set, $\lambda_i(T)$ only depends on the size of T. Therefore, if $\lambda_i(T)$ is a constant for any $T \in \binom{V}{t}$ then the t-*SEED* consists of t-designs. So, for $\lambda = \lambda_E$ and $|E| = t$, $\left(V, \mathfrak{B}^{(i)}\right)$ is a $t-(n,k,\lambda)$ design. As mentioned before; if $\lambda = 1$ in a t-design, then the design is called Steiner t-design and denoted by $S(t,k,n)$. Therefore, if $|\mathfrak{B}|$ is a constant and the union of all $\mathfrak{B}^{(i)}$'s is equal to all k-subset of n-set, then a t-*SEED* is called a large set of a $t-(n,k,\lambda)$ designs.

Example 4.8 There exists a $1-(q^2,q;q+1)$-*SEED* for all prime powers q.

As mentioned in *Subsection 2.2.3*, an affine plane is $2-(q^2,q,1)$ design and affine planes are 1-resolvable. There exists an affine plane for all prime powers q. Since each parallel class is a $1-(q^2,q,1)$ design, there exists a $(q^2,q+1,1)_q$ jump code where m is equal to number of parallel classes. Here, each parallel class corresponds to a basis of the jump code.

Example 4.9 In particular, taking $q=2$ in the previous example, we can construct a $1-(4,2;3)$-*SEED* and so a $(4,3,1)_2$ jump code. The orthonormal basis of this code is given below.

$$|c_1\rangle = \frac{1}{\sqrt{2}}(|1010\rangle + |0101\rangle),$$

$$|c_2\rangle = \frac{1}{\sqrt{2}}(|1100\rangle + |0011\rangle),$$

$$|c_3\rangle = \frac{1}{\sqrt{2}}(|1001\rangle + |0110\rangle).$$

The orthonormal basis of a $1-(4,2;3)$-*SEED* can be obtained from the parallel classes of an affine plane of order 2.

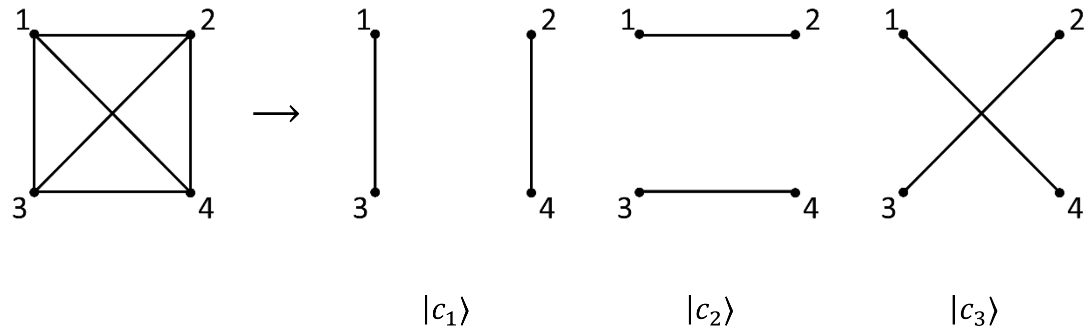


Figure 4. 2 A $1-(4,2;\ 3)$-*SEED*

The next example can be obtained from *Theorem 2.23* and *Corollary 4.3*.

Example 4.10 A $2-(v,2;m)$-*SEED* exists for any even integer v where m is the number of parallel classes in a resolvable $2-(v,2,1)$ design.

Example 4.11 Consider the $2-(6,2,1)$ design given in *Example 2.21*. The orthonormal basis of the corresponding jump code is given below. Each basis can be obtained from the parallel classes of the $2-(6,2,1)$ design. This code is equivalent to a $2-(6,2;5)$-*SEED*.

$$|c_0\rangle = \frac{1}{\sqrt{3}}(|100001\rangle + |010010\rangle + |001100\rangle),$$

$$|c_1\rangle = \frac{1}{\sqrt{3}}(|010001\rangle + |101000\rangle + |000110\rangle),$$

$$|c_2\rangle = \frac{1}{\sqrt{3}}(|001001\rangle + |010100\rangle + |100010\rangle),$$

$$|c_3\rangle = \frac{1}{\sqrt{3}}(|000101\rangle + |001010\rangle + |110000\rangle),$$

$$|c_4\rangle = \frac{1}{\sqrt{3}}(|000011\rangle + |100100\rangle + |011000\rangle).$$

Next corollary can be obtained from *Theorem 2.5* for $\lambda = 1$ and *Corollary 4.3*.

