Advances in Quantum Computing, Quantum Error Correction, and Quantum Algorithms

by

Farzad Shahi

A Dissertation Submitted to the
Graduate School of Sciences and Engineering
in Partial Fulfillment of the Requirements for
the Degree of

Master of Science

in

Physics

July 26, 2024

Advances in Quantum Computing, Quantum Error Correction, and Quantum Algorithms

Koç University

Graduate School of Sciences and Engineering

This is to certify that I have examined this copy of a master's thesis by

Farzad Shahi

and have found that it is complete and satisfactory in all respects,
and that any and all revisions required by the final
examining committee have been made.

Committee Members:

Prof. Özgür Eset Müstecaplıoğlu (Advisor)

Assist. Prof. Asgar Jamneshan

Assist. Prof. Cihan Okay

Date: July 26, 2024

ABSTRACT

Advances in Quantum Computing, Quantum Error Correction, and Quantum Algorithms

Farzad Shahi

Master of Science in Physics

July 26, 2024

The theoretical framework of quantum computing has promised a considerable advantage in the speed-up of the information processing over the classical computers. It harnesses the theory of quantum mechanics to propose novel frameworks of computing. Several models have been suggested and developed for implementing quantum computers, such as the circuit model of quantum computing, topological quantum computing, and measurement-based quantum computing. We will be concerned with the former model, that is the circuit model of quantum computing.

We will first provide a review of the basic axioms of quantum computing that directly rely on those of the theory of quantum mechanics. The circuit model of quantum computation for dealing with computational tasks will be introduced. There are three main problems of concern in this framework including the universality of quantum computing, the advantage of quantum computing over classical computing from the computational complexity point of view, and attempts to counteract the possible effects of noise on a quantum computer, that are studied here.

Inspired by some famous quantum algorithms that are proposed in alignment with this model, a recently proposed quantum algorithm for dealing with the problem of testing the linearity of Boolean functions which promises a speed-up over the well-known classical linearity test referred to as the BLR test, will be discussed. We will also discuss the well-known classical algorithm of testing the Boolean functions for being a low-degree polynomial and we may give suggestions on designing quantum algorithms aiming at this algebraic property testing task.

ÖZETÇE

Yüksek Lisans Tez Başlığı

Farzad Shahi

Fizik, Yüksek Lisans

26 Temmuz 2024

Kuantum hesaplamanın teorik çerçevesi, klasik bilgisayarlara kıyasla bilgi işleme hızında önemli bir avantaj vaat etmiştir. Bu, kuantum mekaniği teorisinden yararlanarak yeni hesaplama çerçeveleri önermektedir. Kuantum bilgisayarlarının uygulanması için devre modeli, topolojik kuantum hesaplama ve ölçüme dayalı kuantum hesaplama gibi çeşitli modeller önerilmiş ve geliştirilmiştir. Biz, devre modeli olarak bilinen ilk modelle ilgileneceğiz.

İlk olarak, kuantum hesaplamanın temel aksiyomlarının kuantum mekaniği teorisine dayanan kısımlarını inceleyeceğiz. Hesaplama görevlerini ele almak için kuantum hesaplamanın devre modeli tanıtılacaktır. Bu çerçevede ele alınması gereken üç ana sorun bulunmaktadır: kuantum hesaplamanın evrenselliği, hesaplama karmaşıklığı açısından kuantum hesaplamanın klasik hesaplamaya göre sağladığı avantajlar ve kuantum bilgisayarında gürültünün olası etkilerini bertaraf etme girişimleri.

Bu modelle uyumlu olarak önerilen bazı ünlü kuantum algoritmalarından ilham alarak, Boolean fonksiyonlarının doğrusallığını test etme problemine yönelik, klasik doğrusallık testi olan BLR testine kıyasla bir hızlanma vaat eden yakın zamanda önerilmiş bir kuantum algoritması tartışılacaktır. Ayrıca, Boolean fonksiyonlarının düşük dereceli bir polinom olup olmadığını test etmek için kullanılan klasik algoritmayı tartışacağız ve bu cebirsel özellik test etme görevine yönelik kuantum algoritmaları tasarlama konusunda önerilerde bulunabiliriz.

AKNOWLEDGEMENTS

I would like to thank Professor Özgür E. Müstecaplıoğlu and Professor Asgar Jamneshan for all their supports, help, and advising during my MSc program. This work is also supported by Scientific and Technological Research Council of Turkey (TÜBITAK). I also thank Professor Cihan Okay for accepting to be a committee member of my thesis defense.

MATHEMATICAL NOTATION

Set-theory

$\varnothing \equiv$ empty-set ..... $\varnothing$

$\mathcal{S}_1 = \mathcal{S}_2 \equiv \mathcal{S}_1$ equals $\mathcal{S}_2$. ..... $=$

$\mathcal{S}_1 \in \mathcal{S}_2 \equiv \mathcal{S}_1$ is an element of $\mathcal{S}_2$. ..... $\in$

$\mathcal{S}_1 \ni \mathcal{S}_2 \equiv \mathcal{S}_1$ contains $\mathcal{S}_2$. ..... $\ni$

$\{\mathcal{S}_1, \mathcal{S}_2\} \equiv$ the set composed of $\mathcal{S}_1$ and $\mathcal{S}_2$ ..... $\{\blacksquare, \blacksquare\}$

$\{\mathcal{S}_1 \in \mathcal{S}_2 \mid \mathfrak{p}(\mathcal{S}_1)\} \equiv$ all elements of $\mathcal{S}_2$ having the property $\mathfrak{p}$ ..... $\{\blacksquare \in \blacksquare \mid \blacksquare\}$

$\bigcup \mathcal{S} \equiv$ union of all elements of $\mathcal{S}$ ..... $\bigcup$

$\bigcap \mathcal{S} \equiv$ intersection of all elements of $\mathcal{S}$ ..... $\bigcap$

$\mathcal{P}(\mathcal{S}) \equiv$ power-set of $\mathcal{S}$ ..... $\mathcal{P}(\blacksquare)$

$\prod_{\alpha \in \mathcal{J}} \mathcal{S}_\alpha \equiv$ Cartesian-product of the collection of indexed sets $\{\mathcal{S}_\alpha\}_{\alpha \in \mathcal{J}}$ ..... $\prod$

$\mathcal{S}_1 \subseteq \mathcal{S}_2 \equiv \mathcal{S}_1$ is a subset of $\mathcal{S}_2$. ..... $\subseteq$

$\mathcal{S}_1 \supseteq \mathcal{S}_2 \equiv \mathcal{S}_1$ includes $\mathcal{S}_2$. ..... $\supseteq$

$\mathcal{S}_1 \subset \mathcal{S}_2 \equiv \mathcal{S}_1$ is a proper subset of $\mathcal{S}_2$. ..... $\subset$

$\mathcal{S}_1 \supset \mathcal{S}_2 \equiv \mathcal{S}_1$ properly includes $\mathcal{S}_2$. ..... $\supset$

$\mathcal{S}_1 \cup \mathcal{S}_2 \equiv$ union of $\mathcal{S}_1$ and $\mathcal{S}_2$ ..... $\cup$

$\mathcal{S}_1 \cap \mathcal{S}_2 \equiv$ intersection of $\mathcal{S}_1$ and $\mathcal{S}_2$ ..... $\cap$

$\mathcal{S}_1 \times \mathcal{S}_2 \equiv$ Cartesian-product of $\mathcal{S}_1$ and $\mathcal{S}_2$ ..... $\times$

$\mathcal{S}_1 \setminus \mathcal{S}_2 \equiv$ the relative complement of $\mathcal{S}_2$ with respect to $\mathcal{S}_1$ ..... $\setminus$

$f(\mathcal{S}) \equiv$ value of the function f at $\mathcal{S}$ ..... $\blacksquare(\blacksquare)$

$\mathsf{dom}(f) \equiv$ domain of the function f ..... $\mathsf{dom}(\blacksquare)$

$\mathsf{codom}(f) \equiv$ codomain of the function f ..... $\mathsf{codom}(\blacksquare)$

$\mathsf{img}(f) \equiv$ image of the function f ..... $\mathsf{img}(\blacksquare)$

$f^{\rightarrow} \equiv$ image-map of the function f ..... $\blacksquare^{\rightarrow}$

$f^{\leftarrow} \equiv$ inverse-image-map of the function f ..... $\blacksquare^{\leftarrow}$

$\mathfrak{resD}_f \equiv$ domain-restriction-map of the function f ..... $\mathfrak{resD}_{\blacksquare}$

$\mathfrak{resCD}_f \equiv$ codomain-restriction-map of the function f ..... $\mathfrak{resCD}_{\blacksquare}$

$\mathfrak{res}_f(\mathcal{S})$ ≡ domain-restriction and codomain-restriction of
the function f to $\mathcal{S}$ and $f^{\rightarrow}(\mathcal{S})$, respectively ..... $\mathfrak{res}_{\blacksquare}$

$\mathsf{F}(\mathcal{S}_1, \mathcal{S}_2)$ ≡ the set of all maps from $\mathcal{S}_1$ to $\mathcal{S}_2$ ..... $\mathsf{F}(\blacksquare, \blacksquare)$

$\mathsf{BF}(\mathcal{S}_1, \mathcal{S}_2)$ ≡ the set of all bijective functions from $\mathcal{S}_1$ to $\mathcal{S}_2$ ..... $\mathsf{BF}(\blacksquare, \blacksquare)$

f^{-1} ≡ the inverse mapping of the bijective function f ..... $\blacksquare^{-1}$

$\mathfrak{sF}(\mathcal{S}_1, \mathcal{S}_2)$ ≡ the set of all surjective functions from $\mathcal{S}_1$ to $\mathcal{S}_2$ ..... $\mathfrak{sF}(\blacksquare, \blacksquare)$

$f_1 \circ f_2$ ≡ composition of the function f_1 with the function f_2 ..... $\circ$

$\mathrm{Inj}_{\mathcal{S}_1 \to \mathcal{S}_2}$ ≡ the injection-mapping of the set $\mathcal{S}_1$ into the set $\mathcal{S}_2$ ..... $\mathrm{Inj}_{\blacksquare \to \blacksquare}$

$f_1 \overset{\mathfrak{f}}{\times} f_2$ ≡ the function-product of the function f_1 and f_2 ..... $\blacksquare \times \blacksquare$

$\mathsf{EqR}(\mathcal{S})$ ≡ the set of all equivalence relations on the set $\mathcal{S}$ ..... $\mathsf{EqR}(\blacksquare)$

$\mathcal{S}_1 / \mathcal{S}_2$ ≡ quotient-set of $\mathcal{S}_1$ by the equivalence-relation $\mathcal{S}_1$ ..... $\blacksquare / \blacksquare$

$[\mathcal{S}_1]_{\mathcal{S}_2}$ ≡ equivalence-class of $\mathcal{S}_1$ by the equivalence-relation $\mathcal{S}_2$ ..... $[\blacksquare]_{\blacksquare}$

$\mathsf{EqC}(\mathcal{S}_1; \mathcal{S}_2)$ ≡ equivalence-class of $\mathcal{S}_2$ by the equivalence-relation $\mathcal{S}_1$ ..... $\mathsf{EqC}(\blacksquare; \blacksquare)$

$|\mathcal{S}_1| \overset{\text{card}}{=} |\mathcal{S}_2| \equiv \mathsf{BF}(\mathcal{S}_1, \mathcal{S}_2)$ is non-empty. ..... $|\blacksquare| \overset{\text{card}}{=} |\blacksquare|$

$\mathsf{card}(\mathcal{S})$ ≡ cardinality of $\mathcal{S}$ ..... $\mathsf{card}(\blacksquare)$

Logic

$\mathfrak{p}_1 \wedge \mathfrak{p}_2 \equiv \mathfrak{p}_1$ and $\mathfrak{p}_2$. ..... $\wedge$

$\mathfrak{p}_1 \vee \mathfrak{p}_2 \equiv \mathfrak{p}_1$ or $\mathfrak{p}_2$. ..... $\vee$

$\mathfrak{p}_1 \Rightarrow \mathfrak{p}_2 \equiv$ if $\mathfrak{p}_1$, then $\mathfrak{p}_2$. ..... $\Rightarrow$

$\mathfrak{p}_1 \Leftrightarrow \mathfrak{p}_2 \equiv \mathfrak{p}_1$, if-and-only-if $\mathfrak{p}_2$. ..... $\Leftrightarrow$

$\neg\mathfrak{p} \equiv \mathfrak{p}_1$, negation of $\mathfrak{p}$. ..... $\neg$

$\forall\, \mathcal{S}_1 \in \mathcal{S}_2 \colon\ \mathfrak{p}(\!|\mathcal{S}_1|\!) \equiv$ for every $\mathcal{S}_2$ in $\mathcal{S}_1$, $\mathfrak{p}(\!|\mathcal{S}_1|\!)$. ..... $\forall\, \blacksquare \in \blacksquare \colon\ \blacksquare$

$\exists\, \mathcal{S}_1 \in \mathcal{S}_2 \colon\ \mathfrak{p}(\!|\mathcal{S}_1|\!) \equiv$ exists $\mathcal{S}_2$ in $\mathcal{S}_1$ such that $\mathfrak{p}(\!|\mathcal{S}_1|\!)$. ..... $\forall\, \blacksquare \in \blacksquare \colon\ \blacksquare$

Group Theory

$\langle S\rangle_G \equiv$ the set of all linear isomorphisms from the vector-space $\mathbb{E}$ to itself ..... $\langle\centerdot\rangle_{\centerdot}$

Linear Algebra

$\mathsf{span}_{\mathbb{E}}(A) \equiv$ the vector-subspace of the vector-space $\mathbb{V}$ spanned by the subset A of the set of all vectors of $\mathbb{E}$ .... $\mathsf{span}_{\centerdot}(\centerdot)$

$\mathsf{L}(\mathbb{E}_1, \mathbb{E}_2) \equiv$ the set of all linear maps from the vector-space $\mathbb{E}_1$ to the vector-space $\mathbb{E}_2$ .... $\mathsf{L}(\centerdot, \centerdot)$

$\mathsf{LIsom}(\mathbb{E}_1, \mathbb{E}_2) \equiv$ the set of all linear isomorphisms from the vector-space $\mathbb{E}_1$ to the vector-space $\mathbb{E}_2$ .... $\mathsf{LIsom}(\centerdot, \centerdot)$

$\mathsf{GL}(\mathbb{E}) \equiv$ the set of all linear isomorphisms from the vector-space $\mathbb{E}$ to itself . $\mathsf{GL}(\centerdot)$

$\mathcal{L}(\mathbb{E}) \equiv$ the set of all linear transmormations from the vector-space $\mathbb{E}$ to itself $\mathcal{L}(\centerdot)$

$\mathrm{U}(\mathbb{E}) \equiv$ the set of all unitary transformations from the vector-space $\mathbb{E}$ to itself $\mathrm{U}(\centerdot)$

$\mathbb{L}(\mathbb{E}_1, \mathbb{E}_2) \equiv$ the canonical vector-space of all linear maps from the vector-space $\mathbb{E}_1$ to the vector-space $\mathbb{E}_2$ .... $\mathbb{L}(\centerdot, \centerdot)$

$\det_n \equiv$ the determinant function on the set of all square $\mathbb{F}$-matrices of degree n for some field $\mathbb{F}$ .... $\det_{\centerdot}$

$\mathbb{E}_1 \oplus \mathbb{E}_2 \equiv$ the direct sum of the vector spaces $\mathbb{E}_1$ and $\mathbb{E}_2$ over the same field . $\centerdot \oplus \centerdot$

$v_1 \otimes v_2 \equiv$ the tensor-product of the elements v_1 and v_2 of a pair of vector-spaces $\centerdot \dot{\otimes} \centerdot$

Mathematical Environments

$\blacksquare \equiv$ end of definition .... $\blacksquare$

$\square \equiv$ end of theorem, lemma, proposition, or corollary .... $\square$

$\diamond \equiv$ end of the introduction of new fixed objects .... $\diamond$

TABLE OF CONTENTS

Chapter 1

INTRODUCTION

The theoretical framework of quantum computing has promised a considerable advantage in the speed-up of the information processing over the classical computers. It harnesses the theory of quantum mechanics to propose novel frameworks of computing. Several models have been suggested and developed for implementing quantum computers, such as the circuit model of quantum computing, topological quantum computing, and measurement-based quantum computing. We will be concerned with the former model, that is the circuit model of quantum computing.

We will first provide a review of the basic axioms of quantum computing that directly rely on those of the theory of quantum mechanics. The circuit model of quantum computation for dealing with computational tasks will be introduced. There are three main problems of concern in this framwork including the universality of quantum computing, the advantage of quantum computing over classical computing from the computational complexity point of view, and attempts to counteract the possible effects of noise on a quantum computer, that will be studied in the later chapters.

We will then introduce the famous stabilizet theory in the framework of quantum computing. Based on the stabilizer theory we will then discuss the famous Gottesmann-Knill theorem which states that a specific class of quantum circuits, those using elements of the Clifford group as gates, elements of Pauli group as measurements and elements of the computational basis as initial states, can be classically simulated in an efficient manner and thus have no advantage over classical computation. Then we will discuss around the problem of acheiving quantum universality and quantum advantage by providing a supply of some particular non-Clifford gates additional to the use of Clifford gates in a quantum circuit. We will also dis-

cuss about some recent works providing methods of classically simulating quantum circuits.

After discussing the problem of quantum advantage obtained by using a supply of non-Clifford gates, we will elaborate on the indirect ways of implementing such gates efficiently on a quantum computer. One of the important relevant methods that we will discuss involves simulating a non-Clifford gate by the aid of somes particular types of initially-given quantum states to be used alongside the main input state, simultaneously going through the operations of Clifford gates and Pauli measurements. Such a process requires accordingly the preparation of such ancillary states which are out of the class of states assumed to be prepared fault-tolerantly, that is the stabilizer states. The preparation process of such quantum states that we will discuss involves the purification of an initial noisy state towards the target ancillary state which is then called a magic state.

Then we will study the problem of noise effecting the accuracy of quantum computational tasks and discuss the models that have been suggested for alleviating the effects of noise and prevent the impact of error on quantum circuits. In this line, we will first review the classical notion of error and the general concept of a classical code to deal with errors, and then the quantum error-correcting procedures for counteracting the effects of noise on single qubits, such as the bit-flip, phase-flip, and Shor codes. Then we will provide a survey of the general problem of the correctability of a quantum error via using a quantum code, and a general class of quantum error-correcting codes called stabilizer codes, which demands a thorough study of the stabilizer theory. Within this discussion two well-known classes of quantum operations, called the Pauli group and the Clifford group will be introduced.

Following the study of the circuit model from different aspects, inspired by some famous quantum algorithms that are proposed in alignment with this model, we will discuss a recently proposed quantum algorithms for dealing with the famous problem of testing the linearity of Boolean functions which promises a speed-up over the well-known classical linearity test referred to as the BLR test. We will also discuss the well-known classical algorithm of testing the Boolean functions for being a low-degree polynomial and we may give suggestions on designing quantum versions of

this algebraic property testing task.

Chapter 2

BACKGROUND

For any vector space $\mathbb{V}$ *we will denote by* $\mathcal{L}(\mathbb{V})$ *the vector space of all linear transformations from* $\mathbb{V}$ *to itself.*

Let $\mathcal{H}$ *be a Hilbert space. We will denote by* $\mathrm{Herm}(\mathcal{H})$ *the set of all Hermitian operators of* $\mathcal{H}$*, that is the set* $\left\{A \in \mathcal{L}(\mathcal{H}) \mid A^\dagger = A\right\}$*. We will use the ket notation* $|\centerdot\rangle$ *to denote the unit vectors of* $\mathcal{H}$*. We will denote the inner product of two unit vectors* $|\psi\rangle$ *and* $|\phi\rangle$*, that is* $(|\psi\rangle, |\phi\rangle)$ *by* $\langle\psi|\phi\rangle$*. For any* $A \in \mathcal{L}(\mathcal{H})$ *and any pair of unit vectors* $|\psi\rangle$ *and* $|\phi\rangle$ *in* $\mathcal{H}$*, we will denote* $(|\psi\rangle, A|\phi\rangle)$ *by* $\langle\psi|A|\phi\rangle$*. A linear operator* $A \in \mathcal{L}(\mathcal{H})$ *is called a "non-negative (positive-semidefinite) operator on* $\mathcal{H}$*" if for every unit vector* $|\psi\rangle$ *in* $\mathcal{H}$*,* $\langle\psi|A|\psi\rangle$ *is a non-negative real number. We will denote by* $\mathrm{Pos}(\mathcal{H})$ *the set of all non-negative operators on* $\mathcal{H}$*.*

For any unit vector $|\psi\rangle \in \mathcal{H}$*,* $\langle\psi|$ *denotes the linear functional canonically corresponded to the vector* $|\psi\rangle$ *in the Hilbert space* $\mathcal{H}$*, and* $|\psi\rangle\langle\psi|$ *denotes the orthogonal projection onto the ray containing* $|\psi\rangle$*. More generally, given unit vectors* $|\psi\rangle, |\phi\rangle \in \mathcal{H}$*,* $|\psi\rangle\langle\phi|$ *denotes the linear map sending each* $v \in \mathcal{H}$ *to* $(|\phi\rangle, v)|\psi\rangle$*.*

We will denote by $\mathrm{U}(\mathcal{H})$ *the set of all unitary transformations of* $\mathcal{H}$*, which is known to be a group when endowed with the composition of operators.*

Since the theory of quantum computation is concerned with finite-dimensional complex vector-spaces, we will be concerned with finite-dimensional complex inner-product spaces (which are then automatically Hilbert spaces) in the entire text.

2.1 The Postulates of Quantum Mechanics

Definition 2.1: Let $\mathcal{H}$ be a Hilbert space.

$$\mathrm{Dens}(\mathcal{H}) := \{A \in \mathrm{Herm}(\mathcal{H}) \mid \mathrm{Tr}\{\rho\} = 1,\ A \in \mathrm{Pos}(\mathcal{H})\}. \tag{1}$$

Any element of $\mathrm{Dens}(\mathcal{H})$ is called a "density-matrix of $\mathcal{H}$".

■

2.1.1 The Postulate of Quantum State

Any isolated quantum system is associated with a Hilbert space (a complex vector-space endowed with an inner-product such that the metric induced by the inner-product is complete) $\mathcal{H}$ to be describable mathematically. At any time t the quantum system under consideration can be mathematically characterized by a density-matrix $\rho(t)$ of its associated Hilbert space $\mathcal{H}$, and then $\rho(t)$ is called the "state of the quantum system at time t". $\rho(t)$ is called a "pure state of $\mathcal{H}$", if $\rho(t) = |\psi\rangle\langle\psi|$ for some unit vector $|\psi\rangle \in \mathcal{H}$, and a "mixed state of $\mathcal{H}$" otherwise.
$\mathcal{H}$ is referred to as the "state space of the considered quantum system".

Remark 2.1: Suppose that the quantum state ρ of a quantum system at a point of time t is a pure state such that $\rho = |\psi\rangle\langle\psi|$. Then considering that $\rho = |\phi\rangle\langle\phi|$ if and only if $|\phi\rangle = e^{i\alpha}|\psi\rangle$, the state of the quantum system at time t can be identified with the set of all unit vectors in $\mathcal{H}$ differing by just a phase factor with $|\psi\rangle$, and hence can be identified with the one-dimensional subspace of $\mathcal{H}$ spanned by $\{|\psi\rangle\}$. Therefore, a pure state can be identified with an element of the complex projective space $\mathbf{P}\mathcal{H}$. So when we say that the state of an isolated quantum system is a pure state represented by a unit vector $|\psi\rangle \in \mathcal{H}$, we mean that the state is identified with $\mathsf{span}\{|\psi\rangle\}$.
Moreover, it is worth noting that if ρ is a pure state then $\rho^2 = \rho$ and hence $\mathrm{Tr}(\rho^2) = 1$, and if ρ is a mixed state then $\mathrm{Tr}(\rho^2) < 1$.

2.1.2 The Postulate of Evolution

The evolution of an isolated quantum system from any time t_1 to any time t_2 is described by a (not unique) unitary operator $U(t_2; t_1)$ with respect to the following rule.

$$\rho(t_2) = [U(t_2; t_1)]\,\rho_1(t)\,[U(t_2; t_1)]^\dagger, \tag{2}$$

where $\rho_1(t)$ and $\rho_2(t)$ denote the states of the system at times t_1 and t_2, respectively.

Remark 2.2: Let $\rho(t_1)$ and $\rho(t_2)$ be the states of a closed quantum system, associated with $\mathcal{H}$, at arbitrary time points t_1 and t_2, and let $U \in \mathrm{U}(\mathcal{H})$ such that $\rho(t_2) = U\rho(t_1)U^\dagger$. Then for any $V \in \mathrm{U}(\mathcal{H})$, $\rho(t_2) = V\rho(t_1)V^\dagger$ if and only if $V = e^{i\phi}U$ for some $\phi \in \mathbb{R}$. So considering that the center of the unitary group $\mathrm{U}(\mathcal{H})$ is the set of all scalar operators $\left\{e^{i\phi}I \mid \phi \in \mathbb{R}\right\}$ (I denotes the identity operator on $\mathcal{H}$), the evolution of the quantum system between two points of time can be fully described by elements of the quotient group $\mathrm{U}(\mathcal{H})/\mathcal{Z}(\mathrm{U}(\mathcal{H}))$.
If $\rho(t_1)$ is a pure state such that for a unit vector $|\psi\rangle \in \mathcal{H}$, $\rho(t_1) = |\psi\rangle\langle\psi|$, then $\rho(t_2) = U|\psi\rangle\langle\psi|U^\dagger$, and the state at t_2 is also a pure state. So if at time t_1 the state of the system is a pure state identified with $|\psi\rangle \in \mathcal{H}$, then the state at time t_2 is also a pure state identified with $U|\psi\rangle \in \mathcal{H}$.

2.1.3 The Postulate of Measurement

General Measurement: A general measurement in the Hilbert space $\mathcal{H}$ is described by a function $\mathcal{M}: R \to \mathcal{L}(\mathcal{H})$ from a finite set R to the set of all linear transformations of $\mathcal{H}$ such that $\sum_{r\in R}[\mathcal{M}(r)]^\dagger\mathcal{M}(r) = I$ (I denotes the identity operator on $\mathcal{H}$), where R is the set of all possible outcomes of the measurement $\mathcal{M}$. Measuring any isolated quantum system with a quantum state $\rho \in \mathrm{Dens}(\mathcal{H})$ at a point of time by $\mathcal{M}$ yields the outcome $r \in R$ with the probability $p(r) = \mathrm{Tr}\left([\mathcal{M}(r)]^\dagger\mathcal{M}(r)\rho\right)$, for every $r \in R$. Moreover, for every quantum state $\rho \in \mathrm{Dens}(\mathcal{H})$ and for every $r \in R$, if the outcome r is observed upon measuring ρ by $\mathcal{M}$, then the state of the quantum system is reduced to the quantum state ρ_r immediately after observing the outcome of the measurement, where,

$$\rho_r := \frac{1}{\mathrm{Tr}\left([M(r)]^\dagger M(r)\rho\right)}[\mathcal{M}(r)]\rho[\mathcal{M}(r)]^\dagger. \tag{3}$$

The image of $\mathcal{M}$, that is $\mathcal{M}(R)$ is called the "operation set of the measurement $\mathcal{M}$".