Corollary 4.6 [23] Any t-resolvable s-design $S(s,k;v)$ forms a $t-\left(v,k;\ \binom{v-t}{s-t}/\binom{k-t}{s-t}\right)$-*SEED*.

Example 4.12 [23] For any $m \geq 2$, there exists a $2-resolvable\, S(3,4;\ 4^m)$. Therefore, there exists a $(2^{2m}, 2^{2m-1}-1, 2)_4$ jump code.

Lemma 4.7 [23] If $v \equiv 3\ (mod\ 6)$, then there exists a $\left(v, \frac{v-1}{2}, 1\right)_3$ jump code.

Proof. There exists a resolvable Steiner triple system if $v \equiv 3\ (mod\ 6)$. There are $\frac{v(v-1)}{6}$ blocks and these blocks are resolved into $\frac{v-1}{2}$ parallel classes.

Next theorem provides a way to construct new t-*SEED*s from known t-*SEED*s.

Theorem 4.8 [53] ***(Direct Product Construction)*** Let there exist a $t-(v,k;\ m)$-*SEED* and a $t-(v',k';\ m')$-*SEED*. Then a $t-(vv',kk';\ mm')$-*SEED* also exists.

Proof. Let $\left(V_1;\ \mathcal{A}^{(1)},\dots,\mathcal{A}^{(m)}\right)$ be a $t-(v,k;\ m)$-*SEED*. Let $\left(V_2;\ \mathfrak{B}^{(1)},\dots,\mathfrak{B}^{(m)}\right)$ be a $t-(v',k';\ m')$-*SEED*. Define $V = V_1 \times V_2$ and $\mathcal{A}^{(i)}\times \mathfrak{B}^{(j)} = \left\{A \times B : A \in \mathcal{A}^{(i)}, B \in \mathfrak{B}^{(j)}\right\}$. Therefore, for any block $A \times B \in \mathcal{A}^{(i)}\times \mathfrak{B}^{(j)}$ the block size of $A \times B$ is kk'. Consider two blocks $A \times B$ and $A' \times B'$ in $\mathcal{A}^{(i)}\times \mathfrak{B}^{(j)}$. If $A \times B = A' \times B'$, then $A = A'$ and $B = B'$. So, $\mathcal{A}^{(i)}\times \mathfrak{B}^{(j)}$ consist of distinct blocks. As $\mathcal{A}^{(i)} \cap \mathcal{A}^{(i')} = \emptyset$ for any $i \neq i'$ and $\mathfrak{B}^{(j)} \cap \mathfrak{B}^{(j')} = \emptyset$ for any $j \neq j'$, $\mathcal{A}^{(i)}\times \mathfrak{B}^{(j)}$ and $\mathcal{A}^{(i')}\times \mathfrak{B}^{(j')}$ are disjoint. For any $u \leq t$, choose a u-tuple $E = \{(a_1,b_1),(a_2,b_2),\dots,(a_u,b_u)\} \in V$. Let $E_1 = \left\{a_1, a_2,\dots,a_u\right\}$ and $E_2 = \left\{b_1, b_2,\dots,b_u\right\}$. Then there are $\lambda_{E_1}\left|\mathcal{A}^{(i)}\right|$ blocks in $\mathcal{A}^{(i)}$ containing E_1 and there are $\lambda_{E_2}\left|\mathfrak{B}^{(j)}\right|$ blocks in $\mathfrak{B}^{(j)}$ containing E_2. That is, E occurs $\lambda_{E_1}\lambda_{E_2}\left|\mathcal{A}^{(i)}\right|\left|\mathfrak{B}^{(j)}\right|$ times for any i and j. Therefore, $\left(V;\ \mathcal{A}^{(1)}\times \mathfrak{B}^{(j)}\right)$ is a $t-(vv',kk';\ mm')$-*SEED* for any $i = 1,\dots,m$ and $j = 1,\dots,m'$.

Example 4.13 In the previous examples, we showed that a $2-(7,3;3)$-*SEED* and a $2-(9,3;7)$-*SEED* exist. By the above theorem, a $2-(56,9;21)$-*SEED* exists.

Next corollary is a result of *Theorem 4.8* and *Theorem 4.3.*

Corollary 4.9 If there exists an $LS_{\lambda_1}(t,k,v)$ and $LS_{\lambda_2}(t,k',\ v')$, then there exists a $t-(vv',kk';\ mm')$-*SEED*, where $m = \frac{\binom{v-t}{k-t}\binom{v'-t}{k'-t}}{\lambda_1\lambda_2}$.

Proof. An $LS_{\lambda_1}(t,k,v)$ is a $t-\left(v,k;\ \binom{v-t}{k-t}/\lambda_1\right)$-*SEED* and an $LS_{\lambda_2}(t,k',v')$ is a $t-\left(v',\ k';\ \binom{v'-t}{k'-t}/\lambda_2\right)$-*SEED*. Therefore, by *Theorem 4.8*, we have a $t-(vv',kk';\ mm')$-*SEED*.

4.2 Bounds and Some Existence Results

In this section, we give the general bound of a quantum jump code and a t-*SEED*. We will state some results and then give the general bound. For detailed proofs and more information, we refer the readers to Beth *et al.* [23]. In Subsection 4.2.1, the general bound of a quantum jump codes will be defined for given any t,k and v. In Subsection 4.2.2, some of the existence and non-existence results are stated with references.

4.2.1 General Bound for a *t-SEED*

The following lemmas and theorem that given for quantum jump codes are the same for t-*SEED*s, since t-*SEED*s are special type of quantum jump codes. Therefore, a jump code $(n,m,t)_k$ and a $t-(n,k;m)$-*SEED* can be used interchangeably.

Lemma 4.10 is an t-*SEED* analogue of *Definition 2.3 (complement design)*. Since complement of a t-design is again a t-design and by the *Theorem 4.4* we have the following lemma.

Lemma 4.10 [23] If $\mathcal{C}$ is an $(n,m,t)_k$ quantum jump code, then binary complement of $\mathcal{C}$, i.e. ${\sigma_x}^{\otimes n}\mathcal{C}$, is also an $(n,m,t)_{n-k}$ quantum jump code.

The following lemma for a jump code is similar to the *Definition 2.9* for designs.

Lemma 4.11 [23] If an $(n,m,t)_k$ quantum jump code exists for $k>t>1$, then an $(n-1,m,t-1)_{k-1}$ exists.

We now give an upper bound for quantum jump codes which is proved by Beth *et al*. [23].

Theorem 4.12 [23] The dimension m of a jump code $\mathcal{C}=(n,m,t)_k$ is bounded by

$$m \leq min\left\{\binom{n-t}{k-t},\binom{n-t}{k}\right\}.$$

Proof. It is clear that $(n,m,0)_k$ jump code has dimension $\mathbb{W}_k=\binom{n}{k}$. If $\mathcal{C}=(n,m,t)_k$, then by *Lemma 4.11*, a $\mathcal{J}_E\mathcal{C}$ is an $(n-t,m,0)_{k-t}$ jump code for $E\subset V$, $|E|=t$. Hence,

$dim\mathcal{C} \leq \binom{n-t}{k-t}$. Also, by *Lemma 4.10*, an $(n,m,t)_{n-k}$ jump code exists, hence an $(n-t,m,0)_{n-k-t}$ jump code exists, that means $dim\mathcal{C} \leq \binom{n-t}{n-k-t} = \binom{n-t}{k}$.

Definition 4.13 A $t-(v,k;m)$-*SEED* $\left(V;\ \mathfrak{B}^{(1)},\dots,\mathfrak{B}^{(m)}\right)$ is called optimal t-*SEED* if $m = min\left\{\binom{n-t}{k-t},\binom{n-t}{k}\right\}$.