Remark 2.3: In the particular case that the quantum state of the quantum system is a pure state $\rho = |\psi\rangle\langle\psi|$ for some unit vector $|\psi\rangle \in \mathcal{H}$, for every $r \in R$ the

measurement of the quantum system by $\mathcal{M}$ yields the outcome r with probability

$$\begin{aligned} p(r) &= \mathrm{Tr}\left([\mathcal{M}(r)]^{\dagger} \mathcal{M}(r) |\psi\rangle\langle\psi| \right) \\ &= \left\langle \psi \middle| [\mathcal{M}(r)]^{\dagger} \mathcal{M}(r) \middle| \psi \right\rangle . \end{aligned} \tag{4}$$

and after observing the outcome r the state of the quantum system is reduced to the pure state identified by the unit vector $|\psi_r\rangle$, where,

$$|\psi_r\rangle := \frac{1}{\left\langle \psi \middle| [\mathcal{M}(r)]^{\dagger} \mathcal{M}(r) \middle| \psi \right\rangle} [\mathcal{M}(r)] |\psi\rangle \tag{5}$$

Projective Measurement: A Projective measurement in the Hilbert space $\mathcal{H}$ is a specific type of a general measurement, described by a function $\mathcal{P} : R \to \mathcal{L}(\mathcal{H})$ such that for every $r \in R$, $\mathcal{P}(r)$ is an orthogonal projection, that is $[\mathcal{P}(r)]^2 = \mathcal{P}(r)$ and $[\mathcal{P}(r)]^{\dagger} = \mathcal{P}(r)$, and furthermore $\mathcal{P}(r)\mathcal{P}(r') = \delta_{r,r'}\mathcal{P}(r)$ for every $r, r' \in R$. Therefore, it is seen that measuring any isolated quantum system with a quantum state $\rho \in \mathrm{Dens}(\mathcal{H})$ at a point of time by $\mathcal{P}$ yields the outcome $r \in R$ with the probability $p(r) = \mathrm{Tr}(\mathcal{P}(r)\rho)$, for every $r \in R$. Moreover, for every quantum state $\rho \in \mathrm{Dens}(\mathcal{H})$ and for every $r \in R$, if the outcome r is observed upon measuring ρ by $\mathcal{P}$, then the state of the quantum system is reduced to the quantum state ρ_r immediately after observing the outcome of the measurement, where,

$$\rho_r := \frac{1}{\mathrm{Tr}(P(r)\rho)} [\mathcal{P}(r)] \rho [\mathcal{P}(r)] . \tag{6}$$

Remark 2.4: It is obviously seen that $\sum_{r \in R} \mathcal{P}(r) = I$.

Remark 2.5: In the particular case that the quantum state of the quantum system is a pure state $\rho = |\psi\rangle\langle\psi|$ for some unit vector $|\psi\rangle \in \mathcal{H}$, for every $r \in R$ the measurement of the quantum system by the projective $\mathcal{P}$ yields the outcome r with probability

$$\begin{aligned} p(r) &= \mathrm{Tr}(\mathcal{P}(r)|\psi\rangle\langle\psi|) \\ &= \langle\psi|\mathcal{P}(r)|\psi\rangle . \end{aligned} \tag{7}$$

and after observing the outcome r the state of the quantum system is reduced to the pure state identified by the unit vector $|\psi_r\rangle$, where,

$$|\psi_r\rangle := \frac{1}{\langle\psi|\mathcal{P}(r)|\psi\rangle}\left[\mathcal{P}(r)\right]|\psi\rangle \tag{8}$$

Remark 2.6: Any Hermitian operator $H \in \mathrm{Herm}(\mathcal{H})$ can regardes as a projective measurement by corresponding it to the projective measurement $\tilde{H} : R \to \mathcal{L}(\mathcal{H})$ where R is the set of all eigenvalue of H, and H has the spectral decomposition

$$H = \sum_{r\in R} r\tilde{H}(r). \tag{9}$$

2.1.4 The Postulate of Composite Quantum Systems

The state space of a composite quantum system comprised of two quantum systems A and B with state spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively, is the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. If the sub-systems A and B are isolated from each other, then the quantum state of the composite system has the form $\rho_A \otimes \rho_B$ for some $\rho_A \in \mathcal{H}_A$ and $\rho_B \in \mathcal{H}_B$.

Remark 2.7: It is very crucial to note that the full characterization of a quantum system at any point of time involves the statistical information of all possible quantum measurements on the quantum system at that point of time. So since the state of quantum system as a density matrix in a Hilbert space implicitly carries the information of all measurement statistics according to the postulate of measurement, it is then justifiable why the postulate of quantum state associates any quantum system at any time point with a density matrix to characterize it. So considering just the sub-system A of the composite system and regarding it as a separate system, to be able to characterize it separately, one requires finding a (unique) density matrix $\rho_A \in \mathcal{H}_A$ whose predictions for the statistics of all measurements $\mathcal{M}_A$ of the Hilbert space $\mathcal{H}$ is in alignment with the statistics of all measurements of the composite Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ acting non-trivially on just $\mathcal{H}_A$, that is the measurements of the form $\mathcal{M}_A \otimes I_B$ with $\mathcal{M}_A \in \mathrm{Herm}(\mathcal{H}_A)$ and I_B denoting the identity operator on

$\mathcal{H}_B$. In this sense, it can be shown that if $\rho \in \mathcal{H}_A \otimes \mathcal{H}_B$ is the state of the composite system, then the unique $\rho_A \in \mathrm{Dens}(\mathcal{H}_A)$ satisfying this condition must be,

$$\rho_A = \mathrm{Tr}_B^{(AB)}(\rho), \tag{10}$$

where $\mathrm{Tr}_B^{(AB)} : \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B) \to \mathcal{L}(\mathcal{H}_A)$ is defined to be the linear map defined by,

$$\begin{aligned} &\mathrm{Tr}_B^{(AB)}\left(\left|e_j^{(A)}\right\rangle\!\left\langle e_k^{(A)}\right| \otimes \left|e_l^{(B)}\right\rangle\!\left\langle e_m^{(B)}\right|\right) \stackrel{\text{def}}{=} \\ &\quad \left(\mathrm{Tr}\left(\left|e_l^{(B)}\right\rangle\!\left\langle e_m^{(B)}\right|\right)\right)\left|e_j^{(A)}\right\rangle\!\left\langle e_k^{(A)}\right| = \delta_{l,m}\left|e_j^{(A)}\right\rangle\!\left\langle e_k^{(A)}\right|, \end{aligned} \tag{11}$$

for every j, k and l, m, where $\left\{e_j^{(A)}\right\}_j$ and $\left\{e_k^{(B)}\right\}_k$ are taken to be orthonormal bases for $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively.
$\mathrm{Tr}_B^{(AB)}$ is called the "partial trace on $\mathcal{H}_A \otimes \mathcal{H}_B$" relative to the second factor $\mathcal{H}_B$".

2.2 Quantum Circuits

We will denote by $\mathcal{H}$ the two-dimensional complex vector-space $\mathbb{C}^2$. We will denote the vectors $(1, 0)$ and $(0, 1)$ in $\mathbb{C}^2$ by $|0\rangle$ and $|1\rangle$, respectively. The ordered basis $\{|0\rangle, |1\rangle\}$ of $\mathbb{C}^2$ will be referred to as the "computational basis of $\mathcal{H}$". For any positive integer n, the set of vectors $\{|s_1\rangle \otimes \cdots \otimes |s_n\rangle \mid s_i \in \{0, 1\},\ i = 1, \cdots, n\}$ which forms a basis for the complex vector-space $\mathcal{H}^{\otimes n}$ is called the "computational basis of $\mathcal{H}^{\otimes n}$". $|s_1\rangle \otimes \cdots \otimes |s_n\rangle$ will be denoted simply by $|s_1 \cdots s_n\rangle$. The set of all unitary transformations of $\mathcal{H}^{\otimes n}$, that is $\mathrm{U}(\mathcal{H}^{\otimes n})$, will simply be denoted by $\mathcal{U}_n$. It is well-known that $\mathcal{U}_n$ endowed with the operation of function composition has the structure of a group, and we will call $\mathcal{U}_n$ the "n-qubit unitary group", which is canonically isomorphic to the unitary group of degree 2^n, that is $U(2^n)$. We will also denote by I_n the identity operator on the Hilbert-space $\mathcal{H}^{\otimes n}$.
Considering that quantum mechanics makes no distinction between two vectors $u, v \in \mathcal{H}^{\otimes n}$ such that $u = cv$ for some $c \in \mathbb{C}$, the points of the projective space $\mathbf{P}\mathcal{H}^{\otimes n}$ are enough to characterize quantum systems. Equivalently, the choice of the specific class of vectors of $\mathcal{H}^{\otimes n}$ constrained to have unit norm, suffice the description of quantum systems. Therefore we will denote destinctively by $\mathcal{Q}_n$ the set of all vectors of $\mathcal{H}^{\otimes n}$ with unit norm. We will also denote the elemetns of $\mathcal{Q}_n$, which are descriptives of

quantum systems, with the ket notation like $|\psi\rangle$*, and refer to them as "quantum states".*

For any $|\psi\rangle \in \mathcal{Q}_n$*,* $\langle\psi|$ *denotes the linear functional canonically corresponded to the vector* $|\psi\rangle$ *in the inner-product-space* $\mathcal{H}^{\otimes n}$*, and* $|\psi\rangle\langle\psi|$ *denotes the orthogonal projection onto the ray containing* $|\psi\rangle$*. More generally, given* $|\psi\rangle, |\phi\rangle \in \mathcal{Q}_n$*,* $|\psi\rangle\langle\phi|$ *denotes the linear map sending each* $v \in \mathcal{H}^{\otimes n}$ *to* $(|\phi\rangle, v)|\psi\rangle$*, where* $(|\phi\rangle, v)$ *denotes the inner product of the two vectors. The inner product of two quantum states* $|\psi\rangle, |\phi\rangle$ *in* $\mathcal{Q}_n$ *is simply denoted by* $\langle\psi|\phi\rangle$*.*

Since any pair $|\psi\rangle, |\phi\rangle \in \mathcal{Q}_n$ *with* $|\psi\rangle = e^{i\phi}|\phi\rangle$ *are physically equivalent, we can further factor out this equivalence* $\sim$ *in* $\mathcal{Q}_n$ *and regard* $\mathcal{Q}_n/\sim$ *as the space of quantum states. So, with some abuse of notation, when we say two quantum states* $|\psi\rangle$ *and* $|\phi\rangle$ *are different, we simply mean that the equivalence classes of* $|\psi\rangle$ *and* $|\phi\rangle$ *are different in* $\mathcal{Q}_n/\sim$*, which is equivalent to* $\langle\psi|\phi\rangle < 1$*.*

Definition 2.2: A quantum gate in the Hilbert space $\mathcal{H}^{\otimes n}$ is defined to be the implementation of a unitary operation $U \in \mathrm{U}(\mathcal{H}^{\otimes n})$ which is capable of receiving a quantum system with any state $\rho \in \mathrm{Dens}(\mathcal{H}^{\otimes n})$ and outputting $U\rho U^\dagger$ instantly.

■

Definition 2.3: A quantum circuit in the Hilbert space $\mathcal{H}^{\otimes n}$ consists of the following.

QC1: A quantum system prepared initially with a quantum state $\rho_0 \in \mathrm{Dens}(\mathcal{H}^{\otimes n})$, as the input

QC2: A finite sequence of quantum gates and quantum measurements to be performed successively starting from the initial state ρ_0 and terminated by a measurement

QC3: A classical processor at the final step

■

Definition 2.4: A "measurement in the computational-basis of $\mathcal{H}^{\otimes n}$" is defined to be a measurement with the operation set $\{|x\rangle\langle x| \mid x \in \mathbb{F}_2{}^n\}$.

■

2.3 Famous Single-Qunit and Two-Qubit Gates

2.3.1 Single-Qubit Gates

We now introduce some famous single-qubit gates, that is unitary operators in $\mathrm{U}\left(\mathcal{H}^{\otimes 1}\right)$. The single-qubit Pauli operators $X, Y, Z \in \mathrm{U}\left(\mathcal{H}^{\otimes 1}\right)$ are defines as,

$$X := |0\rangle\langle 1| + |1\rangle\langle 0|\,, \tag{12}$$

$$Y := -i\,|0\rangle\langle 1| + i\,|1\rangle\langle 0|\,, \tag{13}$$

$$Z := |0\rangle\langle 0| - |1\rangle\langle 1|\,. \tag{14}$$

The single-qubit Hadamard gate $H \in \mathrm{U}\left(\mathcal{H}^{\otimes 1}\right)$ is defined as,

$$H := \frac{1}{\sqrt{2}}\,(X + Z) = \frac{1}{\sqrt{2}}\,(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|)\,. \tag{15}$$

The single-qubit phase gate $P \in \mathrm{U}\left(\mathcal{H}^{\otimes 1}\right)$ is defined as,

$$P := |0\rangle\langle 0| + i\,|1\rangle\langle 1|\,. \tag{16}$$

2.3.2 Two-Qubit Gates

We now introduce some famous two-qubit gates, that is unitary operators in $\mathrm{U}\left(\mathcal{H}^{\otimes 2}\right)$. First we introduce the notion of controlled gates in $\mathrm{U}\left(\mathcal{H}^{\otimes n}\right)$ constructed based on single-qubit gates, for any positive integer $n > 1$.

Definition 2.5: Let n be a positive integer greater than 1. Let $j, k \in \{1, \cdots, n\}$ Let $A \in \mathrm{U}\left(\mathcal{H}^{\otimes 1}\right)$ be a single-qubit gate. Then the gate $C^{(n)}_{[j,k]}(A)$ is defined as the linear transformation on $\mathcal{H}^{\otimes n}$ acting as follows on the computational basis elements. For every $(l_1, \cdots, l_n) \in \{0,1\}^n$,

$$\left[C^{(n)}_{[j,k]}(A)\right] |l_1\rangle \otimes \cdots \otimes |l_j\rangle \otimes \cdots \otimes |l_k\rangle \otimes \cdots \otimes |l_n\rangle :=$$
$$|l_1\rangle \otimes \cdots \otimes |l_j\rangle \otimes \cdots \otimes A^{l_j}\,|l_k\rangle \otimes \cdots \otimes |l_n\rangle\,, \tag{17}$$

where $A^1 = A$ and $A^0 := I$. $C^{(n)}_{[j,k]}(A)$ is called the "n-qubit controlled-A gate with control in the j-th qubit and operation in the k-th qubit".

■

Any gate of type $C^{(n)}_{[j,k]}(X) \in \mathrm{U}(\mathcal{H}^{\otimes n})$ is called a "CNOT gate", for any $n > 1$. Specifically $C^{(2)}_{[1,2]}(X) \in \mathrm{U}(\mathcal{H}^{\otimes 2})$ is simply called the CNOT gate.
The swap gate $\mathrm{SWAP} \in \mathrm{U}(\mathcal{H}^{\otimes 2})$ is defined as,

$$\mathrm{SWAP} := \left[C^{(2)}_{[1,2]}(X)\right]\left[C^{(2)}_{[2,1]}(X)\right]\left[C^{(2)}_{[1,2]}(X)\right]. \tag{18}$$

Thus SWAP acts on the elements of the computational basis as follows.

$$\forall\ (x_1,\, x_2) \in \{0,1\}^2 \colon\ \mathrm{SWAP}\,|x_1\rangle \otimes |x_2\rangle = |x_2\rangle \otimes |x_1\rangle\,. \tag{19}$$

More generally for every $n > 1$ and any $j, k \in \{1, \cdots, n\}$, the swap gate $\mathrm{SWAP}^{(n)}_{[j,k]} \in \mathrm{U}(\mathcal{H}^{\otimes n})$ is defined as

$$\mathrm{SWAP}^{(n)}_{[j,k]} := \left[C^{(n)}_{[j,k]}(X)\right]\left[C^{(n)}_{[k,j]}(X)\right]\left[C^{(n)}_{[j,k]}(X)\right]. \tag{20}$$

2.4 Successive Measurements By a Pair of compatible Observables

Let $\mathcal{H}$ be a finite-dimensional Hilbert space with $\dim \mathcal{H} = n$, and let O_1 and O_2 denote the Hermitian operators correponded to a pair of compatible observables in this Hilbert space. So $[O_1, O_2] = 0$. Due to Hermiticity, O_1 and O_2 have unique spectral decompositions,

$$\begin{aligned} O_1 &= \sum_{i=1}^{m_1} \lambda_i^{(1)} P_i^{(1)}, \\ O_2 &= \sum_{i=1}^{m_2} \lambda_i^{(2)} P_i^{(2)}, \end{aligned} \tag{21}$$

where $m_1, m_2 \leq n$, each $P_i^{(1)}$ and $P_i^{(2)}$ is a projection on $\mathcal{H}$, and,

$$\sum_{i=1}^{m_1} P_i^{(1)} = \sum_{i=1}^{m_2} P_i^{(2)} = I_{\mathcal{H}}, \tag{22}$$

where $I_{\mathcal{H}}$ denotes the identity operator on $\mathcal{H}$.
It is known that given a pair of diagonalizable operators on a finite-dimensional inner-product space, there exists an orthonormal basis for the space whose elements are common eigenvectors of them. Let $(|\phi_1\rangle, \cdots, |\phi_n\rangle)$ denote an n-tuple of common eigenvectors of O_1 and O_2 which is simultaneously an orthonormal basis of $\mathcal{H}$. We

denote by $\mathcal{H}_i^{(O_1)}$ the subspace of $\mathcal{H}$ onto which $P_i^{(1)}$ projects $\mathcal{H}$, that is $\mathcal{H}_i^{(O_1)} := P_i^{(1)}(\mathcal{H})$. Since $P_i^{(1)} P_j^{(1)} = 0$ for $i \neq j$ and $\sum_{i=1}^{m_1} P_i^{(1)} = I_{\mathcal{H}}$, it is clear that,

$$\mathcal{H} = \mathcal{H}_1^{(O_1)} \oplus \cdots \oplus \mathcal{H}_{m_1}^{(O_1)}. \tag{23}$$

Therefore we can choose $(|\phi_1\rangle, \cdots, |\phi_n\rangle)$ such that $\mathcal{H}_1^{(O_1)}$ is spanned by $\{|\phi_1\rangle, \cdots, |\phi_q\rangle\}$, where $q := \dim \mathcal{H}_1^{(O_1)}$. This choice of order is just for the sake of notational convenience in the following discussions. Then clearly,

$$P_1^{(1)} = \sum_{i=1}^{q} |\phi_i\rangle\langle\phi_i| . \tag{24}$$

Suppose that a physical system is prepared with a pure quantum state $|\Psi\rangle \in \mathcal{H}$, and the observable corresponded to O_1 is measured upon this system. Then one of the eigenvalues of O_1 would be observed. There is no loss of generality in assuming that the observed eigenvalue is $\lambda_1^{(1)}$. Then clearly the system after this measurement, without considering the normalization factor, collapses to the state,

$$|\Psi'\rangle := P_1^{(1)} |\Psi\rangle = \sum_{i=1}^{q} \langle\phi_i|\Psi\rangle |\phi_i\rangle . \tag{25}$$

Now assume that after this observation, the observable corresponded to O_2 is measured upon the newly attained state $|\Psi'\rangle$. It is obvious that,

$$\begin{aligned} O_1 &= \sum_{i=1}^{n} \mu_i^{(1)} |\phi_i\rangle\langle\phi_i| , \\ O_2 &= \sum_{i=1}^{n} \mu_i^{(2)} |\phi_i\rangle\langle\phi_i| , \end{aligned} \tag{26}$$

where $\left\{\mu_1^{(1)}, \cdots, \mu_n^{(1)}\right\} \subseteq \left\{\lambda_1^{(1)}, \cdots, \lambda_{m_1}^{(1)}\right\}$ and $\left\{\mu_1^{(1)}, \cdots, \mu_n^{(2)}\right\} \subseteq \left\{\lambda_1^{(2)}, \cdots, \lambda_{m_1}^{(2)}\right\}$. That is, each $\mu_i^{(\alpha)}$ in the above expansions must be one of the eigenvalues of O_α ($\alpha = 1, 2$). It is also clear that for each i, there exists a unique subset $\left\{\left|\phi_{s_i(1)}\right\rangle, \cdots, \left|\phi_{s_i(\beta_i)}\right\rangle\right\}$ of $\{|\phi_1\rangle, \cdots, |\phi_n\rangle\}$ such that,

$$P_i^{(2)} = \sum_{j=1}^{\beta_i} \left|\phi_{s_i(j)}\right\rangle\left\langle\phi_{s_i(j)}\right| , \tag{27}$$

where β_i denotes the dimension of the subspace projected by $P_i^{(2)}$, and s_i denotes the relevant unique increasing (and hence injective) map from $\{1, \cdots, \beta_i\}$ to $\{1, \cdots, n\}$.

For each i, the probability $\mathcal{P}\left(\lambda_i^{(2)}\right)$ of observing the eigenvalue $\lambda_i^{(2)}$ upon measuring O_2 on $|\Psi'\rangle$ is,

$$\mathcal{P}\left(\lambda_i^{(2)}\right) = \left\langle \Psi' \middle| P_i^{(2)} \middle| \Psi' \right\rangle. \tag{28}$$

So it is apparent that $\mathcal{P}\left(\lambda_i^{(2)}\right) \neq 0$ only if the subspace projected by $P_i^{(2)}$, that is the subspace $\mathcal{H}_i^{(O_2)} := P_i^{(2)}(\mathcal{H})$ contains at least one element from the set $\{|\phi_1\rangle, \cdots, |\phi_q\rangle\}$. This is equivalent to saying that $\mathcal{P}\left(\lambda_i^{(2)}\right) \neq 0$ if and only if

$$\left\{\left|\phi_{s_i(1)}\right\rangle, \cdots, \left|\phi_{s_i(\beta_i)}\right\rangle\right\} \cap \{|\phi_1\rangle, \cdots, |\phi_q\rangle\} \neq \varnothing. \tag{29}$$

Now let $\lambda_i^{(2)}$ be an arbitrary choice of an eigenvalue such that $\mathcal{P}\left(\lambda_i^{(2)}\right) \neq 0$. Then define,

$$\left\{\left|\phi_{s_i(1)}\right\rangle, \cdots, \left|\phi_{s_i(\beta_i)}\right\rangle\right\} \cap \{|\phi_1\rangle, \cdots, |\phi_q\rangle\} = \{|\varphi_1\rangle, \cdots, |\varphi_r\rangle\}. \tag{30}$$

It is obvious that all vectors in $\left\{\left|\phi_{s_i(1)}\right\rangle, \cdots, \left|\phi_{s_i(\beta_i)}\right\rangle\right\}$ other than $\{|\varphi_1\rangle, \cdots, |\varphi_r\rangle\}$ are orthogonal to all vectors in $\{|\phi_1\rangle, \cdots, |\phi_q\rangle\}$. Suppose that after measuring O_2 upon $|\Psi'\rangle$, the result $\lambda_i^{(2)}$ is observed. Then the system must collapse, again without considering the normalizing factor, to the state,

$$\begin{aligned} |\Psi''\rangle := P_i^{(2)} |\Psi'\rangle &= \left(\sum_{j=1}^{\beta_i} \left|\phi_{s_i(j)}\right\rangle\left\langle\phi_{s_i(j)}\right|\right)\left(\sum_{i=1}^{q} \langle\phi_i|\Psi\rangle\, |\phi_i\rangle\right) \\ &= \left(\sum_{j=1}^{r} |\varphi_r\rangle\langle\varphi_r|\right)\left(\left(\sum_{i=1}^{q} \langle\phi_i|\Psi\rangle\, |\phi_i\rangle\right)\right) \\ &= \left(\sum_{j=1}^{r} \langle\varphi_r|\Psi\rangle\, |\varphi_r\rangle\right). \end{aligned} \tag{31}$$

Since $\{|\varphi_1\rangle, \cdots, |\varphi_r\rangle\} \subseteq \{|\phi_1\rangle, \cdots, |\phi_q\rangle\}$, it is clear that $|\Psi''\rangle \in \mathcal{H}_1^{(O_1)}$. Therefore, measuring $|\Psi''\rangle$ again by the observable O_1 must yield the same result $\lambda_1^{(1)}$ as observed initially before the intervention of the measurement O_2.

Chapter 3

STABILIZER FORMALISM

3.1 The Pauli and Clifford Groups

Let n be a positive integer. The "Pauli group on n qubits" or simply the "n-Pauli group" is defined as the following set of unitary operators in $\mathcal{L}\left(\mathcal{H}^{\otimes n}\right)$.

$$\mathcal{P}_n := \left\{c\, O_1 \otimes \cdots \otimes O_n \mid c \in \{-1, 1, -i, i\}\,,\ \forall k\ O_k \in \{I, X, Y, Z\}\right\}. \tag{1}$$

It is straightforward to observe that $\mathcal{P}_n$ together with the operator composition is a group, and hence a subgroup of the group of unitary transformations of $\mathcal{H}^{\otimes n}$, that is $\mathcal{U}_n$. Every element of $\mathcal{P}_n$ is called a "(n-qubit) Pauli operator".
Since any pair of 1-qubit Pauli operators either commute or anti-commute, according to the definition of the Pauli group, it is evident that any pair of n-qubit Pauli operators must either commute or anti-commute. That is, for every $g_1, g_2 \in \mathcal{P}_n$, either $g_1 g_2 = g_2 g_1$ or $g_1 g_2 = -g_2 g_1$. The study of the subgroups of the Pauli group is of remarkable importance due to the roles they play in both stabilizer quantum error correcting codes and hence the fault-tolerant quantum computation, and determining a class of quantum states that renders quantum computation classically simulable in an efficient manner from the computational complexity point of view. In this regard, a class of subgroups of the Pauli group, those consisting of pairwise-commuting elements, becomes dominant.

Definition 3.1: For every subgroup S of $\mathcal{P}_n$, $\mathcal{V}_S$ is defined to be the subset of $\mathcal{H}^{\otimes n}$ associated with S as follows.

$$\mathcal{V}_S := \left\{v \in \mathcal{H}^{\otimes n} \mid \left[\forall\, g \in S\colon\ g\,(v) = v\right]\right\}. \tag{2}$$

Put it in other words, $\mathcal{V}_S$ is the intersection of the eigen-spaces of all operators in S corresponded to the eigen-value 1.

Each subgroup of $\mathcal{P}_n$ is called a "(n-qubit) stabilizer group". For every stabilizer group S, $\mathcal{V}_S$ is referred to as the "subspace of $\mathcal{H}^{\otimes n}$ stabilized by S".