From the definition, it is clear that $m = \binom{n-t}{k-t}$ or $m = \binom{n-t}{k}$. As it mentioned in *Lemma 4.10*, the binary complement of a t-*SEED* is again a t-*SEED*. Hence, it is enough to consider an optimal $t-(v,k;m)$-*SEED* where $1 \leq t < k \leq n/2$. Therefore, $m = \binom{n-t}{k-t}$.

Remark. A large set of $t-(v,k,1)$ designs is an optimal t-*SEED*, since in large set notation $N = \lambda\binom{n-t}{k-t}$, and by taking $\lambda = 1$ we have $N = \binom{n-t}{k-t} = m$.

Theorem 4.14 [53] If there exists an optimal $t-(v,k;m)$-*SEED*, then it is an $LS_1(t,k,v)$.

Corollary 4.15 An $LS_1(t,k,v)$ exists if and only if an optimal $t-(v,k;m)$-*SEED* exists.

Lemma 4.16 [53] If an $(n,m,t)_k$ quantum jump code exists for $k > t \geq 1$, then an $(n+1,m,t)_k$ quantum jump code exists.

Proof. If we append $|0\rangle$ to an $(n,m,t)_k$ jump code, we obtain a $(n+1,m,t)_k$ jump code since appending $|0\rangle$ does not change the weight of the code.

Lemma 4.17 [53] If an $(n,m,t)_k$ quantum jump code exists for $k > t \geq 1$, then an $(n+1,m,t)_{k+1}$ quantum jump code exists.

Proof. If we append $|1\rangle$ to an $(n,m,t)_k$ jump code, we obtain a $(n+1,m,t)_{k+1}$ jump code. Because appending $|1\rangle$ increases the length to $n+1$ and increases the weight of the code by 1.

4.2.2 Some Existence and Non-Existence Results for Special Parameters

The dimension m of a jump code $(6,m,2)_3$ is bounded by $m \leq 4$. Beth *et. al.* [23] showed the non-existence of a $(6,4,2)_3$ jump code in 2003. And recently, in 2011, Jimbo and Shiromoto [24] showed that there does not exist a $(6,3,2)_3$ jump code. Then some papers are published by Fang [25, 28, 29], Zhou [26, 27, 30], Lin [31].

Some of the non-existence results for special parameters are given in *Table 1* with references.

Table 4. 1 Results on existence and non-existence of jump codes

Jump Code	n	m	e	k	Reference
$(6,4,2)_3$	6	4	2	3	**[23]**
$(6,3,2)_3$	6	3	2	3	**[24]**
$(5,4,1)_k$	5	4	1	k	**[23]**
$(7,m,2)_3$	7	$\binom{n-t}{k-t}$	2	3	**[25]**
$(8,m,3)_4$	8	$\binom{n-t}{k-t}$	3	4	**[25]**
$(2k+1,m,1)_k$	$2k+1$	$\binom{n-t}{k-t}$	1	k	**[25]**
$(2k,m,2)_k$	$2k$	$\binom{n-t}{k-t}$	2	k	**[25]**

Example 4.14 [23] A $(n,m,1)_{n/2}$ jump code exists for any even integer n with $m=\frac{1}{2}\binom{n}{n/2}$.

In *Example 4.14*, the jump code $(n,m,1)_{n/2}$ with $m=\frac{1}{2}\binom{n}{n/2}$ and even n has orthonormal basis $|c_x\rangle=\frac{1}{\sqrt{2}}(|x\rangle+|\bar{x}\rangle)$. Here $|\bar{x}\rangle$ denotes the binary complement of $|x\rangle$.

Example 4.15 A $(4,3,1)_2$ quantum jump code is given with the following basis.

$$|c_{1010}\rangle=\frac{1}{\sqrt{2}}(|1010\rangle+|0101\rangle),$$

$$|c_{1100}\rangle=\frac{1}{\sqrt{2}}(|1100\rangle+|0011\rangle),$$

$$|c_{1001}\rangle = \frac{1}{\sqrt{2}}(|1001\rangle + |0110\rangle).$$

Next table provides some existence results on t-designs and t-*SEED*s with references.