■

Proposition 3.1: Let S be a subgroup of $\mathcal{P}_n$. $\mathcal{V}_S$ is a vector-subspace of $\mathcal{H}^{\otimes n}$.

proof : Let $c \in \mathbb{C}$, and $v_1, v_2 \in \mathcal{V}_S$. Since for every $g \in S$, $g(v_1) = v_1$ and $g(v_2) = v_2$, considering the linearity of elements of S we have,

$$\forall\, g \in S\colon\ g(cv_1 + v_2) = cg(v_1) + g(v_2) = cv_1 + v_2, \tag{3}$$

and thus $cv_1 + v_2 \in \mathcal{V}_S$.

□

Proposition 3.2: Let S be a subgroup of $\mathcal{P}_n$. If $\mathcal{V}_S$ is a non-trivial subspace of $\mathcal{H}^{\otimes n}$, that is if $\mathcal{V}_S \neq \{0\}$, then $-I_n \notin S$ and every pair of elements in S commute.

proof :

i. Suppose that $-I_n \in S$. Then if $v \in \mathcal{V}_S$, we must have $-I_n v = v$, which implies $v = 0$. Therefore we must have $\mathcal{V}_S = \{0\}$.

ii. Suppose that there exists $g_1, g_2 \in S$ such that they do not commute, that is $g_1 g_2 = -g_2 g_1$. Then if $v \in \mathcal{V}_S$, we must have $v = g_1 g_2(v) = -g_2 g_1(v) = -v$, and hence $v = 0$. Therefore we must have $\mathcal{V}_S = \{0\}$.

□

Based on [proposition 3.2], and considering that we will be concerned merely with the stabilizer groups that stabilize a non-trivial subspace of $\mathcal{H}^{\otimes n}$, we will be interested in studying the stabilizer groups with pairwise commuting elements and without containing $-I_n$. It can also be observed that when a subgroup of $\mathcal{P}_n$ does not contain $-I_n$, it must consist of pairwise commuting elements, and hence this property does not give further information about such subgroups.

Proposition 3.3: Let S be a subgroup of $\mathcal{P}_n$ such that $-I_n \notin S$. Then for every $g \in S$, $g^2 = I_n$ and $g^\dagger = g$, and for every $g \in S \setminus \{I_n\}$, $\{-1, +1\}$ forms the set of all eigenvalues of g.

proof : Let $g \in \mathcal{P}_n$. According to the definition of Pauli group and considering that $X^2 = Y^2 = Z^2 = I_2$, it is straightforward to see that for every $s \in \mathcal{P}_n$ either $s^2 = I_n$ or $s^2 = -I_n$. Since S is a group and $g \in S$, g^2 must also be in S. So because $-I_n$ is assumed to be out of S, the only possibility is $g^2 = I_n$ which means $g = g^{-1}$. Furthermore, since g is a unitary operator, $g^\dagger = g^{-1}$, and thus $g = g^\dagger$.
$g^2 = I_n$ implies that any eigenvalue of g must be in $\{-1, 1\}$. But considering that g is Hermitian and according to the spectral theorem, it is trivial that $+1$ (or -1) is the only eigenvalue of g if and only if $g = I_n$ (or $g = -I_n$).

□

Proposition 3.4: Let S be a subgroup of $\mathcal{P}_n$ such that $-I_n \notin S$. Then for every $g_1, g_2 \in S$, $g_1 g_2 = g_2 g_1$.

proof : Let $g_1, g_2 \in S$. According to [proposition 3.3], $g_1^2 = g_2^2 = (g_1 g_2)^2 = I_n$. Assume that g_1 and g_2 does not commute, that is $g_1 g_2 = -g_2 g_1$. Then

$$(g_1 g_2)^2 = (g_1 g_2)(-g_2 g_1) = -g_1 \left(g_2^2\right) g_1 = -g_1 I_n g_1 = -g_1^2 = -I_n, \tag{4}$$

which is a contradiction. Therefore g_1 and g_2 must commute.

□

Proposition 3.5: Let S be a subgroup of $\mathcal{P}_n$ such that $-I_n \notin S$. Then,

$$S \subseteq \{c\, O_1 \otimes \cdots \otimes O_n \mid c \in \{-1, 1\},\ \forall k\ O_k \in \{I, X, Y, Z\}\}, \tag{5}$$

and for every $g \in S$, $-g \notin S$.

proof : It is trivial.

□

There are smaller subsets of stabilizer groups carrying their necessary information which make the investigations about them and the corresponded stabilized subspaces easier. These subsets are independent (group) generators of the stabilizer groups with their size being the logarithm of the order of the stabilizer groups.

Lemma 3.1: For every non-trivial subgroup S of $\mathcal{P}_n$ such that $-I_n \notin S$, $|S| = 2^m$ for some $m \in \{1, \cdots, n\}$, where m is the number of any independent generator of S.

proof : We prove by induction. Suppose that S is a non-trivial subgroup of $\mathcal{P}_n$ such that $-I_n \notin S$ that is generated by just one non-identity element g. Then $g^2 = I_n$ and hence $S = \langle g \rangle = \{I_n, g\}$ and thus $|S| = 2^1$.
Now suppose that for every subgroup S of $\mathcal{P}_n$ with an independent generator of size $m \geq 1$ such that $-I_n \notin S$, $|S| = 2^m$. Now let $\tilde{S}$ be a subgroup of $\mathcal{P}_n$ generated by an independent generator $\{g_1, \cdots, g_{m+1}\}$ which does not contain $-I_n$. Then according to the assumption of induction $|\langle g_1, \cdots, g_m \rangle| = 2^m$. But considering that $g_{m+1}^2 = I_n$ and all elements of $\tilde{S}$, and in particular all elements of the generating set, commute (according to [proposition 3.4]), it is clearly seen that

$$\langle g_1, \cdots, g_{m+1} \rangle = \langle g_1, \cdots, g_m \rangle \cup g_{m+1} \langle g_1, \cdots, g_m \rangle . \tag{6}$$

But since g_{m+1} is out of $\langle g_1, \cdots, g_m \rangle$, $g_{m+1} \langle g_1, \cdots, g_m \rangle$ is a coset of $\langle g_1, \cdots, g_m \rangle$ in S distinct from $\langle g_1, \cdots, g_m \rangle$ itself. Therefore, $|g_{m+1} \langle g_1, \cdots, g_m \rangle| = |\langle g_1, \cdots, g_m \rangle| = 2^m$, and hence

$$|S| = |\langle g_1, \cdots, g_{m+1} \rangle| = |\langle g_1, \cdots, g_m \rangle| + |g_{m+1} \langle g_1, \cdots, g_m \rangle| = 2^{m+1}. \tag{7}$$

Moreover, according to [proposition 3.5], every subgroup S of $\mathcal{P}_n$ such that $-I_n \notin S$ is isomorphic to a subgroup of the quotient group $\mathcal{P}_n / K_n$ where $K_n := \{cI_n \mid c \in \{-1, 1, -i, i\}\}$ which must be abelian accordingly. But it is known that [13] the maximally commutative subgroups of $\mathcal{P}_n / K_n$ have size 2^n. Therefore every subgroup of $\mathcal{P}_n$ such that $-I_n \notin S$ must be of size 2^m for some $m \in \{1, \cdots, n\}$.

□

An important problem of concern is to find a relation between the size of a subgroup of $\mathcal{P}_n$ that does not contain $-I_n$, and the vector-space stabilized by it. To find such a useful relation we introduce a representation of the elements of the Pauli group $\mathcal{P}_n$ by classical bits. Precisely, there exists a bijection from $\mathcal{P}_n$ to $\mathbb{F}_2^2 \times \mathbb{F}_2^{2n}$ defined as follows.

Definition 3.2: Define the function $\mathbf{r}^{(n)} : \mathcal{P}_n \to \mathbb{F}_2^{2n}$ as follows. For any $c\, O_1 \otimes \cdots \otimes O_n \in \mathcal{P}_n$ (discard the coefficient c),

$$\begin{aligned}
\mathbf{r}_k^{(n)}\left(c\, O_1 \otimes \cdots \otimes O_n\right) &\stackrel{\text{def}}{=} 0, \quad O_k \in \{I, Z\}, \\
\mathbf{r}_k^{(n)}\left(c\, O_1 \otimes \cdots \otimes O_n\right) &\stackrel{\text{def}}{=} 1, \quad O_k \in \{X, Y\}, \\
\mathbf{r}_{n+k}^{(n)}\left(c\, O_1 \otimes \cdots \otimes O_n\right) &\stackrel{\text{def}}{=} 0, \quad O_k \in \{I, X\}, \\
\mathbf{r}_{n+k}^{(n)}\left(c\, O_1 \otimes \cdots \otimes O_n\right) &\stackrel{\text{def}}{=} 1, \quad O_k \in \{Y, Z\},
\end{aligned} \tag{8}$$

where $\mathbf{r}_j^{(n)}(g)$ denotes the j-th component of the vector $\mathbf{r}^{(n)}(g)$ in $\mathbb{F}_2^{2n}$.
Define the function $\mathbf{R}^{(n)} : \mathcal{P}_n \to \mathbb{F}_2^2 \times \mathbb{F}_2^{2n}$ as,

$$\forall\, c\, O_1 \otimes \cdots \otimes O_n \in \mathcal{P}_n\colon\ \mathbf{R}^{(n)}\left(c\, O_1 \otimes \cdots \otimes O_n\right) \stackrel{\text{def}}{=} \left(\alpha(c), \mathbf{r}^{(n)}\left(c\, O_1 \otimes \cdots \otimes O_n\right)\right), \tag{9}$$

where $\alpha : \{1, -1, i, -i\} \to \mathbb{F}_2^2$ is defined as,

$$\begin{aligned}
\alpha(1) &\stackrel{\text{def}}{=} (0,\, 0), \\
\alpha(-1) &\stackrel{\text{def}}{=} (0,\, 1), \\
\alpha(i) &\stackrel{\text{def}}{=} (1,\, 0), \\
\alpha(i) &\stackrel{\text{def}}{=} (1,\, 1).
\end{aligned} \tag{10}$$

■

Proposition 3.6: $\mathbf{R}^{(n)}$ is a bijection from $\mathcal{P}_n$ to $\mathbb{F}_2^2 \times \mathbb{F}_2^{2n}$.

proof : It is straightforward.

□

Proposition 3.7: $\mathbf{r}^{(n)}$ is a group homomorphism from $\mathcal{P}_n$ to the additive group of $\mathbb{F}_2^n$. That is,

$$\forall\, g_1, g_2 \in \mathcal{P}_n\colon\ \mathbf{r}^{(n)}(g_1 g_2) = \left[\mathbf{r}^{(n)}(g_1)\right]\left[\mathbf{r}^{(n)}(g_2)\right]. \tag{11}$$

proof : It suffices to check this when $n = 1$, since the function $\mathbf{r}^{(n)}$ works on each factor of any tensor products of one-qubit Pauli operators independently.

We have $\mathbf{r}^{(1)}(XX) = \mathbf{r}^{(1)}(I) = (0, 0)$, and $\mathbf{r}^{(1)}(X) + \mathbf{r}^{(1)}(X) = (1, 0) + (1, 0) = (0, 0)$. Therefore, $\mathbf{r}^{(1)}(XX) = \mathbf{r}^{(1)}(X) + \mathbf{r}^{(1)}(X)$. Similarly, $\mathbf{r}^{(1)}(YY) = \mathbf{r}^{(1)}(Y) + \mathbf{r}^{(1)}(Y)$, and $\mathbf{r}^{(1)}(ZZ) = \mathbf{r}^{(1)}(Z) + \mathbf{r}^{(1)}(Z)$.
Moreover $\mathbf{r}^{(1)}(XZ) = \mathbf{r}^{(1)}(iY) = \mathbf{r}^{(1)}(Y) = (1, 1)$, and $\mathbf{r}^{(1)}(X) + \mathbf{r}^{(1)}(Z) = (1, 0) + (0, 1) = (1, 1)$, and thus $\mathbf{r}^{(1)}(XZ) = \mathbf{r}^{(1)}(X) + \mathbf{r}^{(1)}(Z)$. Other cases can be checked similarly.

□

Let Λ_{2n} denote the $2n \times 2n$ symplectic matrix (over $\mathbb{F}_2$), that is,

$$\Lambda_{2n} := \begin{bmatrix} 0_n & I_n \\ I_n & 0 \end{bmatrix}. \tag{12}$$

It can be checked that a pair g_1, g_2 of elements of $\mathcal{P}_n$ commute if and only if

$$\left[\mathbf{r}^{(n)}(g_1)\right] \Lambda_{2n} \left[\mathbf{r}^{(n)}(g_2)\right]^\top = 0. \tag{13}$$

Any tuple $(g_1, \cdots, g_l)$ of elements of $\mathcal{P}_n$ can be represented by a $l \times 2n$ binary matrix, which is constructed by setting the k-th row as the binary vector $\mathbf{r}^{(n)}(g_k)$, and referred to as the "check-matrix of the tuple $(g_1, \cdots, g_l)$". For example, in the case of $n = 4$ by setting

$$\begin{aligned} g_1 &:= X \otimes X \otimes I \otimes Y, \\ g_2 &:= I \otimes I \otimes Z \otimes Z, \\ g_3 &:= Y \otimes Y \otimes Y \otimes Y \end{aligned} \tag{14}$$

the check-matrix associated with the tuple (g_1, g_2, g_3) becomes to be

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}. \tag{15}$$

Lemma 3.2: Let S be a non-trivial subgroup of $\mathcal{P}_n$ such that $-I_n \notin S$, and $S = \langle g_1, \cdots, g_l \rangle$. $\{g_1, \cdots, g_l\}$ is an independent set of elements in $\mathcal{P}_n$ if and only if the set of rows of the check-matrix associated with the tuple $(g_1, \cdots, g_l)$ is a linearly independent subset of the vector-space $\mathbb{F}_2^{2n}$ (over the field $\mathbb{F}_2$).

proof : the set of rows of the check-matrix associated with the tuple $(g_1, \cdots, g_l)$ is linearly independent if and only if there exists a tuple $(a_1, \cdots, a_l) \in \mathbb{F}_2^l$ such that $\sum_{k=1}^{l} a_k \mathbf{r}^{(n)}(g_k) = 0$ and $a_j = 1$ for some j, if and only if (according to [proposition 3.7]) there exists a tuple $(a_1, \cdots, a_l) \in \mathbb{F}_2^l$ such that $g_1^{a_1} \cdots g_l^{a_l} = I_n$ and $a_j = 1$ for some j, if and only if there exists a tuple $(a_1, \cdots, a_l) \in \mathbb{F}_2^l$ such that $g_j = g_1 \cdots g_{j-1} g_{j+1} \cdots g_l$ for some j (since $g_j = g_j^{-1} = {g_j}^\dagger$ according to [proposition 3.3]), if and only if $\{g_1, \cdots, g_l\}$ is not an independent set of elements in $\mathcal{P}_n$.

□

Proposition 3.8: Let S be a non-trivial subgroup of $\mathcal{P}_n$ such that $-I_n \notin S$, and $S = \langle g_1, \cdots, g_l \rangle$, where $\{g_1, \cdots, g_l\}$ is an independent set of operators in $\mathcal{P}_n$. For every $k \in \{1, \cdots, l\}$ there exists $h_k \in \mathcal{P}_n$ such that $h_k g_k {h_k}^\dagger = -g_k$ and $h_k g_j {h_k}^\dagger = g_j$ for every $j \neq k$.

proof : Let R denote the check-matrix associated with the tuple $(g_1, \cdots, g_l)$. According to [lemma 3.2], the rows of R forms a linearly independent set of vectors. $R\Lambda_{2n}$ trnsforms R to again a $l \times 2n$ matrix by switching the positions of left and right halves of every row vectors. Therefore the rows of $\mathbb{R}\Lambda_{2n}$ forms a set of linearly independent set again. Hence, for every $k \in \{1, \cdots, l\}$ there exists $x_k \in \mathbb{F}_2^{2n}$ such that $R\Lambda_{2n} {x_k}^\top = e_k$, where $(e_1, \cdots, e_l)$ denotes the standard ordered basis of $\mathbb{F}_2^l$. For every k let h_k be an element of $\mathcal{P}_n$ such that $\mathbf{r}^{(n)}(h_k) = x_k$. Then clearly $\left[\mathbf{r}^{(n)}(g_j)\right] \Lambda_{2n} \left[\mathbf{r}^{(n)}(h_k)\right] = \delta_{jk}$ which means g_j commutes with h_k if and only if $j \neq k$.

□

Lemma 3.3: Let S be a non-trivial subgroup of $\mathcal{P}_n$ that does not contain $-I_n$. Let $\{g_1, \cdots, g_m\}$ be an independent generator of S. Let $P^{(S)}$ denote the orthogonal projection onto $\mathcal{V}_S$. Then for every j, k, $I_n + g_j$ and $I_n - g_j$ commute with both $I_n + g_k$ and $I_n - g_k$, and

$$P^{(S)} = \frac{1}{2^m} \prod_{k=1}^{m} (I_n + g_k). \tag{16}$$

proof : For every j, k, since $g_j g_k = g_k g_j$,

$$\begin{aligned}(I_n + g_j)(I_n + g_k) &= I_n + g_j + g_k + g_j g_k \\ &= I_n + g_k + g_j + g_k g_j = (I_n + g_k)(I_n + g_j). \end{aligned} \tag{17}$$

Other cases can be shown similarly.

For every $g \in S \setminus \{I_n\}$ let Π_g denote the orthogonal projection onto the eigenspace of g corresponded to the eigenvalue 1, and let V_g denote this eigenspace which is the image of Π_g. We know that for every $g \in S$,

$$\Pi_g = \frac{1}{2}(I_n + g), \tag{18}$$

and $v \in V_g$ if and only if $\Pi_g v = v$. Furthermore, since for every $g, g' \in S$, Π_g and $\Pi_{g'}$ commute, $\left(\prod_{g\in S} \Pi_g\right) v = v$ if and only if $\Pi_g v = v$ for every $g \in S$ (because $\Pi_g^2 = \Pi_g$), and hence if and only if $v \in \bigcap_{g\in S} V_g = \mathcal{V}_S$. Moreover, considering that every Π_g and $\Pi_{g'}$ commute, $\prod_{g\in S} \Pi_g$ is an orthogonal projection because then it is straightforward to check that $\left[\prod_{g\in S} \Pi_g\right]^2 = \prod_{g\in S} \Pi_g$ and $\prod_{g\in S} \Pi_g$ is Hermitian. Therefore, it is concluded that,

$$P_S = \prod_{g\in S} \Pi_g. \tag{19}$$

But since every $g, g' \in S$ commute and $g^2 = I_n$ for every $g \in S$, and every $g \in S$ is a finite product of elements from $\{g_1, \cdots, g_n\}$, a simple calculation shows that,

$$\prod_{g\in S} \Pi_g = \prod_{g\in S} \left[\frac{1}{2}(I_n + g)\right] = \frac{1}{2^m} \prod_{k=1}^{m} (I_n + g_k). \tag{20}$$

□

Theorem 3.1: Let S be a subgroup of $\mathcal{P}_n$ that does not contain $-I_n$. The dimension of $\mathcal{V}_S$ equals $2^{n-\log_2 |S|}$.

proof : According to [lemma 3.1], $|S| = 2^m$ for some $m \in \{1, \cdots, n\}$ and there is an independent set of operators $\{g_1, \cdots, g_m\}$ such that $S = \langle g_1, \cdots, g_n \rangle$. For every $\mathbf{x} := (x_1, \cdots, x_m) \in \mathbb{F}_2^m$, we define

$$P_{\mathbf{x}} := \frac{1}{2^m} \prod_{k=1}^{m} (I_n + (-1)^{x_k} g_k), \tag{21}$$

which is easily seen to be an orthogonal projection according to [lemma 3.3]. Clearly,

$$\begin{aligned}\sum_{\mathbf{x}\in\mathbb{F}_2^m} P_{\mathbf{x}} &= \frac{1}{2^m}\sum_{\mathbf{x}\in\mathbb{F}_2^n}\prod_{k=1}^{m}\left(I_n+(-1)^{x_k}\,g_k\right)\\ &= \frac{1}{2^m}\left[(I_n+g_1)+(I_n-g_1)\right]\cdots\left[(I_n+g_m)+(I_n-g_m)\right]\\ &= I_n. \end{aligned} \tag{22}$$

Moreover, if $\mathbf{x}\neq\mathbf{x}'$ then there exists a k such that $x_k\neq x'_k$, and hence $P_{\mathbf{x}}P_{\mathbf{x}'}$ includes the term $(I_n+g_k)(I_n-g_k)$ in its expansion, and hence considering that $(I_n+g_k)(I_n-g_k)=0$ it becomes evident that $P_{\mathbf{x}}P_{\mathbf{x}'}=0$ which means the orthogonal projections are pairwise orthogonal. Therefore knowing that $\{P_{\mathbf{x}}\mid\mathbf{x}\in\mathbb{F}_2^m\}$ is a collection of pairwise-orthogonal orthogonal projections that add up to unity, it becomes clear that,

$$\sum_{\mathbf{x}\in\mathbb{F}_2^m}\dim\left[\mathsf{img}\left(P_{\mathbf{x}}\right)\right]=\dim\left(\mathcal{H}^{\otimes n}\right)=2^n, \tag{23}$$

where $\mathsf{img}\left(P_{\mathbf{x}}\right)$ denotes the image of the orthogonal projection $P_{\mathbf{x}}$ which is the subspace onto which $P_{\mathbf{x}}$ is the orthogonal projection. According to [proposition 3.8], it can be easily seen that for every $\mathbf{x}\in\mathbb{F}_2^m$ there exists $g_{\mathbf{x}}\in\mathcal{P}_n$ such that,

$$g_{\mathbf{x}}P_{\mathbf{0}}{g_{\mathbf{x}}}^{\dagger}=P_{\mathbf{x}}, \tag{24}$$

where,

$$P_{\mathbf{0}}=\frac{1}{2^m}\prod_{k=1}^{m}\left(I_n+g_k\right), \tag{25}$$

which according to [lemma 3.3] is the orthogonal projection onto $\mathcal{V}_S$, and hence

$$\dim\left[\mathsf{img}\left(P_{\mathbf{0}}\right)\right]=\dim\left(\mathcal{V}_S\right). \tag{26}$$

Moreover for every since $\mathbf{x}\in\mathbb{F}_2^m$, $g_{\mathbf{x}}$ is an isometry of $\mathcal{H}^{\otimes n}$,

$$\dim\left[\mathsf{img}\left(g_{\mathbf{x}}P_{\mathbf{0}}{g_{\mathbf{x}}}^{\dagger}\right)\right]=\dim\left[\mathsf{img}\left(P_{\mathbf{0}}\right)\right], \tag{27}$$

and therefore for every $\mathbf{x}\in\mathbb{F}_2^m$,

$$\dim\left[\mathsf{img}\left(P_{\mathbf{x}}\right)\right]=\dim\left(\mathcal{V}_S\right). \tag{28}$$

Therefore, since $|\mathbb{F}_2^m| = 2^m$,

$$2^m \dim(\mathcal{V}_S) - 2^n, \tag{29}$$

and hence,

$$\dim(\mathcal{V}_S) = 2^{n-m} = 2^{n-\log_2|S|}. \tag{30}$$

□

The normalizer of $\mathcal{P}_n$ in $\mathcal{U}_n$, that is $\mathrm{N}_{\mathcal{U}_n}(\mathcal{P}_n)$, is referred to as the "Clifford group on n qubits" or simply the "n-Clifford group", and is denoted by $\mathcal{C}_n$. So in other words,

$$\begin{aligned}\mathcal{C}_n :&= \left\{U \in \mathcal{U}_n \mid U\mathcal{P}_n U^{-1} = \mathcal{P}_n\right\} = \left\{U \in \mathcal{U}_n \mid U\mathcal{P}_n U^\dagger = \mathcal{P}_n\right\} \\ &= \left\{U \in \mathcal{U}_n \mid \left[\forall T \in \mathcal{P}_n\colon\ UTU^\dagger \in \mathcal{P}_n\right]\right\}.\end{aligned} \tag{31}$$

It is known that the center of the unitary group $\mathcal{U}_n$, that is $\mathcal{Z}(\mathcal{U}_n)$, equals the subgroup of all scalar operators which is isomorphic to the unitary group of degree 1. That is,

$$\mathcal{Z}(\mathcal{U}_n) = \{\exp(i\theta) I_n \mid \theta \in [0, 2\pi)\} \cong U(1). \tag{32}$$

Trivially, $\mathcal{C}_n$ includes $\mathcal{Z}(\mathcal{U}_n)$, and $\mathcal{Z}(\mathcal{U}_n)$ is a normal subgroup of $\mathcal{U}_n$. Therefore, $\mathcal{Z}(\mathcal{U}_n)$ is a normal subgroup of $\mathcal{C}_n$, and hence the quotient group $\mathcal{C}_n/\mathcal{Z}(\mathcal{U}_n)$ is well-defined. Since in quantum mechanics two unitary transformations are considered to be equivalent if they differ by just a scalar coefficient (which then inevitably must be in S^1), working with the group $\mathcal{C}_n/\mathcal{Z}(\mathcal{U}_n)$ instead of $\mathcal{C}_n$ will not lead to any loss of information. We define,

$$\tilde{\mathcal{C}}_n := \mathcal{C}_n/\mathcal{Z}(\mathcal{U}_n), \tag{33}$$

which is a finite group of order $2^{n^2+2n}\prod_{k=1}^{n} 4^k - 1$. The name "$n$-Clifford group" will be then used interchangeably to refer to both $\mathcal{C}_n$ and $\tilde{\mathcal{C}}_n$. The n-Clifford group

$\tilde{\mathcal{C}}_n$ is generated by the single-qubit Hadamard and Phase gates together with the two-qubit controlled-NOT gates. Precisely, by defining,

$$\mathcal{C}_n = \left\langle \left\{ H_i^{(n)} \mid i = 1, \cdots, n \right\} \cup \left\{ S_i^{(n)} \mid i = 1, \cdots, n \right\} \cup \left\{ C_{[i,j]}^{(n)}(X) \mid i, j = 1, \cdots, n,\ i \neq j \right\} \right\rangle \tag{34}$$

it has been proved that $\mathcal{C}_n \subset \mathcal{C}_n$, and

$$\tilde{\mathcal{C}}_n = \{[O] \mid O \in \mathcal{C}_n\}, \tag{35}$$

where $[O]$ denotes the coset in $\mathcal{C}_n / \mathcal{Z}(\mathcal{U}_n)$ to which O belongs.

3.2 The Stabilizer States

Let n be a positive integer.

Definition 3.3: Let $|\psi\rangle$ be a quantum state in $\mathcal{H}^{\otimes n}$. The "stabilizer group of $|\psi\rangle$", denoted by $\mathrm{ST}(|\psi\rangle)$ is defined to be the set of all unitary transformations of $\mathcal{H}^{\otimes n}$ having $|\psi\rangle$ as an eigenvector with eigenvalue 1. That is,

$$\mathrm{ST}(|\psi\rangle) := \{U \in \mathcal{U}_n \mid U|\psi\rangle = |\psi\rangle\}. \tag{36}$$

Any $U \in \mathrm{ST}(|\psi\rangle)$ is said to "stabilize $|\psi\rangle$".

■

Lemma 3.4: Let $|\psi\rangle$ be a quantum state in $\mathcal{H}^{\otimes n}$. $\mathrm{ST}(|\psi\rangle)$ is a subgroup of $\mathcal{U}_n$.

proof: Trivially, $I_n \in \mathrm{ST}(|\psi\rangle)$, and hence $\mathrm{ST}(|\psi\rangle) \neq \emptyset$. Let $U, V \in \mathrm{ST}(|\psi\rangle)$. Then $U|\psi\rangle = V|\psi\rangle = |\psi\rangle$, and hence,

$$\left(UV^{-1}\right)|\psi\rangle = \left(UV^{-1}\right)(V|\psi\rangle) = \left(UV^{-1}V\right)|\psi\rangle = U|\psi\rangle = |\psi\rangle, \tag{37}$$

and thus $UV^{-1} \in \mathrm{ST}(|\psi\rangle)$.

□

Lemma 3.5: The function ST from $\mathcal{Q}_n / \sim$ to the set of all subgroups of $\mathcal{U}_n$ is injective, and therefore every quantum state $|\psi\rangle$ is uniquely determined by its stabilizer group $\mathrm{ST}(|\psi\rangle)$, upto a phase factor.

proof : Let $\mathrm{ST}(|\psi\rangle) = \mathrm{ST}(|\phi\rangle)$. There exists an orthonormal basis of $\mathcal{H}^{\otimes n}$ containing $|\psi\rangle$, that is a set of pairwise orthogonal quantum states $\{|\psi\rangle, |\psi_1\rangle, \cdots, |\psi_{N-1}\rangle\}$, where $N := 2^n$. For any tuple of real numbers $(\alpha_1, \cdots, \alpha_{N-1})$ we define the unitary operator $U(\alpha_1, \cdots, \alpha_{N-1})$ as,

$$U(\alpha_1, \cdots, \alpha_{N-1}) := |\psi\rangle\langle\psi| + e^{i\alpha_1}|\psi_1\rangle\langle\psi_1| + \cdots + e^{i\alpha_{N-1}}|\psi_{N-1}\rangle\langle\psi_{N-1}|. \quad (38)$$

Clearly for every $\alpha_1, \cdots, \alpha_{N-1} \in \mathbb{R}$, $U(\alpha_1, \cdots, \alpha_{N-1}) \in \mathrm{ST}(|\psi\rangle)$, and hence $U(\alpha_1, \cdots, \alpha_{N-1}) \in \mathrm{ST}(|\phi\rangle)$. Therefore, for every $\alpha_1, \cdots, \alpha_{N-1} \in \mathbb{R}$,

$$|\psi\rangle\langle\psi|\phi\rangle + e^{i\alpha_1}|\psi_1\rangle\langle\psi_1|\phi\rangle + \cdots + e^{i\alpha_{N-1}}|\psi_{N-1}\rangle\langle\psi_{N-1}|\phi\rangle = |\phi\rangle, \quad (39)$$

which implies $|\phi\rangle = e^{i\beta}|\psi\rangle$ for some $\beta \in \mathbb{R}$, which means $|\psi\rangle$ and $|\phi\rangle$ belong to the same element in $\mathcal{Q}_n/\sim$.

□

Proposition 3.9: The set of all elements of $\mathcal{P}_n$ that stabilize the state $|0\rangle^{\otimes n}$ is $\left\langle Z_1^{(n)}, \cdots, Z_n^{(n)} \right\rangle$. That is,

$$\mathrm{ST}\left(|0\rangle^{\otimes n}\right) \cap \mathcal{P}_n = \left\langle Z_1^{(n)}, \cdots, Z_n^{(n)} \right\rangle. \quad (40)$$

proof : It can be easily proved by induction on n.

□

Lemma 3.6: Let $U \in \mathcal{C}_n$. The map $\chi_U : \mathcal{P}_n \to \mathcal{P}_n$ defined as $\chi_U(g) := UgU^\dagger$ is a group-automorphism.

proof : According to the definition of the Clifford group, it is trivial that χ_U is onto.

If $\chi_U(g_1) = \chi_U(g_2)$, then $Ug_1U^\dagger = Ug_2U^\dagger$, and hence $g_1 = g_2$. Therefore, χ_U is injective.

For every $g_1, g_2 \in \mathcal{P}_n$,

$$\chi_U(g_1g_2) = U(g_1g_2)U^\dagger = Ug_1U^\dagger Ug_2U^\dagger = \chi_U(g_1)\chi_U(g_2), \quad (41)$$

which means χ_U is a group-homomorphism.

□

Proposition 3.10: Let S be a subgroup of $\mathcal{P}_n$ such that $-I_n \notin S$, and let $U \in \mathcal{C}_n$ and $S' := USU^\dagger = \left\{UgU^\dagger \mid g \in S\right\}$. Then,

$$\mathcal{V}_{S'} = U\mathcal{V}_S = \left\{U(v) \mid v \in \mathcal{V}_S\right\}. \tag{42}$$

proof: Let $v \in U\mathcal{V}_S$. Then there exists $u \in \mathcal{V}_S$ such that $v = U(u)$. Therefore, considering that for every $g \in S$, $g(u) = u$,

$$\forall\, g \in S\colon\ UgU^\dagger(v) = UgU^\dagger(U(u)) = Ug(u) = U(g(u)) = U(u) = v, \tag{43}$$

which means $v \in \mathcal{V}_{S'}$. Therefore, $U\mathcal{V}_S \subseteq \mathcal{V}_{S'}$. Furthermore, since U is a unitary operator and hence an isometry of $\mathcal{H}^{\otimes n}$, it is clear that $\dim(U\mathcal{V}_S) = \dim(\mathcal{V}_S)$. On the other hand, according to [lemma 3.6], $|S'| = |S|$, and hence according to [theorem 3.1], $\dim(\mathcal{V}_S) = \dim(\mathcal{V}_{S'})$, and thus $\dim(U\mathcal{V}_S) = \dim(\mathcal{V}_{S'})$. So, $U\mathcal{V}_S = \mathcal{V}_{S'}$.

□

Proposition 3.11: Let $|\psi\rangle$ be a quantum state in $\mathcal{H}^{\otimes n}$, and let U be a unitary operator on $\mathcal{H}^{\otimes n}$. Then,

$$\mathrm{ST}(U|\psi\rangle) = U(\mathrm{ST}(|\psi\rangle))U^\dagger = \left\{UTU^\dagger \mid T \in \mathrm{ST}(|\psi\rangle)\right\}. \tag{44}$$

proof: For every $T \in \mathrm{ST}(|\psi\rangle)$, $UTU^\dagger(U|\psi\rangle) = UT|\psi\rangle = U|\psi\rangle$, and hence $UTU^\dagger \in \mathrm{ST}(U|\psi\rangle)$. Therefore, $U(\mathrm{ST}(|\psi\rangle))U^\dagger \subseteq \mathrm{ST}(U|\psi\rangle)$.
Now let $T \in \mathrm{ST}(U|\psi\rangle)$. Then $TU|\psi\rangle = U|\psi\rangle$, and hence $U^\dagger TU|\psi\rangle = |\psi\rangle$, and therefore $g := U^\dagger TU \in \mathrm{ST}(|\psi\rangle)$, and thus $T = UgU^\dagger$ and hence $T \in U(\mathrm{ST}(|\psi\rangle))U^\dagger$.

□

Proposition 3.12: Let $|\psi\rangle$ be a quantum state in $\mathcal{H}^{\otimes n}$, and let $U \in \mathcal{C}_n$. Then,

$$\mathrm{ST}(U|\psi\rangle) \cap \mathcal{P}_n = \left\{UTU^\dagger \mid T \in \mathrm{ST}(|\psi\rangle) \cap \mathcal{P}_n\right\}, \tag{45}$$

and hence according to [lemma 3.6], $|\mathrm{ST}(U|\psi\rangle) \cap \mathcal{P}_n| = |\mathrm{ST}(|\psi\rangle) \cap \mathcal{P}_n|$.

proof : According to [proposition 3.11],

$$\mathrm{ST}\left(U\left|\psi\right\rangle\right)\cap\mathcal{P}_n=\left\{UTU^\dagger\mid T\in\mathrm{ST}\left(\left|\psi\right\rangle\right)\right\}\cap\mathcal{P}_n. \tag{46}$$

Considering that $U\in\mathcal{C}_n$, it is easy to see that if $T\notin\mathcal{P}_n$ then $UTU^\dagger\notin\mathcal{P}_n$. This is because if $UTU^\dagger\in\mathcal{P}_n$ then $T=U^\dagger gU$ for some $g\in\mathcal{P}_n$, and since $U^\dagger\in\mathcal{C}_n$ (considering that $\mathcal{C}_n$ is a group), clearly $T\in\mathcal{P}_n$. So $T\in\mathcal{P}_n$ if and only if $UTU^\dagger\in\mathcal{P}_n$. Therefore,

$$\left\{UTU^\dagger\mid T\in\mathrm{ST}\left(\left|\psi\right\rangle\right)\right\}\cap\mathcal{P}_n=\left\{UTU^\dagger\mid T\in\mathrm{ST}\left(\left|\psi\right\rangle\right)\cap\mathcal{P}_n\right\}. \tag{47}$$

□

Theorem 3.2: Let $\left|\psi\right\rangle$ be a quantum state in $\mathcal{H}^{\otimes n}$. The followings are equivalent.

i. There exists $U\in\mathcal{C}_n$ such that $\left|\psi\right\rangle=U\left|0\right\rangle^{\otimes n}$.

ii. $\left|\mathrm{ST}\left(\left|\psi\right\rangle\right)\cap\mathcal{P}_n\right|=2^n$. That is, the number of all elements of the n-Pauli group that stabilize $\left|\psi\right\rangle$ is 2^n.

iii. $\left|\psi\right\rangle$ is uniquely determined by $\mathrm{ST}\left(\left|\psi\right\rangle\right)\cap\mathcal{P}_n$, upto a phase factor.

proof :

i→**ii**: Assume that there exists $U\in\mathcal{C}_n$ such that $\left|\psi\right\rangle=U\left|0\right\rangle^{\otimes n}$. According to [proposition 3.9] and [proposition 3.12],

$$\begin{aligned}\left|\mathrm{ST}\left(\left|\psi\right\rangle\right)\cap\mathcal{P}_n\right|&=\left|\mathrm{ST}\left(U\left|0\right\rangle^{\otimes n}\right)\cap\mathcal{P}_n\right|\\&=\left|\left\langle Z_1^{(n)},\cdots,Z_n^{(n)}\right\rangle\right|.\end{aligned} \tag{48}$$

Since $\left\{Z_1^{(n)},\cdots,Z_n^{(n)}\right\}$ is an independent generator of $\mathcal{P}_n$, we have,

$$\left|\left\langle Z_1^{(n)},\cdots,Z_n^{(n)}\right\rangle\right|=2^n. \tag{49}$$

Therefore,

$$\left|\mathrm{ST}\left(\left|\psi\right\rangle\right)\cap\mathcal{P}_n\right|=2^n. \tag{50}$$

ii↔iii: The determination of $|\psi\rangle$ uniquely by $\mathrm{ST}(|\psi\rangle) \cap \mathcal{P}_n$ upto a phase factor is equivalent to saying that the vector-subspace stabilized by $\mathrm{ST}(|\psi\rangle) \cap \mathcal{P}_n$ is one-dimensional. It is clear that $\mathrm{ST}(|\psi\rangle)$ does not contain $-I_n$ because otherwise $|\psi\rangle$ must be the zero vector, which obviously is not the case. Therefore, based on [theorem 3.1], the vector-subspace stabilized by $\mathrm{ST}(|\psi\rangle) \cap \mathcal{P}_n$ is one-dimensional if and only if $|\mathrm{ST}(|\psi\rangle) \cap \mathcal{P}_n| = 2^n$. So, the determination of $|\psi\rangle$ uniquely by $\mathrm{ST}(|\psi\rangle) \cap \mathcal{P}_n$ upto a phase factor is equivalent to the condition that $|\mathrm{ST}(|\psi\rangle) \cap \mathcal{P}_n| = 2^n$.
ii→i: Suppose that $|\mathrm{ST}(|\psi\rangle) \cap \mathcal{P}_n| = 2^n$. Since $\mathrm{ST}(|\psi\rangle) \cap \mathcal{P}_n$ is a subgroup of $\mathcal{P}_n$ that does not contain $-I_n$, it is clear that has an independent generator $\{g_1, \cdots, g_n\}$ of size n whose elements are also known trivially to be pairwise commuting. Then it is known that [6] there exists $V \in \mathcal{C}_n$ such that for every i,

$$g_i = V Z_i^{(n)} V^\dagger. \tag{51}$$

Since $|\psi\rangle$ is inside the one-dimensional vector-space stabilized by $\{g_1, \cdots, g_n\}$, according to [proposition 3.10] and [proposition 3.9], $|\psi\rangle = V|0\rangle^{\otimes n}$ upto some phase factor.

□

Definition 3.4: Let $|\psi\rangle$ be a quantum state in $\mathcal{H}^{\otimes n}$. $|\psi\rangle$ is called a "n-qubit stabilizer state" if any (and hence all) of the conditions of [theorem 3.2] are satisfied for $|\psi\rangle$.
The set of all n-qubit stabilizer states will be denoted by $\mathcal{S}_n$. Any quantum state in $\mathcal{Q}_n \setminus \mathcal{S}_n$ is called a "n-qubit non-stabilizer state".

■

Definition 3.5: Let $|\psi\rangle$ be a quantum state in $\mathcal{H}^{\otimes n}$.

$$\mathcal{G}(|\psi\rangle) := \mathrm{ST}(|\psi\rangle) \cap \mathcal{P}_n. \tag{52}$$

$\mathcal{G}(|\psi\rangle)$ is called the "Pauli stabilizer group of $|\psi\rangle$".

■

According to [definition 3.2], any stabilizer state $|\psi\rangle$ is uniquely determined by a maximally commuting subgroup of $\mathcal{P}_n$ that does not contain $-I_n$ and hence of size 2^n, which is the Pauli stabilizer group of $|\psi\rangle$. Therefore, any stabilizer state $|\psi\rangle$ can be identified with an independent generator $\{g_1, \cdots, g_n\}$ of the Pauli stabilizer group of $|\psi\rangle$.

Corollary 3.1: Any n-qubit stabilizer state is contained in a one-dimensional subspace of $\mathcal{H}^{\otimes n}$ that is stabilized by a maximally commuting subgroup of size 2^n of $\mathcal{P}_n$ (which does not contain $-I_n$).
The set of all n-qubit stabilizer states equals the set of all unit vectors in the union of all $\mathcal{V}_S$ such that S is a subgroup of $\mathcal{P}_n$ of size 2^n without containing $-I_n$.

□

It is also worthwhile to mention that if a quantum state $|\psi\rangle$ happens to be stabilized by a set S of 2^n distinct Pauli operators, then $|\psi\rangle$ is a stabilizer state and its Pauli stabilizer group must equal S. Let us provide a proof of this claim in the following proposition.

Proposition 3.13: Let $|\psi\rangle$ be a quantum state in $\mathcal{H}^{\otimes n}$. Suppose that there exists $S \subseteq \mathcal{P}_n$ with $|S| = 2^n$ such that for every $g \in S$, $g|\psi\rangle = |\psi\rangle$. Then $|\psi\rangle$ is a stabilizer state and $\mathcal{G}(|\psi\rangle) = S$.

proof: Clearly $S \subseteq \mathcal{G}(|\psi\rangle) = \mathrm{ST}(|\psi\rangle) \cap \mathcal{P}_n$. Since $\mathrm{ST}(|\psi\rangle)$ cannot contain $-I_n$ (because otherwise $|\psi\rangle = 0$), $\mathcal{G}(|\psi\rangle)$ is seen not to contain $-I_n$. But $\mathcal{G}(|\psi\rangle)$ is a subgroup of $\mathcal{P}_n$ (because it is the intersection of the group $\mathrm{ST}(|\psi\rangle)$ with the Pauli group $\mathcal{P}_n$). Therefore $\mathcal{G}(|\psi\rangle)$ is a subgroup of $\mathcal{P}_n$ that does not contain $-I_n$. Therefore, according to [lemma 3.1], $|\mathcal{G}(|\psi\rangle)| \leq 2^n$. So considering that $S \subseteq \mathcal{G}(|\psi\rangle)$ and $|S| = 2^n$, clearly $S = \mathcal{G}(|\psi\rangle)$, and hence $|\mathcal{G}(|\psi\rangle)| = 2^n$, and thus $|\psi\rangle$ is seen to be a stabilizer state according to [definition 3.4].

□

One important feature of the class of all n-qubit stabilizer states is that it is invariant under the action of any Clifford operation.

Proposition 3.14: For every $U \in \mathcal{C}_n$ and every $|\psi\rangle \in \mathcal{S}_n$, $U|\psi\rangle \in \mathcal{S}_n$.

proof : Let $U \in \mathcal{C}_n$ and $|\psi\rangle \in \mathcal{S}_n$. Then according to [definition 3.4], there exists $V \in \mathcal{C}_n$ such that $|\psi\rangle = V|0\rangle^{\otimes n}$. Therefore, $U|\psi\rangle = (UV)|0^{\otimes n}\rangle$. But since $\mathcal{C}_n$ is a group under the composition operation, $UV \in \mathcal{C}_n$, and hence according to [definition 3.4] $|\psi\rangle \in \mathcal{S}_n$.

□

Lemma 3.7: Let $|\psi\rangle \in \mathcal{S}_n$, and let $U \in \mathcal{C}_n$. Let $\mathcal{G}(|\psi\rangle) = \langle g_1, \cdots, g_n\rangle$. Then,

$$\mathcal{G}(U|\psi\rangle) = \left\langle Ug_1U^\dagger, \cdots, Ug_2U^\dagger \right\rangle. \tag{53}$$

proof : According to [proposition 3.12] and [theorem 3.2], and considering that $\{g_1, \cdots, g_n\}$ is independent if and only if $\left\{Ug_1U^\dagger, \cdots, Ug_nU^\dagger\right\}$ is independent, it is clear.

□

3.3 Evolution of Stabilizer States Under Pauli Observables

A quantum measurement in the n-qubit Hilbert space $\mathcal{H}^{\otimes n}$ is a Hermitian operator on $\mathcal{H}^{\otimes n}$. An n-qubit Pauli measurement is defined to be a Hermitian element of the n-Pauli group $\mathcal{P}_n$, that is an element of the set $\{g \in \mathcal{P}_n \mid g^2 = I_n\}$. An n-qubit Pauli measurement is called a "n-qubit Pauli observable" if it is not a trivial measurement I_n or $-I_n$, and hence has $\{-1, +1\}$ as its set of all outcomes (eigenvalues). An important feature of Pauli observables is the fact that measuring stabilizer states by Pauli observables they keep the altered state after the measurement in the class of stabilizer states.

Proposition 3.15: Let O be a n-qubit Pauli observable, and let P_+ and P_- denote the orthogonal projections onto the eigenspaces of O corresponded to the eigenvalues $+1$ and -1, respectively.

$$\begin{aligned} P_+ &= \frac{1}{2}(I_n + O), \\ P_- &= \frac{1}{2}(I_n - O). \end{aligned} \tag{54}$$

proof : According to the spectral theorem, $O = P_+ - P_-$ and $P_+ + P_- = I_n$. Therefore, the desired result is straightforward to observe.

□

Proposition 3.16: Let $|\psi\rangle$ be a stabilizer state, and let O be a n-qubit Pauli observable that commutes with all the elements of the Pauli stabilizer group of $|\psi\rangle$, that is $\mathcal{G}(|\psi\rangle)$. The quantum state after measuring $|\psi\rangle$ upon the observable O will be $|\psi\rangle$ itself definitely, and hence a stabilizer state again.

proof : Since $O \in \mathcal{C}_n$ and $|\psi\rangle$ is a stabilizer state, $O|\psi\rangle$ is also a stabilizer state, and hence is stabilized by exactly 2^n elements of the Pauli group. For every $g \in \mathcal{G}(|\psi\rangle)$, $g|\psi\rangle = |\psi\rangle$. Furthermore, since O commutes with all the elements of $\mathcal{G}(|\psi\rangle)$, for every $g \in \mathcal{G}(|\psi\rangle)$, $gO|\psi\rangle = Og|\psi\rangle = O|\psi\rangle$. Therefore $O|\psi\rangle$ is stabilized by $\mathcal{G}(|\psi\rangle)$, and since it is a stabilizer state $\mathcal{G}(O|\psi\rangle) = \mathcal{G}(|\psi\rangle)$. So according to [theorem 3.2], $O|\psi\rangle$ and $|\psi\rangle$ must differ only by a phase factor, that is $O|\psi\rangle = c|\psi\rangle$ for some $c \in S^1$. But because $O^2 = I_n$, inevitable $c \in \{-1, +1\}$. So either $O|\psi\rangle = |\psi\rangle$ or $O|\psi\rangle = -|\psi\rangle$, and since in each case $|\psi\rangle$ is an eigenvector of O, measuring $|\psi\rangle$ upon O must yield a certain outcome without altering it.

□

Proposition 3.17: Let $|\psi\rangle$ be a stabilizer state with $\mathcal{G}(|\psi\rangle) = \langle g_1, \cdots, g_n\rangle$, and let O be a n-qubit Pauli observable that commutes with all g_i but g_1. Then the probabilities of observing the results -1 and $+1$ upon measuring $|\psi\rangle$ by O are both $\frac{1}{2}$.

Let $|\psi_+\rangle$ and $|\psi_-\rangle$ denote the quantum states after measuring $|\psi\rangle$ upon the observable O and observing the outcomes $+1$ and -1, respectively. Then $|\psi_+\rangle$ and $|\psi_-\rangle$ are stabilizer states, and,

$$\mathcal{G}(|\psi_+\rangle) = \langle O, g_2, \cdots, g_n\rangle, \tag{55}$$

$$\mathcal{G}(|\psi_-\rangle) = \langle -O, g_2, \cdots, g_n\rangle. \tag{56}$$

proof : First we show that $\{O, g_2, \cdots, g_n\}$ and $\{-O, g_2, \cdots, g_n\}$ are independent sets of operators in the Pauli group $\mathcal{P}_n$, which is equivalent to stating that O and

$-O$ are not in the generator of $\{g_2, \cdots, g_n\}$. If $O \in \langle g_2, \cdots, g_n\rangle$ then clearly O has to commute with g_1 since $\langle g_1, \cdots, g_n\rangle$ consists of pairwise commuting elements, which contradicts the assumption of the theorem. Moreover, since $-O$ has the same commuting properties as that of O with $\{g_1, \cdots, g_n\}$, the same argument shows the independence of $\{-O, g_2, \cdots, g_n\}$.

Now according to[proposition 3.15] and the postulate of quantum measurement, for the probabilities of observing the outcomes $+1$ and -1 upon measuring $\ker\psi$ by O, that is $\Pr[O, +1; |\psi\rangle]$ and $\Pr[-1, O; |\psi\rangle]$, respectively, we have,

$$\Pr[O, +1; |\psi\rangle] = \left\langle \psi \middle| \frac{I_n + O}{2} \middle| \psi \right\rangle, \tag{57}$$

$$\Pr[O, -1; |\psi\rangle] = \left\langle \psi \middle| \frac{I_n - O}{2} \middle| \psi \right\rangle. \tag{58}$$

Now considering that $Og_1 = -g_1O$, $g_1 |\psi\rangle = |\psi\rangle$, and ${g_1}^\dagger = g_1$, we have,

$$\begin{aligned}
\Pr[O, +1; |\psi\rangle] &= \left\langle \psi \middle| \left(\frac{I_n + O}{2}\right) g_1 \middle| \psi \right\rangle \\
&= \left\langle \psi \middle| g_1 \left(\frac{I_n - O}{2}\right) \middle| \psi \right\rangle \\
&= \left\langle \psi \middle| \frac{I_n - O}{2} \middle| \psi \right\rangle \\
&= \Pr[O, -1; |\psi\rangle].
\end{aligned} \tag{59}$$

Accordingly, considering that $\Pr[O, +1; |\psi\rangle] + \Pr[O, -1; |\psi\rangle] = 1$ (since O has two outcomes), it is seen that,

$$\Pr[O, +1; |\psi\rangle] = \Pr[O, -1; |\psi\rangle] = \frac{1}{2}. \tag{60}$$

According to the postulate of quantum measurement,

$$|\psi_+\rangle = \left(\frac{I_n + O}{2}\right) |\psi\rangle, \tag{61}$$

$$|\psi_-\rangle = \left(\frac{I_n - O}{2}\right) |\psi\rangle. \tag{62}$$

For every $k \in \{2, \cdots, n\}$, considering that $g_k |\psi\rangle = |\psi\rangle$ and $g_k O = O g_k$,

$$\begin{aligned} g_k |\psi_+\rangle &= \left(\frac{g_k + g_k O}{2}\right) |\psi\rangle \\ &= \left(\frac{g_k + O g_k}{2}\right) |\psi\rangle \\ &= \left(\frac{I_n + O}{2}\right) g_k |\psi\rangle \\ &= \left(\frac{I_n + O}{2}\right) |\psi\rangle = |\psi_+\rangle , \end{aligned} \tag{63}$$

and

$$\begin{aligned} g_k |\psi_-\rangle &= \left(\frac{g_k - g_k O}{2}\right) |\psi\rangle \\ &= \left(\frac{g_k - O g_k}{2}\right) |\psi\rangle \\ &= \left(\frac{I_n - O}{2}\right) g_k |\psi\rangle \\ &= \left(\frac{I_n - O}{2}\right) |\psi\rangle = |\psi_-\rangle . \end{aligned} \tag{64}$$

Moreover, considering that $O^2 = I_n$ (since it is a Pauli observable),

$$O |\psi_+\rangle = O \left(\frac{I_n + O}{2}\right) |\psi\rangle = \left(\frac{O + I_n}{2}\right) |\psi\rangle = |\psi_+\rangle , \tag{65}$$

$$(-O) |\psi_-\rangle = (-O) \left(\frac{I_n - O}{2}\right) |\psi\rangle = \left(\frac{-O + I_n}{2}\right) |\psi\rangle = |\psi_-\rangle . \tag{66}$$

Therefore, it is seen that $\{O, g_2, \cdots, g_n\}$ is an independent set of operators in $\mathcal{P}_n$ such that $\langle O, g_2, \cdots, g_n\rangle$ stabilize $|\psi_+\rangle$. Moreover, since $O I_n \notin \langle O, g_2, \cdots, g_n\rangle$, $|\langle O, g_2, \cdots, g_n\rangle| = 2^n$. Therefore according to [proposition 3.13], $\mathcal{G}(|\psi_+\rangle) = \langle O, g_2, \cdots, g_n\rangle$, and since $|\mathcal{G}(|\psi\rangle)| = 2^n$, $|\psi_+\rangle$ is a stabilizer state according to [definition 3.4]. A similar reasoning shows that $\mathcal{G}(|\psi_-\rangle) = \langle -O, g_2, \cdots, g_n\rangle$, and hence $|\psi_-\rangle$ is also a stabilizer state.