Table 4. 2 Results on *t*-designs and *t-SEED*s

$\#m$	t	v	k	λ	t-*SEED*	Reference
5	3	32	8	7	$3-(32,8;5)$	**[54]**
121	5	24	9	6	$5-(24,9;121)$	**[29]**
			15	8580	$5-(24,15;121)$	
66	5	24	12	λ	$5-(24,12;66)$	**[29]**
1035	5	48	15	364	$5-(48,15;1035)$	**[29]**
			18	50456	$5-(48,18;1035)$	
529	5	48	24	λ	$5-(48,24;529)$	**[29]**
34	5	36	12	45	$5-(36,12;34)$	**[29]**
			15	5577	$5-(36,15;34)$	
17	5	36	18	λ	$5-(36,18;17)$	**[29]**
58	5	60	18	3060	$5-(60,18;58)$	**[29]**
			21	449820	$5-(60,21;58)$	
29	5	60	30	λ	$5-(60,30;29)$	**[29]**
124	3	64	18	15504	$3-(64,18;124)$	**[28]**
			21	2229840	$3-(64,21;124)$	

CHAPTER 5

RESULTS AND DISCUSSION

5.1 Conclusion

In this work, we surveyed the relation between quantum jump codes and combinatorial designs, and literature review was done. Firstly; combinatorial designs, quantum computing and quantum jump codes are introduced. Some examples of quantum jump codes are given and the combinatorial structures of these codes are studied. After introducing the basics of combinatorial designs and quantum jump codes, t-$SEED$s are introduced and the relation between combinatorial designs and quantum jump codes is defined. Lastly, it is stated that resolvable designs and large sets of t-designs have close connection to quantum jump codes.

In the fourth chapter, it is stated that optimal t-$SEED$s are large set of t-designs. But, it is still an open problem if there is any t-$SEED$ that attains the upper bound given in *Theorem 4.12* when there is no large set of t-designs with $N = m$.

5.2 Related Works

Known application areas of t-*SEED*s are coding theory and cryptography. In this thesis, we stated one application of t-*SEED*s to coding theory. Beth *et al*. [23] introduced t-*SEED*s as an application to quantum jump codes. Another application of t-*SEED*s takes a place in cryptography. Lin [53] discovered the relation between t-*SEED*s and secret sharing schemes in cryptography. We refer the readers interested in cryptography to [31, 53, 55, 56, 57].

REFERENCES

[1] Kirkman, Thomas P., (1847). "On a problem in combinations.", Cambridge and Dublin Math. J, 2:191-204.

[2] Kirkman, Thomas P., (1850). "Query VI.", Lady’s and Gentleman’s Diary, 48:1850.

[3] Steiner, J., (1853). "Combinatorische Aufgaben.", Journal für die reine und angewandte Mathematik, 45:181-182.

[4] Teirlinck, L., (1987). "Non-trivial t-designs without repeated blocks exist for all t.", Discrete Mathematics, 65.3:301-311.

[5] Hanani H., (1961). "The existence and construction of balanced incomplete block designs", Annals Mathematical Statistics, 32:361–386.

[6] Wilson R. M., (1975). "An existence theory for pairwise balanced designs III. Proof of the existence conjectures", J. Combinatorial Theory Ser. A, 18:71–79.

[7] Wilson R. M., (1973). "The necessary conditions for t-designs are sufficient for something", Utilitas Math., 4:207–215.

[8] Keevash, P., (2014). "The existence of designs.", arXiv preprint arXiv:1401.3665.

[9] Euler, L., (1782). "Recherches sur une nouvelle espece de quarres magiques".

[10] Tarry, G., (1900). "Le Probléme de 36 Officiers", Compte Rendu de l'Association Française pour l'Avancement de Science Naturel. Secrétariat de l'Association. 1: 122–123.

[11] Tarry, G. (1901). "Le Probléme de 36 Officiers", Compte Rendu de l'Association Française pour l'Avancement de Science Naturel. Secrétariat de l'Association. 2: 170–203.

[12] Fisher, R. A., (1925). Statistical Methods for Research Workers, Oliver and Boyd, Edinburgh.

[13] Fisher, R. A., (1947). The Design of Experiments, Oliver and Boyd, Edinburgh.

[14] Yates, F., (1936). "Incomplete randomized blocks", Ann. Eugen., 7:121–40.

[15] Shannon, C. E., (1948). "A mathematical theory of communication", Bell Syst. Tech. J., 27:379–423, 623–656.

[16] Hamming, R. W., (1950). "Error detecting and error correcting codes", Bell System Technical Journal, 29:147–160.

[17] Shor, Peter W., (1995). "Scheme for reducing decoherence in quantum computer memory.", Physical review A, 52.4: R2493.

[18] Steane, A. M., (1996). "Multiple particle interference and quantum error correction", Proc. R. Soc. Lond. A, 452:2551–2577.

[19] Djordjevic, I. B., (2008). "Quantum LDPC codes from balanced incomplete block designs", IEEE Commun. Lett., 12:389–391.

[20] Y. Fujiwara, D. Clark, P. Vandendriessche, M. De Boeck, and V. D. Tonchev, (2010). "Entanglement-assisted quantum low-density parity-check codes", Phys. Rev. A, 82:042338.

[21] Tonchev, V. D., (2008). "Quantum codes from caps", Discrete Math., 398:6368–6372.

[22] Alber, G., et al., (2001). "Stabilizing distinguishable qubits against spontaneous decay by detected-jump correcting quantum codes.", Physical Review Letters, 86.19: 4402.

[23] Beth, T., et al., (2003). "A new class of designs which protect against quantum jumps.", Designs, Codes and Cryptography, 29.1: 51-70.

[24] Jimbo, M., and Keisuke, S., (2011). "Quantum jump codes and related combinatorial designs.", Information Security, Coding Theory and Related Combinatorics, 29:285-311.

[25] Fang, J., Junling Z., and Yanxun C., (2014). "Nonexistence of some quantum jump codes with specified parameters.", Designs, codes and cryptography, 73.1:223-235.

[26] Zhou, J., and Yanxun C., (2016). "Bounds on the Dimensions of 2-Spontaneous Emission Error Designs.", Journal of Combinatorial Designs, 24.10:439-460.

[27] Zhou, J., and Yanxun C., (2015). "3-Spontaneous Emission Error Designs from PSL (2, q) or PGL (2, q).", Journal of Combinatorial Designs.

[28] Fang, J., and Yanxun C., (2015). "Mutually Disjoint 3-designs and 3-spontaneous Emission Error Designs.", Advances in Mathematics, 2015, China.

[29] Fang, J., and Yanxun C., (2015). "Mutually Disjoint 5-Designs and 5-Spontaneous Emission Error Designs from Extremal Ternary Self-Dual Codes.", Journal of Combinatorial Designs, 23.2:78-89.

[30] Zhou, J., and Yanxun C., (2016). "Bounds and constructions of t-spontaneous emission error designs.", Designs, Codes and Cryptography, 1:23.

[31] Lin, Y., and Masakazu J., (2014). "Extremal properties of t-SEEDs and recursive constructions.", Designs, codes and cryptography, 73.3:805-823.

[32] Stinson, Douglas R., (2007). Combinatorial designs: constructions and analysis, Springer Science & Business Media.

[33] Ernst W., (1938). "Uber Steinersche Systeme. Abh. Math. Semin. der Universitat Hamburg", 12:265–275.

[34] Magliveras, S., and David W. Leavitt, (1984). "Simple 6-(33; 8; 36) designs from PL 2 (32). ", Computational Group Theory, MD Atkinson ed.:337-352.

[35] Colbourn C. J. and J. H. Dinitz, (2006). Handbook of Combinatorial Designs, 2nd ed., Chapman & Hall / CRC, Boca Raton.

[36] Hanani, H., (1960). "On quadruple systems.", Canad. J. Math, 12.2:145-157.

[37] Diener, I., Eberhard S., and Hans L. de Vries., (1985). "All 80 Steiner triple systems on 15 elements are derived.", Discrete mathematics, 55.1:13-19.