□

Proposition 3.18: Let $|\psi\rangle$ be a stabilizer state with $\mathcal{G}(|\psi\rangle) = \langle g_1, \cdots, g_n\rangle$, and let O be a n-qubit Pauli observable such that $O g_i = \beta_i \; g_i O$ for every i, with $(\beta_1, \cdots, \beta_n) \in \{-1, 1\}^n$. Without loss of generality we assume that O anti-commutes

with g_1, that is $\beta_1 = -1$. Define,

$$\forall\, k \in \{2, \cdots, n\}\colon\ g'_k := \begin{cases} g_k, & \beta_k = 1, \\ g_1 g_k, & \beta_k = -1, \end{cases} . \tag{67}$$

Then $\{g_1, g'_2, \cdots, g'_n\}$ is an independent set of operators in $\mathcal{P}_n$, $\mathcal{G}(|\psi\rangle) = \langle g_1, g'_2, \cdots, g'_n\rangle$, and O commutes with g'_k for every $k \in \{2, \cdots, n\}$.

proof: It is straightforward.

□

3.4 The Action of $\mathcal{C}_n$ on $\mathcal{P}_n$ by Conjugation

Let n be a positive integer. The action of the n-Clifford group on the n-Pauli group by conjugation as discussed in the [lemma 3.6], that is the mapping $\chi^{(n)} : \mathcal{C}_n \to \mathsf{Aut}(\mathcal{P}_n)$ (which is easily seen to be a homomorphism from the Clifford group to the group of automorphisms of the Pauli group, and hence a group action) contains the information of updating every stabilizer state by any Clifford operator or any Pauli observable (when there is no ambiguity about the number of qubits, $\chi^{(n)}$ will be simply denoted by χ). This is due to the fact that (based on the discussions of the previous sections) a stabilizer state $|\psi\rangle$ can be identified by an independent set of operators $\{g_1, \cdots, g_n\}$ inside the Pauli group $\mathcal{P}_n$, and a Clifford operator $U \in \mathcal{C}_n$ transforms $|\psi\rangle$ to the stabilizer state $U|\psi\rangle$ which is identified by the independent set of operators $\{Ug_1U^\dagger, \cdots, Ug_nU^\dagger\}$ inside $\mathcal{P}_n$, and a Pauli observable O transforms $|\psi\rangle$ to itself or a stabilizer state identified by the independent set $\{O, g_2, \cdots, g_n\}$ or $\{-O, g_2, \cdots, g_n\}$ according to the commutation relation of O to the elements of $\{g_1, g_2, \cdots, g_n\}$ and the observed outcome.

Since two unitary transformations differing by just a phase factor are equivalent in quantum mechanics, we are interested in the quotient group $\mathcal{C}_n/\mathcal{Z}(\mathcal{U}_n)$ as discussed before. Furthermore, automatically the action of two Clifford transformations on $\mathcal{P}_n$ differing by just a phase factor are the same, noting that scalar operators act trivially on $\mathcal{P}_n$. Therefore, since one-qubit Hadamard and phase gates, and two-qubit CNOT gates generate $\mathcal{C}_n/\mathcal{Z}(\mathcal{U}_n)$, the action of any $U \in \mathcal{C}_n$ can be determined by actions of

the operators of this class. But since the Pauli group is also generated by a smaller set, that is the collection of all one-qubit X and Z Pauli operators in $\mathcal{P}_n$, the action of each of these basic Clifford operators on $\mathcal{P}_n$ can be determined by its action on the elements of this generating set of Pauli operators.

Now we list the actions (by conjugation) of (single-qubit) Hadamard and phase operators on the (single-qubit) X and Z operators, and the action of the (two-qubit) CNOT operator on $X \otimes I$, $I \otimes X$, $Z \otimes I$, and $I \otimes Z$ that generate $\mathcal{P}_2$, that can be calculated easily.

$$HXH^\dagger = Z, \tag{68}$$

$$HZH^\dagger = X, \tag{69}$$

$$PXP^\dagger = Y, \tag{70}$$

$$PZP^\dagger = Z, \tag{71}$$

and,

$$C^{(2)}_{[1,2]}(X)\,(X \otimes I)\,C^{(2)}_{[1,2]}(X)^\dagger = X \otimes X, \tag{72}$$

$$C^{(2)}_{[1,2]}(X)\,(I \otimes X)\,C^{(2)}_{[1,2]}(X)^\dagger = I \otimes X, \tag{73}$$

$$C^{(2)}_{[1,2]}(X)\,(Z \otimes I)\,C^{(2)}_{[1,2]}(X)^\dagger = Z \otimes I, \tag{74}$$

$$C^{(2)}_{[1,2]}(X)\,(I \otimes Z)\,C^{(2)}_{[1,2]}(X)^\dagger = Z \otimes Z. \tag{75}$$

3.5 The Stabilizer Circuits, and Gottesman-Knill Theorem

Let n be a positive integer.

Definition 3.6: Any quantum circuit with the following properties is referred to as a "stabilizer circuit", or more specifically a "n-qubit quantum circuit".

SC1. The initial quantum state of the circuit is $|0\rangle^{\otimes n}$.

SC2. The set of quantum gates of the circuit is restricted to the n-Clifford group $\mathcal{C}_n$.

SC3. The set of quantum measurements of the circuit is restricted to the Hermitian elements of the n-Pauli group $\mathcal{P}_n$, that is the set $\{g \in \mathcal{P}_n \mid g^2 = I_n\}$.

■

Remark 3.1: Relaxing the initial quantum state, as mentioned in the first condition of [definition 3.6], to be set to any computational-basis element, or more generally any stabilizer state, alters the collection of three conditions equivalent to what is stated in [definition 3.6]. This is because any stabilizer state can be acheived by the action of a Clifford operator on $|0\rangle^{\otimes n}$.

The set of all stabilizer circuits form a class of quantum computational tasks that have no superiority over the classical computation. More precisely, it means that a stabilizer circuit can be efficiently simulated by a classical computer. The efficiency of such a classical simulation is assessed from the computational complexity point of view in terms of the number of qubits harnessed by the quantum circuit. This fact is famously known as the "Gottesman-Knill theorem". The following is the rigorous statement and proof of the Gottesman-Knill theorem.

Theorem 3.3: Any n-qubit stabilizer circuit can be simulated by a classical algorithm with $\mathbf{Poly}\,(n)$ number of classical operations.

proof : Clearly, a stabilizer circuit keeps the evolved quantum states at every level of the circuit inside the class of stabilizer states. The set of gates of the circuit can be assumed to be restricted to the famous generators of n-Clifford group, thagt is the one-qubit Hadamard and phase, and two-qubit CNOT gates. Suppose that there are n_G of such gates.

At each level of the circuit involving the action of a Clifford gate U (among Hadamard, phase, or CNOT gates) the current stabilizer state $|\psi\rangle$ identified by a set of n independent operators $\{g_1, \cdots, g_n\}$ of $\mathcal{P}_n$ will be transformed to the stabilizer state identified by $\left\{Ug_1U^\dagger, \cdots, Ug_nU^\dagger\right\}$. So to keep track of the state after the operation of U, one needs n number of look-ups for each g_i to infer its single-qubit factors in the total tensor-product, and then acting U on each g_i according to the rules stated in the previous section, which requires at most $2n$ number of additions modulo 2 to evolve $\mathbf{r}^{(n)}\,(g_i) \in \mathbb{F}_2^{2n}$ to $\mathbf{r}^{(n)}\left(Ug_iU^\dagger\right) \in \mathbb{F}_2^{2n}$. So, evaluating the evolution of all g_i-s under the action of U, and hence keeping track of the state requires at most

$n(n+2n) = 3n^2$ classical bitwise operations.

The set of measurements of the circuit are restricted to the Pauli observables, and we denote by n_M the number of measurements used in the circuit. At each level of the circuit involving the action of a Pauli observable O, the following are required to be done. O must be checked for its commutation relation with each g_i which can be done by using the binary representations of the Pauli operators. This requires $(2n)(2n) + 2n = 4n^2 + 2n$ classical bitwise operations to evaluate $\left[\mathbf{r}^{(n)}(O)\right] \Lambda_{2n} \left[\mathbf{r}^{(n)}(g_i)\right]$ for each g_i, and hence $n(4n^2+n) = 4n^3 + n^2$ classical operations in total. Then if O commutes with all the g_i-s the state will not be altered, but if it anti-commutes with some of them, the anti-commuting g_i-s are needed to be changed as discussed previously to give rise to a new independent set of Pauli operators that identify the state, with just the first element anti-commuting with O. This requires updating at most $n-1$ number of g_i-s by multiplying them with a fixed g_k which is equivalent to performing at most $n-1$ addition operations in $\mathbb{F}_2^n$ according to the discussions of the previous sections and considering the Boolean representations of Pauli operators, and hence requires $(n-1)2n = 2n^2 - n$ classical bitwise operations. Finally according to the observed outcome, the first element of the new set of n Pauli operators that identify the state must be changed to the observable under consideration which requires at most $2n$ classical bitwise operations. Therefore totally at most $(4n^3 + n^2) + (2n^2 - 2n) + 2n = 4n^3 + 3n^2$ classical bitwise operations are needed.

Therefore, totally $n_G(3n^2) + n_M(4n^3 + 3n^2)$ classical bitwise operations are required to simulate the operation of the circuit classically. So it is seen that, overall, the stabilizer circuit can be simulated by $\mathcal{O}(n^3)$ classical bitwise operations. Hence a stabilizer circuit in n qubits can be simulated classically with the classical computational complexity in the class $\mathbf{Poly}(n)$.

□

Chapter 4

UNIVERSAL QUANTUM COMPUTING

4.1 Finite Universal Quantum Gate Sets

Let n be any positive integer. One of the important problems in the theory of quantum computing is the possibility of implementing any unitary gate in $\mathrm{U}(\mathcal{H}^{\otimes n})$ using a finite sequence of the elements of a finite subset of $\mathrm{U}(\mathcal{H}^{\otimes n})$. Note that in quantum mechanics two unitary operators are considered to be equivalent if they differ by just a phase factor. Therefore the group of importance is actually the quotient group $\mathrm{U}(\mathcal{H}^{\otimes n})/\mathcal{Z}(\mathcal{H}^{\otimes n})$. This precisely means that the implementation of a unitary gate U is equivalent to the implementation of any operator in $[U]$, where $[U]$ denotes the coset in $\mathrm{U}(\mathcal{H}^{\otimes n})/\mathcal{Z}(\mathcal{H}^{\otimes n})$ containing U, and it is better to speak of implementing a $[U] \in \mathrm{U}(\mathcal{H}^{\otimes n})/\mathcal{Z}(\mathcal{H}^{\otimes n})$. Furthermore, note that since $\mathrm{U}(\mathcal{H}^{\otimes n})/\mathcal{Z}(\mathcal{H}^{\otimes n})$ is an uncountable group, it cannot be the case that every element of $\mathrm{U}(\mathcal{H}^{\otimes n})$ equals the composition of a finite sequence of elements of a finite subset of $\mathrm{U}(\mathcal{H}^{\otimes n})$.

The implementation of a unitary gate $U \in \mathrm{U}(\mathcal{H}^{\otimes n})$ is determined not only by U itself, but also by the accuracy ε of approximating U. The validity of the following theorem is well-known in quantum computing theory. Prior to the statement of the theorem, we state a definition.

Definition 4.1: Let S be a subset of $\mathrm{U}(\mathcal{H}^{\otimes n})$. S is called a "universal gate set for $\mathcal{H}^{\otimes n}$" if for every $\mathcal{U} \in \mathrm{U}(\mathcal{H}^{\otimes n})/\mathcal{Z}(\mathcal{H}^{\otimes n})$ and any positive real number ε, there exists a sequence $(V_1, \cdots, V_n)$ of elements of S and there exists $U \in \mathcal{U}$ such that,

$$\|U - V_n \cdots V_1\|\mathrm{op} \leq \varepsilon, \tag{1}$$

where $\|\centerdot\|\text{op}$ denotes the operator norm of the vector space $\mathcal{L}\left(\mathcal{H}^{\otimes n}\right)$, defined as,

$$\forall\, A \in \mathcal{L}\left(\mathcal{H}^{\otimes n}\right):\ \|A\|\text{op} \stackrel{\text{def}}{=} \sup\left\{\frac{\|A\left(v\right)\|}{\|v\|} \mid v \neq 0\right\}, \tag{2}$$

where $\|\centerdot\|$ denotes the standard norm of the $\mathcal{H}^{\otimes n}$.

■

For every $\theta \in \left\{\Theta \in [0, 2\pi) \mid \nexists q \in \mathbb{Z}\ \ \theta = q\frac{\pi}{2}\right\}$ define the unitary operation $\Gamma\left(\theta\right) \in \mathcal{U}_1$ as,

$$\Gamma\left(\theta\right) := |0\rangle\langle 0| + \exp\left(i\theta\right)|1\rangle\langle 1|\,. \tag{3}$$

Theorem 4.1: There exists finite universal gate sets for $\mathcal{H}^{\otimes n}$, with several instances as the following [3][6].

n=1: The collection of the Hadamard, Phase, and the $\frac{\pi}{4}$-phase-shift $\Gamma\left(\frac{\pi}{4}\right)$ gates, that is the set $\left\{H, P, \Gamma\left(\frac{\pi}{4}\right)\right\}$.

n>1: The collection of all one-qubit Hadamard, Phase, and $\frac{\pi}{4}$-phase-shift gates, together with the collection of all two-qubit CNOT gates. That is the set
$\left\{H_k^{(n)} \mid k \in \{1, \cdots, n\}\right\} \cup \left\{S_k^{(n)} \mid k \in \{1, \cdots, n\}\right\} \cup$
$\left\{\left[\Gamma\left(\frac{\pi}{4}\right)\right]_k^{(n)} \mid k \in \{1, \cdots, n\}\right\} \cup \left\{C_{[j,k]}^{(n)}\left(X\right) \mid j, k \in \{1, \cdots, n\}\right\}$.

n>1: The collection of all one-qubit Hadamard, Phase, and $\frac{\pi}{6}$-phase-shift gates, together with the collection of all two-qubit CNOT gates. That is the set
$\left\{H_k^{(n)} \mid k \in \{1, \cdots, n\}\right\} \cup \left\{S_k^{(n)} \mid k \in \{1, \cdots, n\}\right\} \cup$
$\left\{\left[\Gamma\left(\frac{\pi}{6}\right)\right]_k^{(n)} \mid k \in \{1, \cdots, n\}\right\} \cup \left\{C_{[j,k]}^{(n)}\left(X\right) \mid j, k \in \{1, \cdots, n\}\right\}$.

Since the set of all one-qubit Hadamard and phase gates together with the set of all two-qubit CNOT gates generate the n-Clifford group, it is seen that $\mathcal{C}_n$ together with one-qubit $\Gamma\left(\frac{\pi}{4}\right)$ gates, or $\mathcal{C}_n$ together with one-qubit $\Gamma\left(\frac{\pi}{6}\right)$ gates forms a universal quantum gate set. This means that combining the Clifford group $\mathcal{C}_n$ with just one-qubit $\frac{\pi}{4}$-phase-shift (or $\frac{\pi}{6}$-phase-shift) gates, constitutes universal quantum computation

□

4.2 Implementing Non-Clifford Gates using Magic States

In this section we will consider the implementation of a particular class of single-qubit non-Clifford gates, with the assumption that only the gates from the Clifford group and the measurements from the Pauli group can be implemented directly and efficiently relying on the methods of fault-tolerant quantum computation. So all the elements of a circuit containing the action of a non-Clifford gate will be the same as those of a stabilizer circuit, except for the initial state whose dimension is augmented to make use of ancillary qubits initialized to some non-stabilizer state. The preparation of such non-stabilizer states is definitely a matter of concern, since only the preparation of stabilizer states are assumed on the basis of fault-tolerant quantum computation. In this section we assume the possibility of ideal preparation of such states, and we will discuss later their preparation with any desired precision by performing a series of Clifford gates and Pauli measurements on an initially given (unknown) quantum state.

Let $\theta \in \left\{\Theta \in [0, 2\pi) \mid \nexists q \in \mathbb{Z} \;\; \theta = q\frac{\pi}{2}\right\}$. Clearly,

$$\begin{aligned}\Gamma(\theta) X \Gamma(\theta)^{\dagger} &= [|0\rangle\langle 0| + \exp(i\theta)|1\rangle\langle 1|][|0\rangle\langle 1| + |1\rangle\langle 0|][|0\rangle\langle 0| + \exp(-i\theta)|1\rangle\langle 1|] \\ &= \exp\{-i\theta\}|0\rangle\langle 1| + \exp\{i\theta\}|1\rangle\langle 0|,\end{aligned} \tag{4}$$

and hence considering that θ is not an integer multiple of $\frac{\pi}{2}$, it is easily seen that $\Gamma(\theta) X \Gamma(\theta)^{\dagger}$ is not an element of the 1-Pauli group $\mathcal{P}_1$. Therefore, according to the definition of the Pauli group, $\Gamma(\theta)$ is not element of the 1-Clifford group $\mathcal{C}_1$.

Considering that all gates from the Clifford group can be implemented fault-tolerantly [12] with any desired precision, but not gates out of the Clifford group in general, investigating indirect ways of implementing non-Clifford gates is of remarkable importance. One method of simulating the non-Clifford gates of the class $\left\{\Gamma(\theta) \mid \theta \in [0, 2\pi), \nexists q \in \mathbb{Z} \;\; \theta = q\frac{\pi}{2}\right\}$ is harnessing an ancillary qubit state $|\Gamma_\theta\rangle$, setting the initial state to $|\psi\rangle \otimes |\Gamma_\theta\rangle$ for any state $|\psi\rangle$ to be acted upon the gate $\Gamma(\theta)$, and then choosing a sequence of Clifford gates and Pauli measurements properly to

be performed on it. Define,

$$|\Gamma_\theta\rangle := \frac{1}{\sqrt{2}}\left(|0\rangle + \exp\left(i\theta\right)|1\rangle\right). \tag{5}$$

Let $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ in $\mathcal{H}$. We now describe a procedure that receives the state $|\psi\rangle$ as the input and transforms it randomly to one of the states $\Gamma\left(\theta\right)|\psi\rangle$ or $\Gamma\left(-\theta\right)|\psi\rangle$ as the output with the uniform probability.

Define $|\Psi^0\rangle := |\psi\rangle \otimes |\Gamma_\theta\rangle \in \mathcal{H}^{\otimes 2}$. By preparing the two-qubit quantum state $|\Psi^0\rangle$ and performing the Pauli measurement $Z \otimes Z$ on it, denoting by $\left|\Psi^0_+\right\rangle$ and $\left|\Psi^0_-\right\rangle$ the modified states after observing the outcomes $+1$ and -1 respectively, and considering that $Z \otimes Z = (|00\rangle\langle 00| + |11\rangle\langle 11|) - (|01\rangle\langle 01| + |10\rangle\langle 10|)$, we have,

$$\begin{aligned}
\Pr\left[Z \otimes Z, +1; \left|\Psi^0\right\rangle\right] &= \left\langle\Psi^0\right|(|00\rangle\langle 00| + |11\rangle\langle 11|)\left|\Psi^0\right\rangle \\
&= |\langle\psi|0\rangle|^2|\langle\Gamma_\theta|0\rangle|^2 + |\langle\psi|1\rangle|^2|\langle\Gamma_\theta|1\rangle|^2 \\
&= \frac{1}{2}|a|^2 + \frac{1}{2}|b|^2 = \frac{1}{2}\left(|a|^2 + |b|^2\right) = \frac{1}{2},
\end{aligned} \tag{6}$$

and hence,

$$\Pr\left[Z \otimes Z, +1; \left|\Psi^0\right\rangle\right] = \frac{1}{2}, \tag{7}$$

where $\Pr\left[Z \otimes Z, +1; |\Psi^0\rangle\right]$ and $\Pr\left[Z \otimes Z, -1; |\Psi^0\rangle\right]$ denote the probabilities of observing outcomes $+1$ and -1 respectively, upon measuring $|\Psi^0\rangle$ by $Z \otimes Z$, and

$$\begin{aligned}
\left|\Psi^0_+\right\rangle &= \frac{1}{\sqrt{\Pr\left[Z \otimes Z, +1; |\Psi^0\rangle\right]}}\left(|00\rangle\langle 00| + |11\rangle\langle 11|\right)|\psi\rangle \otimes |\Gamma_\theta\rangle \\
&= a\,|00\rangle + b\exp\left(i\theta\right)|11\rangle,
\end{aligned} \tag{8}$$

and

$$\begin{aligned}
\left|\Psi^0_-\right\rangle &= \frac{1}{\sqrt{\Pr\left[Z \otimes Z, -1; |\Psi^0\rangle\right]}}\left(|01\rangle\langle 01| + |10\rangle\langle 10|\right)|\psi\rangle \otimes |\Gamma_\theta\rangle \\
&= a\exp\left(i\theta\right)|01\rangle + b\,|10\rangle.
\end{aligned} \tag{9}$$

Now performing the CNOT gate on the modified state after measuring $|\Psi^0\rangle$ by $Z \otimes Z$ will yield one of the states $\left|\Psi^1_+\right\rangle$ and $\left|\Psi^2_-\right\rangle$, each with probability $\frac{1}{2}$, where,

$$\begin{aligned}
\left|\Psi^1_+\right\rangle :&= C^{(2)}_{[1,2]}\left(X\right)\left|\Psi^0_+\right\rangle = a\,|00\rangle + b\exp\left(i\theta\right)|10\rangle \\
&= \left[a\,|0\rangle + b\exp\left(i\theta\right)|1\rangle\right] \otimes |0\rangle,
\end{aligned} \tag{10}$$

and

$$\begin{aligned}\left|\Psi_{-}^{1}\right\rangle :&= C_{[1,2]}^{(2)}(X)\left|\Psi_{-}^{0}\right\rangle = a\exp(i\theta)|01\rangle + b|11\rangle \\ &= [a\exp(i\theta)|0\rangle + b|1\rangle]\otimes|1\rangle .\end{aligned} \tag{11}$$

So, discarding the second qubit, this procedure yields one of the states ψ_{+}^{1} or ψ_{-}^{1} each with probability -1, where,

$$\begin{aligned}\left|\psi_{+}^{1}\right\rangle &:= a|0\rangle + b\exp(i\theta)|1\rangle = \Gamma(\theta)|\psi\rangle \\ \left|\psi_{-}^{1}\right\rangle &:= a|0\rangle + b\exp(-i\theta)|1\rangle = \Gamma(-\theta)|\psi\rangle .\end{aligned} \tag{12}$$

Let us consider the most general case where the input of this procedure is a mixed state represented by a density operator $\rho \in \mathrm{Dens}(\mathcal{H}^{\otimes n})$. Let us then denote output state of this procedure when receiving any mixed state $\rho \in \mathrm{Dens}(\mathcal{H}^{\otimes n})$ as the input by $\mathbf{o}(\rho)$ which is clearly a mixed state in $\mathrm{Dens}(\mathcal{H}^{\otimes n})$. In the particular case of a pure state $|\psi\rangle\langle\psi|$ as the input, based on the discussion above, it is clear that

$$\mathbf{o}(|\psi\rangle\langle\psi|) = \frac{1}{2}\Gamma(\theta)|\psi\rangle\langle\psi|\Gamma(\theta)^{\dagger} + \frac{1}{2}\Gamma(-\theta)|\psi\rangle\langle\psi|\Gamma(-\theta)^{\dagger}. \tag{13}$$

So, successively performing this procedure for some N number of times, upon receiving a pure state $|\psi\rangle\langle\psi|$, yields the output as the mixed state $\mathbf{o}^{N}(|\psi\rangle\langle\psi|)$. It is not difficult to observe that $\mathbf{o}^{N}(|\psi\rangle\langle\psi|)$ is the density matrix representation of the mixture of the states of the set

$$\{\Gamma(p\theta)|\psi\rangle \mid p \in \Delta_N\},$$

with the uniform probability, where,

$$\Delta_N := \left\{\sum_{k=1}^{N} x_k \mid x \in \{-1,+1\}^N\right\}. \tag{14}$$

Therefore,

$$\mathbf{o}^{N}(|\psi\rangle\langle\psi|) = \frac{1}{2^N}\sum_{p\in\Delta_N}\Gamma(p\theta)|\psi\rangle\langle\psi|\Gamma(p\theta)^{\dagger}, \tag{15}$$

and one of the states $\Gamma(p\theta)|\psi\rangle$ will be obtained eventually, picked randomly among all possible states as described above. This is an stochastic problem equivalent to the

random walk on the set of integers. So since the random walk on the set of integers meets each integer p with certainty, that is every integer p is met after a large enough number N of walks, the procedure described above will yield the quantum state $\Gamma(\theta)|\psi\rangle$ with certainty, after being operated successively for a number of times.

4.2.1 Obtaining $\left|\Gamma_{\frac{-\pi}{6}}\right\rangle$ *from* $|T_0\rangle$

By definition, $T := SH$, where S and H are the phase and Hadamard gates, respectively. So,

$$\begin{aligned} T &:= SH \\ &= \left[\exp\left(-\frac{i\pi}{4}\right)|0\rangle\langle 0| + \exp\left(\frac{i\pi}{4}\right)|1\rangle\langle 1|\right]\left[\frac{1}{\sqrt{2}}\left(|0\rangle\langle 0| - |1\rangle\langle 1| + |0\rangle\langle 1| + |1\rangle\langle 0|\right)\right] \\ &= \frac{\exp\left(\frac{i\pi}{4}\right)}{\sqrt{2}}\left(|0\rangle\langle 0| - i|1\rangle\langle 1| + |0\rangle\langle 1| + i|1\rangle\langle 0|\right) \end{aligned} \tag{16}$$

Clearly, T is a Clifford gate, that is an element of $\mathcal{C}_1$. It is also easy to check that the set of all eigenvalues of T is $\left\{\exp\left(\frac{i\pi}{3}\right), \exp\left(\frac{-i\pi}{3}\right)\right\}$. Denoting by $|T_0\rangle\langle T_0|$ and $|T_1\rangle\langle T_1|$ the eigenspaces of T corresponded to the eigenvalues $\exp\left(\frac{i\pi}{3}\right)$ and $\exp\left(\frac{-i\pi}{3}\right)$ respectively, we have,

$$T = \exp\left(\frac{i\pi}{3}\right)|T_0\rangle\langle T_0| + \exp\left(\frac{-i\pi}{3}\right)|T_1\rangle\langle T_1|. \tag{17}$$

Moreover, it is straightforward to observe that the action of T on $\mathcal{P}_1$ by conjugation is determined by,

$$\begin{aligned} TXT^\dagger &= Z, \\ TZT^\dagger &= Y, \\ TYT^\dagger &= X. \end{aligned} \tag{18}$$

before proceeding, we state a definition and two lemmas which will be used in the upcoming calculations.