[38] Cayley, A., "Iv. on the triadic arrangements of seven and fifteen things.", The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science, 37.247:50-53.

[39] Teirlinck, L., (1991). "A completion of Lu's determination of the spectrum for large sets of disjoint Steiner triple systems.", Journal of Combinatorial Theory, Series A, 57.2:302-305.

[40] Magliveras, S. S., (2009). "Large sets of t-designs from groups.", Mathematica Slovaca, 59.1:19-38.

[41] Chouinard L. G., (1983). "Partitions of the 4-subsets of a 13-set into disjoint projective planes", Discrete Math. 45:297–300.

[42] Kramer E. S., Magliveras S. S. and O’Brien E. A., (1993). "Some new large sets of t-designs", Australas. J. Combin., 7:189–193.

[43] Lu J. X., (1983). "On large sets of disjoint Steiner triple systems I, II and III", J. Combin. Theory Ser., A 37:140–182.

[44] Lu J. X., (1984). "On large sets of disjoint Steiner triple systems IV, V and VI", J. Combin. Theory Ser., A 37:136–192.

[45] Schreiber S., (1973). "Covering all triples on n marks by disjoint Steiner systems", J. Combin. Theory Ser., A 15:347–350.

[46] Schreiber S., (1974). "Some balanced complete block designs", Israel J. Math., 18:31–37.

[47] Mathon R. A., Searching for spreads and packings, Geometry, Combinatorial Designs and Related Structures, London Math. Soc. Lecture Note Ser. 245, Spetses 1996, Cambridge Univ. Press, 161–176 (1997).

[48] Teirlinck L., (1989). "Locally trivial t-designs and t-designs without repeated blocks", Discrete Math., 77:345–356.

[49] Teirlinck L., (1984). "On large sets of disjoint quadruple systems", Ars Combin., 17:173–176.

[50] Shor, Peter W., (1995). "Scheme for reducing decoherence in quantum computer memory.", Physical review, A 52.4:R2493.

[51] Wootters, William K., and Wojciech H. Zurek., (1982). "A single quantum cannot be cloned.", Nature 299.5886:802-803.

[52] Knill, E., and Raymond L., (1997). "Theory of quantum error-correcting codes.", Physical Review, A 55.2:900.

[53] Lin, Y., (2015). "Combinatorial designs and codes related to information-communication.", Phd. Thesis, Nagoya University, Japan.

[54] Fang, J., and Yanxun C., (2014). "Mutually disjoint t-designs and t-SEEDs from extremal doubly-even self-dual codes.", Designs, codes and cryptography, 73.3:769-780.

[55] Stinson, Douglas R., and Scott A. Vanstone., (1988). "A combinatorial approach to threshold schemes.", SIAM Journal on Discrete Mathematics, 1.2:230-236.

[56] Lin, Y., et al., (2014). "Optimal equi-difference conflict-avoiding codes of odd length and weight three.", Finite Fields and Their Applications, 26:49-68.

[57] Lin, Y., Miwako M., and Masakazu J., (2016). "Optimal equi-difference conflict-avoiding codes of weight four.", Designs, Codes and Cryptography, 78.3:747-776.

[58] Charnes, C., and Beth, T., (2005). "Combinatorial aspects of jump codes.", Discrete mathematics, 294.1:43-51.

[59] Heiss, Dieter, ed. Fundamentals of quantum information: quantum computation, communication, decoherence and all that. Vol. 587. Springer, 2008.

[60] Rieffel, E. G., and Wolfgang, H. P., (2011). Quantum computing: A gentle introduction. MIT Press.

[61] Brualdi, Richard A., (1977). Introductory combinatorics. Pearson Education India.

[62] Lindner, C. C., and Christopher A. Rodger, (2008). Design theory. CRC press.

CURRICULUM VITAE

PERSONAL INFORMATION

Name Surname	: EMRE ERSOY
Date of birth and place	: 04/07/1993, Istanbul / Turkey
Foreign Languages	: English
E-mail	: emrersoy10@gmail.com

EDUCATION

Degree	**Department**	**University**	**Date of Graduation**
Undergraduate	Mathematics	Yıldız Technical University	2015