Definition 4.2: For any positive integer n, the group action $\chi^{(n)} : \mathcal{C}_n \to \mathsf{Aut}(\mathcal{P}_n)$ as defined before, has the property that $\chi^{(n)}(U) = \chi^{(n)}\left(e^{i\phi}U\right)$ for every $U \in \mathcal{C}_n$ and every $\phi \in \mathbb{R}$. Therefore, the map $\tilde{\chi}^{(n)} : \mathcal{C}_1/\mathcal{Z}(\mathcal{U}_1) \to \mathsf{Aut}(\mathcal{P}_n)$ sending any representative U of any element of $\mathcal{C}_1/\mathcal{Z}(\mathcal{U}_1)$ to $\chi^{(n)}(U)$ is well-defined, and obviously a group action.

■

Proposition 4.1: Let n be a positive integer. The group action $\chi^{(n)} : \mathcal{C}_n/\mathcal{Z}(\mathcal{U}_n) \to \mathsf{Aut}(\mathcal{P}_n)$ is a faithful action. That is $[I]$ is the only element of $\mathcal{C}_n/\mathcal{Z}(\mathcal{U}_n)$ that is sent to $\mathcal{I}$, where $[I]$ denotes the coset in $\mathcal{C}_n/\mathcal{Z}(\mathcal{U}_n)$ containing I and $\mathcal{I}$ denotes the identity element of $\mathsf{Aut}(\mathcal{P}_n)$.

proof: Let $U \in \mathcal{C}_n$ such that $\tilde{\chi}([U]) = \mathcal{I}$. Then for every $g \in \mathcal{P}_n$, $[\chi(U)](g) = UgU^\dagger = g$, and hence $\chi(U) = \mathcal{I}$. Extending $\chi(U)$ to the function $f : \mathcal{L}(\mathcal{H}^{\otimes n}) \to \mathcal{L}(\mathcal{H}^{\otimes n})$ defined by $T \mapsto UTU^\dagger$ is seen to be a linear map, because

$$\begin{aligned} \forall\, c \in \mathbb{C}\colon\ \forall\, T_1, T_2 \in \mathcal{L}\left(\mathcal{H}^{\otimes n}\right)\colon\ f(cT_1 + T_2) &= U(cT_1 + T_2)U^\dagger \\ &= c\left(UT_1U^\dagger\right) + UT_2U^\dagger \\ &= cf(T_1) + f(T_2). \end{aligned} \tag{19}$$

Therefore, considering that $\mathcal{P}_n$ spans $\mathcal{L}(\mathcal{H}^{\otimes n})$, f is uniquely determined by the restriction of f to $\mathcal{P}_n$, that is by $\chi(U)$. Therefore f is the identity map from $\mathcal{L}(\mathcal{H}^{\otimes n})$ to itself, and hence,

$$\forall\, T \in \mathcal{L}\left(\mathcal{H}^{\otimes n}\right)\colon\ UTU^\dagger = T, \tag{20}$$

and thus,

$$\forall\, T \in \mathcal{L}\left(\mathcal{H}^{\otimes n}\right)\colon\ UT = TU. \tag{21}$$

Therefore U commutes with all elements of $\mathcal{L}(\mathcal{H}^{\otimes n})$ and hence with all elements of $\mathcal{U}_n$, which means U is in the center of $\mathcal{U}_n$ which is the set of all scalar operators of the form $\left\{e^{i\phi}I_n \mid \phi \in \mathbb{R}\right\}$. Therefore, $[U] = [I]$.

□

Lemma 4.1: Let n be a positive integer, and let $U \in \mathcal{U}_n$ such that $UgU^\dagger = g$ for all $g \in \mathcal{P}_n$. Then U must be in the center of $\mathcal{U}_n$ and hence a scalar operator of the type $e^{i\phi}I_n$ for some $\phi \in \mathbb{R}$.

proof: It can be shown in completely a similar way as [proposition 4.1] is proved.

□

Lemma 4.2: Let n be a positive integer.
Let $\mathcal{G}_n := \{O_1 \otimes \cdots \otimes O_n \mid [\forall\, k \in \{1, \cdots, n\} \colon\ O_k \in \{I, X, Y, Z\}]\}$. Let $T_1, T_2 \in \mathcal{U}_n$ such that,

$$\forall\, g \in \mathcal{G}_n \colon\ T_1 g {T_1}^\dagger = T_2 g {T_2}^\dagger. \tag{22}$$

Then T_1 and T_2 are the same upto a phase factor, that is $T_1 = e^{i\phi} T_2$ for some $\phi \in \mathbb{R}$. So, knowing the action of a unitary operator on the elements of $\mathcal{G}_n$ uniquely determines it.

proof : Since $\mathcal{G}_n$ generates $\mathcal{P}_n$, we have,

$$\forall\, g \in \mathcal{P}_n \colon\ T_1 g {T_1}^\dagger = T_2 g {T_2}^\dagger, \tag{23}$$

and hence,

$$\forall\, g \in \mathcal{P}_n \colon\ {T_2}^\dagger T_1 g {T_1}^\dagger T_2 = g, \tag{24}$$

and thus,

$$\left({T_2}^\dagger T_1 g\right) g \left({T_2}^\dagger T_1 g\right)^\dagger = g. \tag{25}$$

Therefore according to [lemma 4.1], ${T_2}^\dagger T_1 = e^{i\phi} I_n$ for some $\phi \in \mathbb{R}$, and hence $T_1 = e^{i\phi} T_2$.

□

It can be calculated that the unitary operator

$$\frac{e^{\frac{i\pi}{3}}}{2}\left[I_1 + \frac{1}{\sqrt{3}}(X + Y + Z)\right] + \frac{e^{\frac{-i\pi}{3}}}{2}\left[I_1 - \frac{1}{\sqrt{3}}(X + Y + Z)\right]$$

satisfies the same conjugation relations with the Pauli operators as those satisfied by T. Therefore, according to [lemma 4.2],

$$\begin{aligned} |T_0\rangle\langle T_0| &= \frac{1}{2}\left[I_1 + \frac{1}{\sqrt{3}}(X + Y + Z)\right], \\ |T_1\rangle\langle T_1| &= \frac{1}{2}\left[I_1 - \frac{1}{\sqrt{3}}(X + Y + Z)\right]. \end{aligned} \tag{26}$$

Then it can be easily calculated that, upto a phase factor,

$$|T_0\rangle = \cos(\beta)|0\rangle + \exp\left(\frac{i\pi}{4}\right)\sin(\beta)|1\rangle, \tag{27}$$

where $\cos(2\beta) = \frac{1}{\sqrt{3}}$.

We now describe a procedure to obtain a copy of the quantum state $\left|\Gamma_{-\frac{\pi}{6}}\right\rangle$ given a supply of the state $|\mathrm{T}_0\rangle$, by using just gates from the Clifford group and measurements from the Pauli group. Initially prepare an ensemble of the state $|\Phi_0\rangle := |T_0\rangle \otimes |T_0\rangle$. Then perform the Pauli measurement $Z \otimes Z$ on $|\Phi_0\rangle$ on copies of the state $|\Phi_0\rangle$ until observing the outcome $+1$ which occurs with probability

$$\Pr[Z \otimes Z, +1; |\Phi_0\rangle] = \langle\Phi_0|Z \otimes Z|\Phi_0\rangle = \frac{2}{3}. \tag{28}$$

After observing the outcome $+1$, the state is reduced to

$$\begin{aligned}|\Phi_1\rangle &= \frac{1}{\sqrt{\Pr[Z \otimes Z, +1; |\Phi_0\rangle]}}\left(|00\rangle\langle 00| + |11\rangle\langle 11|\right)|T_0\rangle \otimes |T_0\rangle \\ &= \frac{\sqrt{3}}{2}\cos^2(\beta)|00\rangle + i\frac{\sqrt{3}}{2}\sin^2(\beta)|11\rangle \\ &= \cos\left(\frac{\pi}{12}\right)|00\rangle + i\sin\left(\frac{\pi}{12}\right)|11\rangle.\end{aligned} \tag{29}$$

Now apply the CNOT gate $C^{(2)}_{[1,2]}(X)$ on $|\Phi_1\rangle$ to obtain the state,

$$|\Phi_2\rangle := C^{(2)}_{[1,2]}(X)|\Phi_1\rangle = \left[\cos\left(\frac{\pi}{12}\right)|0\rangle + i\sin\left(\frac{\pi}{12}\right)|1\rangle\right] \otimes |0\rangle, \tag{30}$$

and hence to obtain the single-qubit state

$$|\phi_2\rangle := \cos\left(\frac{\pi}{12}\right)|0\rangle + i\sin\left(\frac{\pi}{12}\right)|1\rangle. \tag{31}$$

Finally, apply the Hadamard gate H on the state $|\phi_2\rangle$ to get

$$H|\phi_2\rangle = \left|\Gamma_{-\frac{\pi}{6}}\right\rangle. \tag{32}$$

4.3 Distillation of the Magic State $|T_0\rangle$

The preparation of stabilizer states, Clifford gates, and Pauli measurements with a desired precision is well-established in the quantum computing literature, based on the achievements of the theory of fault-tolerant quantum computation. So, their

ideal preparation (in the sense of being able to be prepared with arbitrary precision) can be assumed as an standard fact of the quantum computing theory. According to the discussions of the previous sections, there are specific non-stabilizer single-qubit quantum states that can play a prominent role in universal quantum computing if they can be prepared with any desired precision. Our focus in this section will be on dealing with the preparation of the state $|T_0\rangle$, particularly. Since the basic assumption is having access to just stabilizer states, Clifford gates, and Pauli measurements ideally, the goal is to purify a supply of an initially given noisy state (noisy in the sense that it differs from $|\mathrm{T}_0\rangle$ with an acceptable distance quantitatively) represented by a density matrix $\rho \in \mathrm{Dens}\left(\mathcal{H}^{\otimes n}\right)$ towards a single copy of $|T_0\rangle$. The closeness measure between two quantum states considered here is the fidelity measure. For any positive integer n, we will denote the fidelity of two quantum states $\rho_1, \rho_2 \in \mathrm{Dens}\left(\mathcal{H}^{\otimes n}\right)$ by $\mathcal{F}_n\left(\rho_1, \rho_2\right)$ defined as,

$$\mathcal{F}_n\left(\rho_1, \rho_2\right) := \mathrm{Tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}. \tag{33}$$

The range of the fidelity measure is $[0, 1]$. It can be easily seen that for any state $\rho \in \mathrm{Dens}\left(\mathcal{H}^{\otimes n}\right)$ and a pure state $|\psi\rangle \in \mathcal{H}^{\otimes n}$, the fidelity between them can be expressed as,

$$\mathcal{F}_n\left(\rho, |\psi\rangle\langle\psi|\right) = \sqrt{\langle\psi|\rho|\psi\rangle}. \tag{34}$$

The closer the fidelity between two quantum states to 1, the closer their measurement statistics to each other with respect to any quantum measurement, and accordingly the more similar the states to each other. So for any two states $\rho, \sigma \in \mathrm{Dens}\left(\mathcal{H}^{\otimes n}\right)$, the quantity $1 - \mathcal{F}_n\left(\rho, \sigma\right)$ can also be regarded as a measure of distance between them, and the closer this quantity to 0, the more similar the states to each other.

Now assume that $N = 5^{N_0}$ copies of a state $\rho \in \mathrm{Dens}\left(\mathcal{H}\right)$ are provided initially, for a large enough N_0. Define,

$$\varepsilon_0 := 1 - \mathcal{F}_n\left(\rho, |T_0\rangle\langle T_0|\right) = 1 - \langle T_0|\rho|T_0\rangle\,. \tag{35}$$

We now describe a subroutine that receives as input the state $\rho^{\otimes N}$ and outputs a state $\left[\xi\left(\rho\right)\right]^{\otimes \frac{N}{5}}$ with the distance ε_1 from $|T_0\rangle$, that is

$$\varepsilon_1 := 1 - \mathcal{F}_n\left(\xi\left(\rho\right), |T_0\rangle\langle T_0|\right) = 1 - \langle T_0|\xi\left(\rho\right)|T_0\rangle\,. \tag{36}$$

We will call this subroutine the "magic state $|T_0\rangle$ distillation subroutine".

The Magic State $|T_0\rangle$ Distillation Subroutine:

Consider the elements of the Pauli group $\mathcal{P}_5$ defined as,

$$\begin{aligned} g_1 &:= X \otimes Z \otimes Z \otimes X \otimes I, \\ g_2 &:= I \otimes X \otimes Z \otimes Z \otimes X, \\ g_3 &:= X \otimes I \otimes X \otimes Z \otimes Z, \\ g_4 &:= Z \otimes X \otimes I \otimes X \otimes Z. \end{aligned} \tag{37}$$

The elements of $\{g_1, g_2, g_3, g_4\}$ can be easily seen to pairwise commute, and more specifically $-I_5 \notin \langle g_1, g_2, g_3, g_4\rangle =: S$. Hence, according to [lemma 3.3]

$$P^{(S)} = \frac{1}{16}\prod_{k=1}^{4}\left(I_5 + g_k\right), \tag{38}$$

where $P^{(S)}$ denotes the orthogonal projection onto the vector subspace of $\mathcal{H}^{\otimes 5}$ stabilized by S, that is $\mathcal{V}_S$. Moreover, considering that $\{g_1, g_2, g_3, g_4\}$ is an independent set of Pauli operators (which can be verified by using the check-matrix method), according to [theorem 3.1], $\dim\left(\mathcal{V}_S\right) = 2^{5-4} = 2$.

Partition the ensemble of N copies of ρ to the identical groups each consisting of 5 copies of ρ. Apply the quantum operation $\mathcal{E}$ to each ρ, defined by,

$$\forall\, \sigma \in \mathrm{Dens}\left(\mathcal{H}^{\otimes n}\right):\ \mathcal{E}\left(\sigma\right) \stackrel{\mathrm{def}}{=} \frac{1}{3}\left(\sigma + T\sigma T^{\dagger} + T^{\dagger}\sigma T\right), \tag{39}$$

to obtain the 5-qubit state $\tilde{\rho}$,

$$\tilde{\rho} := \left[\mathcal{E}\left(\rho\right)\right]^{\otimes 5}. \tag{40}$$

It can be easily calculated that,

$$\mathcal{E}\left(\rho\right) = \left(1-\varepsilon_0\right)|T_0\rangle\langle T_0| + \varepsilon_0\,|T_1\rangle\langle T_1|. \tag{41}$$

Therefore,

$$\begin{aligned} \tilde{\rho} &= \left[\left(1-\varepsilon_0\right)|T_0\rangle\langle T_0| + \varepsilon_0\,|T_1\rangle\langle T_1|\right]^{\otimes 5} \\ &= \sum_{x\in\mathbb{F}_2^5} \varepsilon_0^{|x|}\left(1-\varepsilon_0\right)^{5-|x|}|T_x\rangle\langle T_x|, \end{aligned} \tag{42}$$

where for every binary string $x \in \mathbb{F}_2^5$, $|x| := |\{x_i \mid x_i = 1\}|$, and

$$|T_x\rangle := \bigotimes_{k=1}^{5} |T_{x_k}\rangle = |T_{x_1}\rangle \otimes \cdots \otimes |T_{x_5}\rangle . \tag{43}$$

So each group can be identified with the state $\tilde{\rho} \in \mathrm{Dens}\left(\mathcal{H}^{\otimes 5}\right)$. The following is the description of a process executed on each 5-qubit group $\tilde{\rho}$. Perform successively the tuple (g_1, g_2, g_3, g_3) of Pauli measurements (in the indicated order) on the state $\tilde{\rho}$. Then proceed as follows if the outcome of this tuple of measurements is $(1, 1, 1, 1)$, and halt the process otherwise.

Suppose that the outcome $(1, 1, 1, 1)$ is observed following the measurement of $\tilde{\rho}$ by (g_1, g_2, g_3, g_3). Then denoting by $\tilde{\rho}_1$ the reduced state following this sequence of measurements, according to the postulate of measurements, and considering that for each k, $\frac{1}{2}\left(I_5 + g_k\right)$ is the orthogonal projector onto the eigenspace of g_k corresponded with the eigenvalue 1, it is obvious that,

$$\tilde{\rho}_1 = \frac{1}{\mathrm{Tr}\left(\Pi\tilde{\rho}\Pi^\dagger\right)}\Pi\tilde{\rho}\Pi^\dagger = \frac{1}{\mathrm{Tr}\left(\Pi\tilde{\rho}\Pi\right)}\Pi\tilde{\rho}\Pi = \frac{1}{\mathrm{Tr}\left(\Pi\tilde{\rho}\right)}\Pi\tilde{\rho}\Pi. \tag{44}$$

On the other hand denoting by p the probability of observing the outcome $(1, 1, 1, 1)$, and defining P_k as the orthogonal projector onto the eigenspace of g_k corresponded to the eigenvalue 1, that is $P_k := \frac{1}{2}\left(I_5 + g_k\right)$ for every k, and considering the postulate of measurement, the commutativity of P_j and P_k for every j and k, and the fact that $P_k P_k = P_k$ for each k, we have,

$$\begin{aligned} p &= \mathrm{Tr}\left(P_1\rho\right)\mathrm{Tr}\left[P_2\left(P_1\rho P_1\right)\right]\mathrm{Tr}\left[P_3\left(P_2P_1\rho P_1P_2\right)\right]\mathrm{Tr}\left[P_4\left(P_3P_2P_1\rho P_1P_2P_3\right)\right] \\ &= \mathrm{Tr}\left(P_4P_3P_2P_1\rho\right)p\,\mathrm{Tr}\left(P_3P_2P_1\rho\right)\mathrm{Tr}\left(P_2P_1\rho\right)\mathrm{Tr}\left(P_1\rho\right). \end{aligned} \tag{45}$$

It can be proved that [12],

$$\begin{aligned} P^{(S)}X^{\otimes 5} &= X^{\otimes 5}P^{(S)}, \\ P^{(S)}Y^{\otimes 5} &= Y^{\otimes 5}P^{(S)}, \\ P^{(S)}Z^{\otimes 5} &= Z^{\otimes 5}P^{(S)}, \\ P^{(S)}T^{\otimes 5} &= T^{\otimes 5}P^{(S)}. \end{aligned} \tag{46}$$

So, since $X^{\otimes 5}$, $Y^{\otimes 5}$, $Z^{\otimes 5}$, and $T^{\otimes 5}$ commute with the orthogonal projection $P^{(S)}$, they all preserve the subspace $\mathcal{V}_S$. On the other hand, according to [equation 18],

$$\begin{aligned} T^{\otimes 5} X^{\otimes 5} \left[T^{\otimes 5}\right]^\dagger &= Z^{\otimes 5}, \\ T^{\otimes 5} Z^{\otimes 5} \left[T^{\otimes 5}\right]^\dagger &= Y^{\otimes 5}, \\ T^{\otimes 5} Y^{\otimes 5} \left[T^{\otimes 5}\right]^\dagger &= X^{\otimes 5}. \end{aligned} \tag{47}$$

Moreover, it is clear that $X^{\otimes 5}$, $Y^{\otimes 5}$, and $Z^{\otimes 5}$ obey the same commutation relations as those X, Y, and Z, correspondingly. Therefore, defining the unitary operators,

$$\begin{aligned} \hat{X} &:= P^{(S)} X^{\otimes 5} \left[P^{(S)}\right]^\dagger + \left(I_5 - P^{(S)}\right) = P^{(S)} X^{\otimes 5} + \left(I_5 - P^{(S)}\right), \\ \hat{Y} &:= P^{(S)} Y^{\otimes 5} \left[P^{(S)}\right]^\dagger + \left(I_5 - P^{(S)}\right) = P^{(S)} Y^{\otimes 5} + \left(I_5 - P^{(S)}\right), \\ \hat{Z} &:= P^{(S)} Z^{\otimes 5} \left[P^{(S)}\right]^\dagger + \left(I_5 - P^{(S)}\right) = P^{(S)} Z^{\otimes 5} + \left(I_5 - P^{(S)}\right), \\ \hat{T} &:= P^{(S)} T^{\otimes 5} \left[P^{(S)}\right]^\dagger + \left(I_5 - P^{(S)}\right) = P^{(S)} T^{\otimes 5} + \left(I_5 - P^{(S)}\right), \end{aligned} \tag{48}$$

we have,

$$\begin{aligned} \hat{T} \hat{X} \left[\hat{T}\right]^\dagger &= \hat{Z}, \\ \hat{T} \hat{Z} \left[\hat{T}\right]^\dagger &= \hat{Y}, \\ \hat{T} \hat{Y} \left[\hat{T}\right]^\dagger &= \hat{X}, \end{aligned} \tag{49}$$

and that $\hat{X}$, $\hat{Y}$, $\hat{Z}$ obey the same commutation relations as those of X, Y, and Z, correspondingly. It is also trivial to see that the restrictions of $\hat{X}$, $\hat{Y}$, $\hat{Z}$, and $\hat{T}$ to $\mathcal{V}_S$ coincide with the restrictions of $X^{\otimes 5}$, $Y^{\otimes 5}$, $Z^{\otimes 5}$, and $T^{\otimes 5}$ to $\mathcal{V}_S$ respectively, because they commute with $P^{(S)}$. Now define the states,

$$\left|T_0^L\right\rangle := \sqrt{6} P^{(S)} \left|T_1\right\rangle^{\otimes 5}, \tag{50}$$

$$\left|T_1^L\right\rangle := \sqrt{6} P^{(S)} \left|T_0\right\rangle^{\otimes 5}, \tag{51}$$

which can be shown to be actually normalized vectors [6]. Then, considering that $T^{\otimes 5} P^{(S)} = P^{(S)} T^{\otimes 5}$, and according to [equation 17] we have,

$$\begin{aligned} T^{\otimes 5} \left|T_1^L\right\rangle &= \sqrt{6} T^{\otimes 5} P^{(S)} \left|T_0\right\rangle^{\otimes 5} = \sqrt{6} P^{(S)} T^{\otimes 5} \left|T_0\right\rangle^{\otimes 5} \\ &= \sqrt{6} P^{(S)} \left(T \left|T_0\right\rangle\right)^{\otimes 5} = \sqrt{6} P^{(S)} \left(e^{\frac{i\pi}{3}} \left|T_0\right\rangle\right)^{\otimes 5} \\ &= \exp\left(\frac{5i\pi}{3}\right) \left[\sqrt{6} P^{(S)} \left|T_0\right\rangle^{\otimes 5}\right] = e^{-\frac{i\pi}{3}} \left|T_1^L\right\rangle. \end{aligned} \tag{52}$$

Similarly, it is seen that,

$$T^{\otimes 5}\left|T_0^L\right\rangle = e^{\frac{i\pi}{3}}\left|T_0^L\right\rangle. \tag{53}$$

Since $\left|T_0^L\right\rangle$ and $\left|T_1^L\right\rangle$ are eigenvectors of $T^{\otimes 5}$ corresponded to different eigenvalues, and considering that they belong to the two-dimensional subspace $\mathcal{V}_S$, we must have $\mathcal{V}_S = \mathsf{span}\left\{\left|T_0^L\right\rangle, \left|T_1^L\right\rangle\right\}$, and

$$\hat{T} = \left[\exp\left(\frac{i\pi}{3}\right)\left|T_0^L\right\rangle\!\left\langle T_0^L\right| + \exp\left(-\frac{i\pi}{3}\right)\left|T_1^L\right\rangle\!\left\langle T_1^L\right|\right] + \left(I_5 - P^{(S)}\right). \tag{54}$$

Note that in deriving the equation above, we used the fact that the eigenvectors corresponded to other eigenvalues of $\hat{T}$ are orthogonal to $\left|T_0^L\right\rangle$ and $\left|T_1^L\right\rangle$ and hence orthogonal to $\mathcal{V}_S$, and therefore their projection onto $\mathcal{V}_S$ is the zero vector.
Since the restrictions of $\hat{X}$, $\hat{Y}$, and $\hat{Z}$ to $\mathcal{V}_S$ obey the same commutation relations as those of X, Y, and Z, they must be mutually orthogonal and all with the same norms correspondingly, with respect to the Hilbert-Schmidt inner product of the vector-space $\mathcal{L}(\mathcal{V}_S)$. Therefore, considering that the restriction of $\hat{T}$ to $\mathcal{V}_S$ satisfies the conjugation relations with the restrictions of $\hat{X}$, $\hat{Y}$, and $\hat{Z}$ to $\mathcal{V}_S$, similar to [equation 18], based on [lemma 4.2] and according to [equation 26], we must have,

$$\begin{aligned}\left|T_0^L\right\rangle\!\left\langle T_0^L\right| &= \frac{1}{2}P^{(S)}\left[I_5 + \frac{1}{\sqrt{3}}\left(\hat{X}+\hat{Y}+\hat{Z}\right)\right] \\ &= \frac{1}{2}P^{(S)}\left[I_5 + \frac{1}{\sqrt{3}}\left(X^{\otimes 5}+Y^{\otimes 5}+Z^{\otimes 5}\right)\right],\end{aligned} \tag{55}$$

$$\begin{aligned}\left|T_1^L\right\rangle\!\left\langle T_1^L\right| &= \frac{1}{2}P^{(S)}\left[I_5 - \frac{1}{\sqrt{3}}\left(\hat{X}+\hat{Y}+\hat{Z}\right)\right] \\ &= \frac{1}{2}P^{(S)}\left[I_5 - \frac{1}{\sqrt{3}}\left(X^{\otimes 5}+Y^{\otimes 5}+Z^{\otimes 5}\right)\right].\end{aligned} \tag{56}$$

It also can be calculated that [6],

$$\tilde{\rho}_1 = \frac{\varepsilon_0^5 + 5\varepsilon_0^2\left(1-\varepsilon_0\right)^3}{6}\left|T_0^L\right\rangle\!\left\langle T_0^L\right| + \frac{\left(1-\varepsilon_0\right)^5 + 5\varepsilon_0^3\left(1-\varepsilon_0\right)^2}{6}\left|T_1^L\right\rangle\!\left\langle T_1^L\right|. \tag{57}$$

Since $\{S_1, S_2, S_3, S_4\}$ consists of pairwise-commuting elements, it is known that [6] there exists a Clifford operation $U \in \mathcal{C}_5$ such that,

$$US_kU^\dagger = Z_k^{(5)}, \quad k = 2,3,4,5, \tag{58}$$

where $Z_k^{(5)}$ denotes the 5-qubit Pauli operation with Z in the k-th place of the tensor product and identity everywhere else. Moreover, according to [proposition 3.10], $U\mathcal{V}_S$ is stabilized by the subgroup $\left\langle US_1U^\dagger, US_2U^\dagger, US_3U^\dagger, US_4U^\dagger \right\rangle$ of $\mathcal{P}_5$. Therefore, $U\mathcal{V}_S$ is stabilized by $\left\{Z_2^{(5)}, Z_3^{(5)}, Z_4^{(5)}, Z_5^{(5)}\right\}$. Thus,

$$U\mathcal{V}_S = \mathbb{C}^2 \otimes |0\rangle^{\otimes 4} := \left\{ v \otimes |0\rangle \otimes |0\rangle \otimes |0\rangle \otimes |0\rangle \;\middle|\; v \in \mathbb{C}^2 \right\}. \tag{59}$$

So considering that $\hat{X}$, $\hat{Y}$, $\hat{Z}$, and $\hat{T}$ act trivially on the orthogonal complement of $\mathcal{V}_S$, $U\hat{X}U^\dagger$, $U\hat{Y}U^\dagger$, $U\hat{Z}U^\dagger$, and $U\hat{T}U^\dagger$ must act trivially on the orthogonal complement of $U\mathcal{V}_S = \mathbb{C}^2 \otimes |0\rangle^{\otimes 4}$. By defining,

$$\begin{aligned}
\hat{\hat{X}} &:= U\hat{X}U^\dagger, \\
\hat{\hat{Y}} &:= U\hat{X}U^\dagger, \\
\hat{\hat{Z}} &:= U\hat{Z}U^\dagger \\
\hat{\hat{T}} &:= U\hat{T}U^\dagger,
\end{aligned} \tag{60}$$

and according to [equation 49],

$$\begin{aligned}
\hat{\hat{T}}\hat{\hat{X}}\hat{\hat{T}}^\dagger &= \hat{\hat{Z}}, \\
\hat{\hat{T}}\hat{\hat{Z}}\hat{\hat{T}}^\dagger &= \hat{\hat{Y}}, \\
\hat{\hat{T}}\hat{\hat{Y}}\hat{\hat{T}}^\dagger &= \hat{\hat{X}}.
\end{aligned} \tag{61}$$

Moreover, $\hat{\hat{X}}$, $\hat{\hat{Y}}$, and $\hat{\hat{Z}}$ satisfiy the same commutation relations as those of $\hat{X}$, $\hat{Y}$, and $\hat{Z}$, and hence as those of X, Y, and Z, and moreover it can be shown that they act like X, Y, and Z in the subspace $\mathbb{C}^2 \otimes |0\rangle^{\otimes 4}$ [6]. Therefore,

$$\hat{\hat{T}} = \exp\left(\frac{i\pi}{3}\right) \left|\tilde{T}_0\right\rangle\!\left\langle\tilde{T}_0\right| + \exp\left(-\frac{i\pi}{3}\right) \left|\tilde{T}_1\right\rangle\!\left\langle\tilde{T}_1\right| + U\left(I_5 - P^{(S)}\right)U^\dagger, \tag{62}$$

where,

$$\begin{aligned}
\left|\tilde{T}_0\right\rangle &:= |T_0\rangle \otimes |0\rangle^{\otimes 4}, \\
\left|\tilde{T}_1\right\rangle &:= |T_1\rangle \otimes |0\rangle^{\otimes 4},
\end{aligned} \tag{63}$$

and $U\left(I_5 - P^{(S)}\right)U^\dagger$ is the orthogonal projector onto $\left(\mathbb{C}^2 \otimes |0\rangle^{\otimes 4}\right)^\perp$. On the other hand, it is clear that upto a phase factor,

$$\begin{aligned}\left|\tilde{T}_0\right\rangle &= U\left|T_0^L\right\rangle, \\ \left|\tilde{T}_1\right\rangle &= U\left|T_1^L\right\rangle.\end{aligned} \tag{64}$$

Therefore applying U to the state $\tilde{\rho}_1$ yields the 5-qubit state,

$$\begin{aligned}&\tilde{\rho}_2 := U\tilde{\rho}_1 U^\dagger = \\ &\left[\frac{\varepsilon_0^5 + 5\varepsilon_0^2\left(1-\varepsilon_0\right)^3}{6}|T_0\rangle\langle T_0| + \frac{\left(1-\varepsilon_0\right)^5 + 5\varepsilon_0^3\left(1-\varepsilon_0\right)^2}{6}|T_1\rangle\langle T_1|\right] \otimes |0000\rangle\langle 0000|.\end{aligned} \tag{65}$$

Now, tracing out the last 4 qubits, we will be left with the single-qubit state

$$\tilde{\rho}_3 := \frac{\varepsilon_0^5 + 5\varepsilon_0^2\left(1-\varepsilon_0\right)^3}{6}|T_0\rangle\langle T_0| + \frac{\left(1-\varepsilon_0\right)^5 + 5\varepsilon_0^3\left(1-\varepsilon_0\right)^2}{6}|T_1\rangle\langle T_1|. \tag{66}$$

Now apply the Clifford gate YH to $\tilde{\rho}_3$ to obtain,

$$o\left(\tilde{\rho}\right) := YH\tilde{\rho}HY = \left(1 - f\left(\varepsilon_0\right)\right)|T_0\rangle\langle T_0| + f\left(\varepsilon_0\right)|T_1\rangle\langle T_1|, \tag{67}$$

where,

$$f\left(\varepsilon_0\right) := \frac{t^5 + 5t^2}{1 + 5t^2 + 5t^3 + t^5}, \quad t := \frac{\varepsilon_0}{1-\varepsilon_0}. \tag{68}$$

Let ε_c denote the only non-trivial value such that $f\left(\varepsilon_c\right) = \varepsilon_c$. It can be calculated that [6],

$$\varepsilon_c = \frac{1}{2}\left(1 - \sqrt{\frac{3}{7}}\right) < 1. \tag{69}$$

Moreover, it can seen that [6] f is monotonically increasing in the interval $[0, \varepsilon_c]$, and hence $f\left(\varepsilon_0\right) < \varepsilon_0$ in this interval.

Now let us explain an algorithm to purify $\tilde{\rho}$ towards $|T_0\rangle$ with a desired precission ε.

The Algorithm for Magic State $|T_0\rangle$ Purification with a Desired Precision:

Let $\varepsilon \in (0,1)$. Starting initially from the state $\tilde{\rho}$ as the input, successively iterate the magic state $|T_0\rangle$ distillation subroutine as described above. For any number n of iterations, the output state must be

$$o^n(\tilde{\rho}) = (1 - f^n(\varepsilon_0))\,|T_0\rangle\langle T_0| + f^n(\varepsilon_0)\,|T_1\rangle\langle T_1|\,. \tag{70}$$

It can be shown that

$$\lim_{n\to\infty} f^n(\varepsilon_0) = 0. \tag{71}$$

Thus, $\tilde{\rho}$ can be purified towards $|\mathrm{T}_0\rangle$ with any desired precision by preparing a large enough number N copies of ρ priorly, and iterating the subroutine for a large enough number of times n. For $\varepsilon_0 \ll 1$, it is seen that $f(\varepsilon_0) \approx 5\varepsilon_0^2$, and hence for every n, $f^n(\varepsilon_0) \approx \frac{1}{5}(5\varepsilon_0)^{2^n}$. Denoting by p_0 the probability of observing the syndrome $(1,1,1,1)$ and hence keeping the state, in the case of $\varepsilon_0 \ll 1$, the number of copies of the single-qubit output state after n iterations of the subroutine must approximately equal $\left(\frac{5}{p_0}\right)^n N$.

Chapter 5

QUANTUM CODES AND CORRECTABLE ERRORS

Let $\mathcal{H}$ denote the Hilbert space of a single qubit, that is a Hilbert space isomorphic to $\mathbb{C}^2$, and let n be a positive integer. Let $\mathrm{U}\left(\mathcal{H}^{\otimes n}\right)$ denote the set of all unitary transformations on the Hilbert space $\mathcal{H}^{\otimes n}$. Let $\mathrm{Dens}\left(\mathcal{H}^{\otimes n}\right)$ denote he set of all density matrices of the Hilbert space $\mathcal{H}^{\otimes n}$. Let $\{|0\rangle, |1\rangle\}$ be a fixed basis of $\mathcal{H}$.

5.1 General Definitions

Definition 5.1: "An error set in the Hilbert space $\mathcal{H}^{\otimes n}$" is defined to be a finite subset $U := \{U_1, \cdots, U_m\}$ of $\mathrm{U}\left(\mathcal{H}^{\otimes n}\right)$. Let $p : U \to [0, 1]$ be a probability distribution on U. The ordered pair (U, p) is called a "noise in the Hilbert space $\mathcal{H}^{\otimes n}$", and the "noise operation corresponded to (U, p)" is defined to be the linear transformation $\mathcal{E} : \mathcal{L}\left(\mathcal{H}^{\otimes n}\right) \to \mathcal{L}\left(\mathcal{H}^{\otimes n}\right)$ such that,

$$\forall\, \rho \in \mathcal{L}\left(\mathcal{H}^{\otimes n}\right) :\ \mathcal{E}(\rho) := \sum_{k=1}^{m} E_k \rho E_k^{\dagger}, \tag{1}$$

where for each k,

$$E_k := p(U_k)\, U_k. \tag{2}$$

It is also conventional to consider the noise as the set $E := \{E_1, \cdots, E_m\}$.

■

Definition 5.2: A linear transformation $\mathcal{E} : \mathcal{L}\left(\mathcal{H}^{\otimes n}\right) \to \mathcal{L}\left(\mathcal{H}^{\otimes n}\right)$ is called a "(n-qubit) quantum channel" if there exists $\{E_1, \cdots, E_m\} \subseteq \mathcal{L}\left(\mathcal{H}^{\otimes n}\right)$ such that,

$$\sum_{k=1}^{m} {E_k}^{\dagger} E_k = I_n, \tag{3}$$

and

$$\forall\, A \in \mathcal{L}\left(\mathcal{H}^{\otimes n}\right):\ \mathcal{E}\left(A\right) = \sum_{k=1}^{m} E_k A {E_k}^{\dagger}. \tag{4}$$

Then $\{E_1, \cdots, E_m\} \subseteq \mathcal{L}\left(\mathcal{H}^{\otimes n}\right)$ is called a "set of operation elements for the quantum channel $\mathcal{E}$".

■

Corollary 5.1: For every noise in $\mathcal{H}^{\otimes n}$, the noise operation is a quantum channel.

□

Proposition 5.1: Let $\mathcal{E} : \mathcal{L}\left(\mathcal{H}^{\otimes n}\right) \to \mathcal{L}\left(\mathcal{H}^{\otimes n}\right)$ be a quantum channel. Then for every density matrix $\rho \in \mathrm{Dens}\left(\mathcal{H}^{\otimes n}\right)$, $\mathcal{E}\left(\rho\right) \in \mathrm{Dens}\left(\mathcal{H}^{\otimes n}\right)$. That is, $\mathcal{E}$ sends density matrices to density matrices.

proof: Let $\rho \in \mathrm{Dens}\left(\mathcal{H}^{\otimes n}\right)$, and let $\{E_1, \cdots, E_m\}$ be a set of operation elements for $\mathcal{E}$.

- Considering that $\mathrm{Tr}\left(\rho\right) = 1$,

$$\begin{aligned}\mathrm{Tr}\left[\mathcal{E}\left(\rho\right)\right] &= \mathrm{Tr}\left[\sum_{k=1}^{m} E_k \rho {E_k}^{\dagger}\right] = \sum_{k=1}^{m} \mathrm{Tr}\left(E_k \rho {E_k}^{\dagger}\right) \\ &= \sum_{k=1}^{m} \mathrm{Tr}\left({E_k}^{\dagger} E_k \rho\right) = \mathrm{Tr}\left[\sum_{k=1}^{m} \left({E_k}^{\dagger} E_k\right) \rho\right] \\ &= \mathrm{Tr}\left[\left(\sum_{k=1}^{m} {E_k}^{\dagger} E_k\right) \rho\right] = \mathrm{Tr}\left(\rho\right) = 1. \end{aligned} \tag{5}$$

- Considering that $\rho^{\dagger} = \rho$,

$$\mathcal{E}\left(\rho\right)^{\dagger} = \left[\sum_{k=1}^{m} E_k \rho {E_k}^{\dagger}\right]^{\dagger} = \sum_{k=1}^{m} E_k \rho {E_k}^{\dagger} = \mathcal{E}\left(\rho\right). \tag{6}$$

- Considering that ρ is a non-negative operator, that is for every unit vector $|\psi\rangle \in \mathcal{H}^{\otimes n}$, $\langle\psi|\rho|\psi\rangle \geq 0$, we have, for every unit vector $|\psi\rangle \in \mathcal{H}^{\otimes n}$,

$$\begin{aligned}\langle\psi|\mathcal{E}\left(\rho\right)|\psi\rangle &= \left\langle \psi \middle| \left[\sum_{k=1}^{m} E_k \rho {E_k}^{\dagger}\right] \middle| \psi \right\rangle \\ &= \sum_{k=1}^{m} \left\langle \psi \middle| E_k \rho {E_k}^{\dagger} \middle| \psi \right\rangle \geq 0. \end{aligned} \tag{7}$$

□

Lemma 5.1: Let $\mathcal{E} : \mathcal{L}(\mathcal{H}^{\otimes n}) \to \mathcal{L}(\mathcal{H}^{\otimes n})$ and $\mathcal{R} : \mathcal{L}(\mathcal{H}^{\otimes n}) \to \mathcal{L}(\mathcal{H}^{\otimes n})$ be a pair of quantum channels. Let $\{E_1, \cdots, E_m\}$ and $\{F_1, \cdots, F_m\}$ be sets of operation elements for $\mathcal{E}$ and $\mathcal{R}$ respectively. Then $\mathcal{E} = \mathcal{R}$ if and only if there exists a $m \times m$ unitary matrix u with entries in $\mathbb{C}$ such that for every j,

$$E_j = \sum_{k=1}^{m} u_{jk} F_k. \tag{8}$$

□

Definition 5.3: A "quantum code (or code space)" $\mathcal{C}$ is defined to be a non-trivial linear subspace of $\mathcal{H}^{\otimes n}$. $\mathcal{C}$ is referred to as a "$[n, k]$ quantum code" if it is a k-dimensional linear subspace of $\mathcal{H}^{\otimes n}$.

■

Definition 5.4: Let $E := \{E_1, \cdots, E_m\}$ be a noise in the Hilbert space $\mathcal{H}^{\otimes n}$ and let $\mathcal{E}$ denote the noise operation associated with it. Let $\mathcal{C}$ be a code space in $\mathcal{H}^{\otimes n}$. E is called a "correctable noise in the code space $\mathcal{C}$" if there exists a quantum channel $\mathcal{R} : \mathcal{L}(\mathcal{H}^{\otimes n}) \to \mathcal{L}(\mathcal{H}^{\otimes n})$ such that for every density-matrix ρ in $\mathcal{L}(\mathcal{H}^{\otimes n})$ with support in $\mathcal{C}$,

$$(\mathcal{R} \circ \mathcal{E})(\rho) = \rho. \tag{9}$$

Then such a transformation $\mathcal{R}$ is called an "error-correction operation correcting the noise E (or $\mathcal{E}$) on the code space $\mathcal{C}$".

■

5.2 The General Criteria For the Correctability of a Noise On a Code Space

Theorem 5.1: Let $E := \{E_1, \cdots, E_m\}$ be a noise in $\mathcal{H}^{\otimes n}$, and let $\mathcal{C}$ be a code space in $\mathcal{H}^{\otimes n}$. Let $P_{\mathcal{C}}$ denote the orthogonal projector onto the subspace $\mathcal{C}$ of $\mathcal{H}^{\otimes n}$. E is

a correctable noise in the code space $\mathcal{C}$ if and only if there exists a $m \times m$ matrix with entries in complex numbers such that for each j and k,

$$P_{\mathcal{C}} E_j^{\dagger} E_k P_{\mathcal{C}} = \alpha_{jk} P_{\mathcal{C}}. \tag{10}$$

It is trivial to see that if this condition is satisfied the matrix α must be Hermitian.

□

Theorem 5.2: Let $E := \{E_1, \cdots, E_m\}$ and $F := \{F_1, \cdots, F_l\}$ be a pair of noises in $\mathcal{H}^{\otimes n}$, and let $\mathcal{C}$ be a code space in $\mathcal{H}^{\otimes n}$. Suppose that E is a correctable noise in the code space $\mathcal{C}$, and let $\mathcal{R} : \mathcal{L}(\mathcal{H}^{\otimes n}) \to \mathcal{L}(\mathcal{H}^{\otimes n})$ be an operation that corrects the noise E on the code space $\mathcal{C}$. If there exists a $l \times m$ matrix M with complex entries such that for all $j \in \{1, \cdots, l\}$,

$$F_j = \sum_{k=1}^{m} M_{jk} E_k, \tag{11}$$

then F is also a correctable noise on the code space $\mathcal{C}$ and $\mathcal{R}$ also corrects F on $\mathcal{C}$.

□

5.3 Syndrome Measurements and Noise Recovery Algorithms

Definition 5.5: Let $(\mathcal{M}_1, \cdots, \mathcal{M}_p)$ be a tuple of projective measurements in the Hilbert space $\mathcal{H}^{\otimes n}$, and let $|\psi\rangle$ be a quantum state in $\mathcal{H}^{\otimes n}$. We say that "the tuple $(\mathcal{M}_1, \cdots, \mathcal{M}_p)$ of measurements has a syndrome on the state $|\psi\rangle$" if $|\psi\rangle$ is an eigenstate of each measurement $\mathcal{M}_k$. If $(\mathcal{M}_1, \cdots, \mathcal{M}_p)$ has a syndrome on $|\psi\rangle$, then trivially measuring $|\psi\rangle$ upon each measurement $\mathcal{M}_k$ yields a result m_k with absolute certainty, and then the tuple $(m_1, \cdots, m_p)$ is called the "syndrome of the tuple $(\mathcal{M}_1, \cdots, \mathcal{M}_p)$ of measurements on the state $|\psi\rangle$".

■

Definition 5.6: Let $(\mathcal{M}_1, \cdots, \mathcal{M}_p)$ be a tuple of projective measurements, let $\mathcal{C}$ be a code space, and let $E := \{E_1, \cdots, E_m\}$ be a noise in the Hilbert space $\mathcal{H}^{\otimes n}$. We

say that "$(\mathcal{M}_1, \cdots, \mathcal{M}_p)$ is a tuple of syndrome measurements on the pair $(\mathcal{C},\, E)$" if $(\mathcal{M}_1, \cdots, \mathcal{M}_p)$ has a syndrome on each state of the set

$$\bigcup_{k=1}^{k} \{E_k \left|\psi\right\rangle \mid \left|\psi\right\rangle \in \mathcal{C}\}\,.$$

■

Definition 5.7: Let $\mathcal{C}$ be a code space in $\mathcal{H}^{\otimes n}$, and let $E := \{E_1, \cdots, E_m\}$ be a correctable noise in the code space $\mathcal{C}$. A "syndrome-based noise recovery algorithm correcting the noise E on the code space $\mathcal{C}$" is by definition an algorithm of the following type employing a tuple $(\mathcal{M}_1, \cdots, \mathcal{M}_p)$ of syndrome measurements on $(\mathcal{C},\, E)$ such that the quantum operation associated with the algorithm corrects the noise E on the code space $\mathcal{C}$.

Algorithm: Suppose that a state $\left|\psi\right\rangle \in \mathcal{H}^{\otimes n}$ is given. For each k, let p_k and U_k denote the unique real number and unitary operator such that $E_k = p_k U_k$. Let R_k denote the set of all results of the measurement $\mathcal{M}_k$, for each k.

i. Set a map $\Gamma :\, R_1 \times \cdots \times R_p \to \{U_1, \cdots, U_m\}$.

ii. Perform the measurements of the tuple $(\mathcal{M}_1, \cdots, \mathcal{M}_p)$ successively respecting the order of the tuple, and record the ordered tuple of results $(m_1, \cdots, m_p)$ obtained.

iii. Apply the unitary gate $\Gamma\,(m_1, \cdots, m_p)$ on the state.

∗ *Note that this algorithm is assumed to act on any state of the whole Hilbert space $\mathcal{H}^{\otimes n}$ rather than the restricted space $\bigcup_{k=1}^{k} \{E_k \left|\psi\right\rangle \mid \left|\psi\right\rangle \in \mathcal{C}\}$. There is no fundamental difference between this case and that of limiting the input states of the algorithm to this subset of the whole Hilbert space as far as we are concerned with correcting a noise occurring on the code space. The motivation behind taking this approach is to be able to associate a quantum operation with the algorithm.*
In addition, note that when the input states are restricted to $\bigcup_{k=1}^{k} \{E_k \left|\psi\right\rangle \mid \left|\psi\right\rangle \in \mathcal{C}\}$, then the order of measurements of the second step of the algorithm will not matter.

Furthermore, it is important to note that as far as the main concern is to correct the noise E on $\mathcal{C}$, the only subset of $R_1 \times \cdots \times R_p$ that matters in constructing the function Γ is the set of all possible tuples of results of the tuple of measurements that can occur upon measuring the states in $\bigcup_{k=1}^{k} \{E_k |\psi\rangle \mid |\psi\rangle \in \mathcal{C}\}$, and the values of Γ at other points can be chosen arbitrarily. So the noise recovery algorithm can be stated just by considering the construction of the map Γ within this restricted domain. Again the motivation behind considering Γ as a map over the whole result space is a matter of formality, that is to regard the algorithm as a quantum operation on the whole Hilbert space.

If $(\mathcal{M}_1, \cdots, \mathcal{M}_p)$ is not a syndrome measurement on $(\mathcal{C}, E)$, but the quantum operation associated with the algorithm above corrects the noise E on $\mathcal{C}$, then it is referred to as a "measurement-based noise recovery algorithm correcting the noise E on the code space $\mathcal{C}$".

■

5.4 Examples of Correctable Noise On a Code Space

We will simply denote by $|000\rangle$ and $|111\rangle$ the states $|0\rangle \otimes |0\rangle \otimes |0\rangle$ and $|1\rangle \otimes |1\rangle \otimes |1\rangle$, respectively. We denote by I, X, Y, Z the identity, x-Pauli, y-Pauli, and $z-Pauli$ operators on the single qubit space $\mathcal{H}$, respectively. For any unitary operator on $\mathcal{H}$ we will simply denote by U_k the unitary operator $O_1 \otimes \cdots \otimes O_n$ where $O_i = U_i$ and $O_k = I$ for $k \neq I$, when there is no confusion about the number n. Additionally, when there is no chance of confusion, we will also denote by I the identity operator of the Hilbert space $\mathcal{H}^{\otimes n}$.

5.4.1 Three-Qubit Bit-Flip Code

Definition 5.8: The "three-qubit bit-flip code $\mathcal{C}_{3B}$" is defined as

$$\mathcal{C}_{3B} := \mathsf{span}\,\{|000\rangle, |111\rangle\} \subseteq \mathcal{H}^{\otimes 3}. \tag{12}$$

The single-qubit bit-flip noise in the Hilbert space $\mathcal{H}^{\otimes 3}$ is defined to be $B_3 := \{I, X_1, X_2, X_3\}$.

■

Theorem 5.3: The single-qubit bit-flip noise $B_3 := \{I, X_1, X_2, X_3\}$ is correctable in the code space $\mathcal{C}_{3B}$. The pair of projective measurements (Z_1Z_2, Z_2Z_3) is a pair of syndrome measurements on ($\mathcal{C}_{3B}$, B_3). The following is a syndrome-based noise recovery algorithm correcting the noise B_3 on the code space $\mathcal{C}_{3B}$.

Single-Qubit Bit-Flip Noise Recovery Algorithm in Three-Qubit Bit-Flip Code

It is known that the result set of each of the measurements Z_1Z_2 and Z_2Z_3 is $\{+1, -1\}$.

i. Set the map $\Gamma : \{+1, -1\}^2 \to \{I, X_1, X_2, X_3\}$ as

$$\begin{aligned} \Gamma(+1, +1) &= I, \\ \Gamma(-1, +1) &= X_1, \\ \Gamma(-1, -1) &= X_2, \\ \Gamma(+1, -1) &= X_3. \end{aligned} \tag{13}$$

ii. Perform the measurements Z_1Z_2 and Z_2Z_3 successively, and record the ordered pair of results (m_1, m_2) obtained.

iii. Apply the unitary gate $\Gamma(m_1, m_2)$ on the state.

□

5.4.2 Three-Qubit Phase-Flip Code

Definition 5.9: The "three-qubit phase-flip code $\mathcal{C}_{3Ph}$" is defined as

$$\mathcal{C}_{3Ph} := \mathsf{span}\left\{|+\rangle^{\otimes 3}, |-\rangle^{\otimes 3}\right\} \subseteq \mathcal{H}^{\otimes 3}, \tag{14}$$

where,

$$|+\rangle := \frac{|0\rangle + |1\rangle}{\sqrt{2}},$$
$$|-\rangle := \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{15}$$

The single-qubit phase-flip noise in the Hilbert space $\mathcal{H}^{\otimes 3}$ is defined to be $Ph_3 := \{I, Z_1, Z_2, Z_3\}$.

■

Theorem 5.4: The single-qubit phase-flip noise $Ph_3 := \{I, Z_1, Z_2, Z_3\}$ is correctable in the code space $\mathcal{C}_{3Ph}$. The pair of projective measurements $(X_1X_2,\ X_2X_3)$ is a pair of syndrome measurements on $(\mathcal{C}_{3Ph},\ Ph_3)$. The following is a syndrome-based noise recovery algorithm correcting the noise Ph_3 on the code space $\mathcal{C}_{3Ph}$.

Single-Qubit Phase-Flip Noise Recovery Algorithm in Three-Qubit Phase-Flip Code

It is known that the result set of each of the measurements X_1X_2 and X_2X_3 is $\{+1, -1\}$.

i. Set the map $\Gamma : \{+1, -1\}^2 \to \{I, Z_1, Z_2, Z_3\}$ as

$$\Gamma(+1, +1) = I,$$
$$\Gamma(-1, +1) = Z_1,$$
$$\Gamma(-1, -1) = Z_2,$$
$$\Gamma(+1, -1) = Z_3. \tag{16}$$

ii. Perform the measurements X_1X_2 and X_2X_3 successively, and record the ordered pair of results (m_1, m_2) obtained.

iii. Apply the unitary gate $\Gamma(m_1, m_2)$ on the state.

□

5.4.3 Shor Code

Definition 5.10: The "9-qubit Shor code $\mathcal{C}_{9Sh}$" is defined as

$$\mathcal{C}_{9Sh} := \mathsf{span}\left\{\left(\frac{|000\rangle+|111\rangle}{\sqrt{2}}\right)^{\otimes 3}, \left(\frac{|000\rangle-|111\rangle}{\sqrt{2}}\right)^{\otimes 3}\right\} \subseteq \mathcal{H}^{\otimes 9}. \tag{17}$$

■

Theorem 5.5: The noise $P = \{I\} \cup \{X_i \mid i = 1, \cdots, 9\} \cup \{Y_i \mid i = 1, \cdots, 9\} \cup \{Z_i \mid i = 1, \cdots, 9\}$ consisting merely of single-qubit Pauli errors is correctable in the code space $\mathcal{C}_{9Sh}$. The tuple of projective measurements $(Z_1Z_2, Z_2Z_3, Z_4Z_5, Z_5Z_6, Z_7Z_8, Z_8Z_9, X_1X_2X_3X_4X_5X_6, X_4X_5X_6X_7X_8X_9)$ is a tuple of syndrome measurements on $(\mathcal{C}_{9Sh}, P)$. The following is a syndrome-based noise recovery algorithm correcting the noise P on the code space $\mathcal{C}_{9Sh}$.

Single-Qubit Pauli Noise Recovery Algorithm in Shor Code

It is known that the result set of each of the measurements mentioned above is $\{+1, -1\}$. *On the other hand it can be easily verified that the set of all possible* 8*-tuple of outcomes of the mentioned tuple of measurements upon measuring a state*

in $\bigcup_{E\in P}\{E\,|\psi\rangle \mid |\psi\rangle \in \mathcal{C}_{9Sh}\}$ *is* $\{x_0,\cdots,x_9\}\times\{z_0,\cdots,z_3\}$, *where*

$$
\begin{aligned}
x_0 &= (+1,+1,+1,+1,+1,+1)\\
x_1 &= (-1,+1,+1,+1,+1,+1)\\
x_2 &= (-1,-1,+1,+1,+1,+1)\\
x_3 &= (+1,-1,+1,+1,+1,+1)\\
x_4 &= (+1,+1,-1,+1,+1,+1)\\
x_5 &= (+1,+1,-1,-1,+1,+1)\\
x_6 &= (+1,+1,+1,-1,+1,+1)\\
x_7 &= (+1,+1,+1,+1,-1,+1)\\
x_8 &= (+1,+1,+1,+1,-1,-1)\\
x_9 &= (+1,+1,+1,+1,+1,-1)\\
z_0 &= (+1,+1)\,,\\
z_1 &= (-1,+1)\,,\\
z_2 &= (-1,-1)\,,\\
z_3 &= (+1,-1)\,.
\end{aligned}
\tag{18}
$$

i. Set the map $\Gamma:\{x_0,\cdots,x_9\}\times\{z_0,\cdots,z_3\}\to P$ as

$$
\begin{aligned}
&\Gamma(x_0,z_0)=I,\\
&\Gamma(x_i,z_0)=X_i,\quad i=1,\cdots,9,\\
&\Gamma(x_0,z_i)=Z_{3i},\quad i=1,2,3,\\
&\Gamma(x_i,z_1)=Y_i,\quad i=1,2,3,\\
&\Gamma(x_i,z_2)=Y_i,\quad i=4,5,6,\\
&\Gamma(x_i,z_3)=Y_i,\quad i=7,8,9.
\end{aligned}
\tag{19}
$$

ii. Perform the measurements successively, and record the 8-tuple of results $(m_1,\cdots,m_8)$ obtained.

iii. Apply the unitary gate $\Gamma(m_1,\cdots,m_8)$ on the state.

□

Theorem 5.6: Let $E = \{U_1, \cdots, U_m\}$ be a noise in $\mathcal{H}^{\otimes 9}$ such that each U_i is a single-qubit unitary error, that is an operator of type $O_1 \otimes \cdots \otimes O_n$ such that at most one O_i is a non-identity unitary operator on $\mathcal{H}$. The noise E is correctable in $\mathcal{C}_{9Sh}$, and the algorithm of [theorem 5.5] is a measurement-based noise recovery algorithm correcting the noise E on the code space $\mathcal{C}_{9Sh}$.

$*$ *Let $\mathcal{H}$ denote the Hilbert space of a single qubit, that is a Hilbert space isomorphic o $\mathbb{C}^2$, and let n be a positive integer. Let $\mathrm{U}(\mathcal{H}^{\otimes n})$ denote the set of all unitary transformations on the Hilbert space $\mathcal{H}^{\otimes n}$. Let $\mathrm{Dens}(\mathcal{H}^{\otimes n})$ denote he set of all density matrices of the Hilbert space $\mathcal{H}^{\otimes n}$. Let $\{|0\rangle, |1\rangle\}$ be a fixed basis of $\mathcal{H}$.*

□

5.5 Stabilizer Codes

In this section, some definitions and claims stated in the "stabilizer formalism" chapter are recalled, and since the claims are proved in that chapter we do not repeat their proofs here.

Definition 5.11: The "Pauli group on n qubits" is defined as

$$\mathcal{P}_n := \{\alpha O_1 \otimes \cdots \otimes O_n \mid \alpha \in \{1, -1, i, -i\},\ O_i \in \{I, X, Y, Z\},\ i = 1, \cdots, n\}. \tag{20}$$

■

Lemma 5.2:

- Each element of $\mathcal{P}_n$ is diagonalizable and has $\{1, -1\}$ as its set of all eigenvalues.
- Any pair g_1 and g_2 of elements of S either commute or anti-commute. That is, either $g_1 g_2 = g_2 g_1$ or $g_1 g_2 = -g_2 g_1$.
- $\mathcal{P}_n$ spans $\mathcal{L}(\mathcal{H}^{\otimes n})$.

□

Lemma 5.3: $\mathcal{P}_n$ has the structure of a group when endowed with the binary operation of composition of operators.

$*$ *If the I, X, Y, Z are viewed alternatively as he matrix representations of these operators with respect to the standard basis of $\mathcal{H}$, then the operation of $\mathcal{P}_n$ can be viewed as the matrix multiplication operation.*

□

Definition 5.12: Any subgroup of $\mathcal{P}_n$ is called a "stabilizer group" in the Hilbert space $\mathcal{H}^{\otimes n}$. For any stabilizer group S in $\mathcal{H}^{\otimes n}$,

$$\mathcal{V}_S := \left\{ |\psi\rangle \in \mathcal{H}^{\otimes n} \mid (\forall\, g \in S\colon\ g\,|\psi\rangle = |\psi\rangle) \right\}. \tag{21}$$

In other words, $\mathcal{V}_S$ is defined to be the set of all common eigen-vectors of all elements of S with eigen-value 1, that is the intersection of the eigen-spaces of all elements of S with eigen-value 1. $\mathcal{V}_S$ is called the "space stabilized by the Pauli group S in $\mathcal{H}^{\otimes n}$". Such a space $\mathcal{V}_S$ is called a "stabilizer code" or an "additive quantum code".

■

Lemma 5.4: Let S be a stabilizer group in $\mathcal{H}^{\otimes n}$. $\mathcal{V}_S$ is a linear subspace of $\mathcal{H}^{\otimes n}$.

□

Lemma 5.5: If $-I \notin S$ then $-iI$ and iI are also not in S. Generally, if $-I \notin S$ then

$$S \subseteq \{\alpha O_1 \otimes \cdots \otimes O_n \mid \alpha \in \{1, -1\},\ O_i \in \{I, X, Y, Z\},\ i = 1, \cdots, n\}, \tag{22}$$

and hence for all $g \in S$, $g^2 = I$ and $g^\dagger = g$.

□

Theorem 5.7: Let S be a stabilizer group in $\mathcal{H}^{\otimes n}$. $\mathcal{V}_S$ is a non-trivial linear subspace of $\mathcal{H}^{\otimes n}$ if and only if the following conditions hold.

- $-I \notin S$.

- The elements of S commute pairwise, that is for each pair g_1 and g_2 of elements in S, $g_1 g_2 = g_2 g_1$.

□

Theorem 5.8: Let S be a stabilizer group in $\mathcal{H}^{\otimes n}$ such that $\mathcal{V}_S$ is non-trivial. Let $\{g_1, \cdots, g_m\}$ be a set of independent generators of the group S, that is $S = \langle g_1, \cdots, g_m \rangle$ and no g_i is in the subgroup generated by $\{g_1, \cdots, g_m\} \setminus \{g_i\}$. Then the dimension of the vector space $\mathcal{V}_S$ is $n - m$.

$*$ *This theorem, on the other hand, implies that all sets of independent generators of a stabilizer group that stabilizes a non-trivial vector space must have the same number of elements.*

□

5.5.1 A Criteria for the Correctability of Pauli Errors on Stabilizer Codes

Lemma 5.6: Let S be a stabilizer group in $\mathcal{H}^{\otimes n}$. If $-I \notin S$, and in particular if $\mathcal{V}_S$ is non-trivial, then the centralizer and the normalizer of S in $\mathcal{P}_n$, that is $Z(S)$ and $N(S)$ are equal, that is,

$$Z(S) = \{g \in \mathcal{P}_n \mid (\forall\, s \in S\colon\ sg = gs)\} = \left\{g \in \mathcal{P}_n \mid gSg^\dagger \subseteq S\right\} = N(S). \quad (23)$$

□

Theorem 5.9: Let S be a stabilizer group in $\mathcal{H}^{\otimes n}$ that stabilizes a non-trivial space. Let $E = \{E_1, \cdots, E_l\} \subseteq \mathcal{P}_n$ such that for each E_j and E_k in E, $E_j^\dagger E_k \notin N(S) \setminus S$. Then E is correctable on the code space $\mathcal{V}_S$.

proof: Let P denote the orthogonal projector onto $\mathcal{V}_S$, and let $\{g_1, \cdots, g_m\}$ be an independent generator of S. So,

$$P = \frac{1}{2^m} \prod_{i=1}^{m} (I_n + g_i)\,. \quad (24)$$

Let $E_j, E_k \in E$. Then either ${E_j}^\dagger E_k \in S$ or ${E_j}^\dagger E_k \in \mathcal{P}_n - N(S)$.

First suppose that ${E_j}^\dagger E_k \in S$. Then since for every $g \in S$, $PgP = P$, we have

$PE_j{}^\dagger E_k P = P$.

Now suppose that $E_j{}^\dagger E_k \in \mathcal{P}_n - N(S)$. Then there must exist at least one g_j in the generating set of S such that $\left(E_j{}^\dagger E_k\right) g_j = -g_j \left(E_j{}^\dagger E_k\right)$. Without loss of generality we can safely assume that $g_j = g_1$. So $\left(E_j{}^\dagger E_k\right) g_1 = -g_1 \left(E_j{}^\dagger E_k\right)$, and hence,

$$\begin{aligned}\left(E_j{}^\dagger E_k\right) P &= \frac{1}{2^m}\left(E_j{}^\dagger E_k\right) \prod_{i=1}^{m} \left(I_n + g_i\right) \\ &= \frac{1}{2^m}\left(I_n - g_1\right)\left(E_j{}^\dagger E_k\right) \prod_{i=2}^{m} \left(I_n + g_i\right). \end{aligned} \tag{25}$$

Therefore,

$$P\left(E_j{}^\dagger E_k\right) P = \frac{1}{2^m} P\left(I_n - g_1\right)\left(E_j{}^\dagger E_k\right) \prod_{i=2}^{m} \left(I_n + g_i\right). \tag{26}$$

But considering that $\left(I_n - g_1\right)\left(I_n + g_1\right) - 0$, we have,

$$P\left(I_n - g_1\right) = \left(I_n - g_1\right) P = \frac{1}{2^m}\left(I_n - g_1\right)\left(I_n - g + 1\right) \prod_{i=2}^{m} \left(I_n + g_i\right) = 0. \tag{27}$$

Therefore $P\left(E_j{}^\dagger E_k\right) P = 0$. So according to [theorem 5.1] E is correctable on $\mathcal{V}_S$.

□

Theorem 5.10: Let S be a stabilizer group in $\mathcal{H}^{\otimes n}$ that stabilizes a non-trivial space. Let $E = \{E_1, \cdots, E_l\} \subseteq \mathcal{P}_n$ such that for each E_1 and E_2 in E, $E_1^\dagger E_2 \notin N(S) \setminus S$. Let $\{g_1, \cdots, g_m\}$ be a independent set of generators of S. $(g_1, \cdots, g_m)$ is a tuple of syndrome measurements on $(\mathcal{V}_S, E)$. Furtheremore, for every $|\psi\rangle \in \mathcal{V}_S$ and for every $E_k \in E$, the syndrome of the tuple $(g_1, \cdots, g_m)$ of measurements on $E_k|\psi\rangle$ is $\left(\beta_1^k, \cdots, \beta_m^k\right)$, where for each j, β_j^k is the unique element of $\{1, -1\}$ such that $E_k g_j E_k^\dagger = \beta_j^k g_j$. The following is a syndrome-based noise recovery algorithm correcting the noise E on the code space $\mathcal{V}_S$.

Pauli Noise Recovery Algorithm in Additive Quantum Codes

It is clear that the result set of each measurement g_i is $\{+1, -1\}$.

i. Set the map $\Gamma : \left\{\left(\beta_1^k, \cdots, \beta_m^k\right) \mid k = 1, \cdots, l\right\} \to E$ as

$$\Gamma\left(\beta_1^k, \cdots, \beta_m^k\right) = E_k,\ k = 1, \cdots, l. \tag{28}$$

ii. Perform the measurements g_i successively, and record the tuple of results $(\beta_1, \cdots, \beta_m)$ obtained.

iii. Apply the unitary gate $\Gamma(\beta_1, \cdots, \beta_m)$ on the state.

□

5.6 The Structure of Classical Linear Codes

We will simply denote by $\mathbb{F}_2$ *the quotient ring* $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$ *with its canonical addition and multiplication operations, which is known to have the structure of a field. Let* n *be a positive integer. It is clear that* $\mathbb{F}_2^n$ *is a finite vector space over the field* $\mathbb{F}_2$ *with* 2^n *elements and dimension* n*. We will simply denote by* $\mathbf{0}$ *the neutral element of addition in the vector space* $\mathbb{F}_2^n$*. We assume that the vector space* $\mathbb{F}_2^n$ *over the field* $\mathbb{F}_2$ *is endowed with the standard inner product* $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{j=1}^{n} x_j y_j$ *for every* $\mathbf{x} = x_1 \cdots x_n$ *and* $\mathbf{y} = y_1 \cdots y_n$ *in* $\mathbb{F}_2^n$*, and hence will consider* $\mathbb{F}_2^n$ *as an inner-product space. For any linear subspace* V *of* $\mathbb{F}_2^n$*, we will simply denote by* $V^\perp$ *the orthogonal complement of* V *in* $\mathbb{F}_2^n$*, that is the unique linear subspace* $V^\perp$ *of* $\mathbb{F}_2^n$ *such that* $\mathbb{F}_2^n = V \oplus V^\perp$*, which equivalently consists of all vectors in* $\mathbb{F}_2^n$ *perpendicular to all vectors of* V *with respect to the standard inner product.*

5.6.1 General Classical Codes

Definition 5.13: Any non-empty subset C of $\mathbb{F}_2^n$, that is a collection of strings $\mathbf{x} = x_1 \cdots x_n$ with each x_i in $\mathbb{F}_2$, is called a "n-bit classical code". Any element of $\mathbb{F}_2^n - C$ is called a "corrupted vector with respect to the code C".

■

Definition 5.14: Let C be a n-bit classical code. For every $\mathbf{x}$ and $\mathbf{y}$ in $\mathbb{F}_2$, the "Hamming distance between $\mathbf{x}$ and $\mathbf{y}$" is defined as the number of components at which they differ, that is,

$$\mathrm{d}_H(\mathbf{x}, \mathbf{y}) := |\{k \mid x_k \neq y_k\}|. \tag{29}$$

■

Definition 5.15: Let C be a n-bit classical code. For every $\mathbf{x}$ in $\mathbb{F}_2$, the Hamming weight of $\mathbf{x}$ is defined as the Hamming distance between $\mathbf{x}$ and $\mathbf{0}$, that is,

$$\mathrm{w}_H(\mathbf{x}) := \mathrm{d}_H(\mathbf{x}, \mathbf{0}), \tag{30}$$

which clearly equals the number of non-zero components of $\mathbf{x}$.

■

Lemma 5.7: Let C be a n-bit classical code. For every $\mathbf{x}$ and $\mathbf{y}$ in $\mathbb{F}_2$,

$$\mathrm{d}_H(\mathbf{x}, \mathbf{y}) = \mathrm{w}_H(\mathbf{x} + \mathbf{y}). \tag{31}$$

□

Theorem 5.11: Let C be a n-bit classical code. d_H is a metric on $\mathbb{F}_2^n$.

□

Definition 5.16: Let C be a n-bit classical code. For every $\mathbf{x} \in \mathbb{F}_2^n$, the "hamming distance of $\mathbf{x}$ from the code C" is defined as,

$$\mathrm{d}_H(\mathbf{x}; C) := \min\{\mathrm{d}_H(\mathbf{x}, \mathbf{v}) \mid \mathbf{v} \in C\}. \tag{32}$$

■

Definition 5.17: Let C be a n-bit classical code. The "distance of the code C" is defined to be,

$$\mathrm{D}_n(C) := \min\{\mathrm{d}_H(\mathbf{x}, \mathbf{y}) \mid \mathbf{x} \neq \mathbf{y}\}. \tag{33}$$

■

Definition 5.18: Let C be a n-bit classical code with 2^k elements for some positive integer k. Then C is called a "$[n, k, \mathrm{D}_n(C)]$ classical code".

■

Lemma 5.8: Let C be a n-bit classical code with 2^k elements for some positive integer k. Let t be an integer such that $\mathrm{D}_n(C) \geq 2t + 1$. For every $\mathbf{x} \in \mathbb{F}_2^n - C$ such that $\mathrm{d}_H(\mathbf{x}; C) \leq t$, there exists a unique $\mathbf{v} \in C$ such that $\mathrm{d}_H(\mathbf{x}, \mathbf{v}) \leq t$.

□

Definition 5.19: Let C be a n-bit classical code with 2^k elements for some positive integer k. Let t be the greatest integer such that $\mathrm{D}_n(C) \geq 2t+1$. Then it is said that "the code C is capable of correcting errors on upto t bits", and the "vector recovered from $\mathbf{x}$" for any $\mathbf{x} \in \mathbb{F}_2^n - C$ such that $\mathrm{d}_H(\mathbf{x}; C) \leq t$, is defined to be the unique vector $\mathbf{v}$ satisfying $\mathrm{d}_H(\mathbf{x}, \mathbf{v}) \leq t$. Also any vector $\mathbf{x} \in \mathbb{F}_2^n - C$ such that $\mathrm{d}_H(\mathbf{x}; C) \leq t$ is called a "correctable corrupted vector with respect to the code C".

■

Theorem 5.12: Let C be a $[n, k, d]$ classical code such that $d = 2t+1$ for some integer. Then,

$$2^k \sum_{j=0}^{t} \binom{n}{j} \leq 2^n. \tag{34}$$

This inequality is referred to as the "Hamming bound on the classical codes".

□

5.6.2 Classical Linear Codes

Definition 5.20: Let C be a n-bit classical code. C is referred to as a "classical linear code" if C is a linear subspace of $\mathbb{F}_2^n$. If C is a k-dimensional vector subspace of $\mathbb{F}_2^n$ then it is also called a "$[n, k, \mathrm{D}_n(C)]$, or simply a "$[n, k]$, classical linear code".

■

Definition 5.21: Let C be a $[n, k, d]$ classical linear code. Let $\{\mathbf{g}_1, \cdots \mathbf{g}_k\}$ be a basis for the vector space C. Then we call the function $f : \mathbb{F}_2^k \to \mathbb{F}_2^n$ a "linear map encoding k bits into n bits of information", where for every $\mathbf{v} = v_1 \cdots v_k$ in $\mathbb{F}_2^k$,

$$f(\mathbf{v}) := \sum_{j=1}^{k} v_k \mathbf{g}_k. \tag{35}$$

Equivalently, for every $\mathbf{v} = v_1 \cdots v_k$ in $\mathbb{F}_2^k$, $f(\mathbf{v}) = \mathbf{v}G$, where is a $k \times n$ matrix with

entries in $\mathbb{F}_2$ defines as,

$$G := \begin{pmatrix} \mathbf{g}_1 \\ \cdots \\ \mathbf{g}_k \end{pmatrix}. \tag{36}$$

The matrix G is called a "generator matrix of the linear code C (corresponded to the basis $\{\mathbf{g}_1, \cdots \mathbf{g}_k\}$)".

■

Definition 5.22: Let C be a $[n, k, d]$ classical linear code. Let $\{\mathbf{h}_1, \cdots \mathbf{h}_{n-k}\}$ be a basis for the vector space $C^{\perp}$. The matrix

$$H := \begin{pmatrix} \mathbf{h}_1 \\ \cdots \\ \mathbf{h}_{n-k} \end{pmatrix}, \tag{37}$$

is called a "parity-check matrix of the linear code C (corresponded to the basis $\{\mathbf{h}_1, \cdots \mathbf{h}_{n-k}\}$)".

■

Lemma 5.9: Let C be a $[n, k, d]$ classical linear code. Let $\{\mathbf{h}_1, \cdots \mathbf{h}_{n-k}\}$ be a basis for the vector space $C^{\perp}$, and let H denote the parity-check matrix correponded to this basis. C equals the kernel of $H^{\intercal}$. A matrix is considered to act on a vector from the right, here.

□

Lemma 5.10: Let C be a $[n, k, d]$ classical linear code. Let $\{\mathbf{g}_1, \cdots \mathbf{g}_k\}$ be a basis for the vector space C, let $\{\mathbf{h}_1, \cdots \mathbf{h}_{n-k}\}$ be a basis for the vector space $C^{\perp}$, and let G and H be the generator and parity-check matrices associated with them, respectively.

$$GH^{\intercal} = 0, \tag{38}$$

where 0 denotes the $k \times (n-k)$ zero matrix.

□

Definition 5.23: Let C be a $[n, k, d]$ classical linear code. Any vector $\mathbf{x}$ in $\mathbb{F}_2^n - C$ is a correctable corrupted vector. For any vector $\mathbf{x}$ in $\mathbb{F}_2^n - C$, the vector $\mathbf{x} - \mathbf{e}$ is the vector recovered from $\mathbf{x}$, where $\mathbf{e}$ is the unique vector in the coset of C in $\mathbb{F}_2^n$ containing $\mathbf{x}$ with the least Hamming weight, that is the unique vector $\mathbf{e} \in C$ with the least Hamming weight such that $[\mathbf{e}] = [\mathbf{x}]$.

■

5.7 Calderbank-Shor-Steane Codes

Let n be a positive integer. For a given unitary operation U on $\mathcal{H}$, and a non-negative positive integer t less than or equal to n, We will denote by $[U]_n^{\leq t}$ the set of all operators like $O_1 \otimes \cdots O_n$ with each O_i in $\{I, U\}$ such that the number of O_i-s equal to U is less than or equal to t.

5.7.1 The Construction of CSS Codes

Definition 5.24: Let C_1 and C_2 be $[n, k_1, d]$ and $[n, k_2, d]$ classical linear codes such that $C_2 \subset C_1$. For every $\mathbf{x} \in \mathbb{F}_2^n$,

$$|\mathbf{x} + C_2\rangle := \frac{1}{\sqrt{|C_2|}} \sum_{\mathbf{y} \in C_2} |\mathbf{x} + \mathbf{y}\rangle \,. \tag{39}$$

■

Lemma 5.11: Let C_1 and C_2 be $[n, k_1, d]$ and $[n, k_2, d]$ classical linear codes such that $C_2 \subset C_1$. Let $\mathbf{x}_1, \mathbf{x}_2 \in C_1$ such that $\mathbf{x}_1$ and $\mathbf{x}_2$ are in the same coset in C_1/C_2, that is $\mathbf{x}_1 - \mathbf{x}_2 \in C_2$. Then

$$|\mathbf{x}_1 + C_2\rangle = |\mathbf{x}_2 + C_2\rangle \,. \tag{40}$$

□

Definition 5.25: Let C_1 and C_2 be $[n, k_1, d]$ and $[n, k_2, d]$ classical linear codes such that $C_2 \subset C_1$. According to the lemma above, for every element a in the quotient

group C_1/C_2 the following is well-defined.

$$|a\rangle_{C_1/C_2} := \frac{1}{\sqrt{|C_2|}} \sum_{\mathbf{y} \in C_2} |\mathbf{x} + \mathbf{y}\rangle \,, \tag{41}$$

for any choice of $\mathbf{x} \in a$.

■

Lemma 5.12: Let C_1 and C_2 be $[n, k_1, d]$ and $[n, k_2, d]$ classical linear codes such that $C_2 \subset C_1$. For every $a, b \in C_1/C_2$ such that $a \neq b$, $|a\rangle_{C_1/C_2} \neq |b\rangle_{C_1/C_2}$. Moreover, $\left\{ |a\rangle_{C_1/C_2} \mid a \in C_1/C_2 \right\}$ is an orthonormal subset of $\mathcal{H}^{\otimes n}$ with respect to the standard inner product on $\mathcal{H}^{\otimes n}$.

□

Definition 5.26: Let C_1 and C_2 be $[n, k_1, d]$ and $[n, k_2, d]$ classical linear codes such that $C_2 \subset C_1$. The quantum code $\mathrm{CSS}\,(C_1, C_2)$ is defined as,

$$\mathrm{CSS}\,(C_1, C_2) := \mathsf{span} \left\{ |a\rangle_{C_1/C_2} \mid a \in C_1/C_2 \right\}. \tag{42}$$

■

Lemma 5.13: Let C_1 and C_2 be $[n, k_1, d]$ and $[n, k_2, d]$ classical linear codes such that $C_2 \subset C_1$. The dimension of the vector space $\mathrm{CSS}\,(C_1, C_2)$ is $2^{k_1 - k_2}$.

□

5.7.2 Error Correction in CSS Codes

Theorem 5.13: Let C_1 and C_2 be $[n, k_1, d]$ and $[n, k_2, d]$ classical linear codes such that $C_2 \subset C_1$. Let t be a non-negative integer such that $d \geq 2t + 1$. Any subset of $[X]_n^{\leq t} \cup [Z]_n^{\leq t}$, that is any noise consisting merely of bit-flip errors on upto t qubits or phase-flip errors on upto t qubits is correctable in $\mathrm{CSS}\,(C_1, C_2)$.

□

5.8 Several Examples of Stabilizer Codes

5.8.1 Three-Qubit Bit and Phase Flip, and Shor Codes

Theorem 5.14: The three-qubit bit-flip code $\mathcal{C}_{3B}$ is stabilized by the group $\{I, Z_1Z_2, Z_2Z_3, Z_1Z_3\}$ and $\{Z_1Z_2, Z_2Z_3\}$ is an independent generator of this group.

□

Theorem 5.15: The three-qubit phase-flip code $\mathcal{C}_{3Ph}$ is stabilized by the group $\{I, X_1X_2, X_2X_3, X_1X_3\}$ and $\{X_1X_2, X_2X_3\}$ is an independent generator of this group.

□

Theorem 5.16: The nine-qubit Shor code $\mathcal{C}_{9Sh}$ is stabilized by the group generated by the following set of independent elements of the Pauli group of the Hilbert space $\mathcal{H}^{\otimes 9}$.

$$\{Z_1Z_2, Z_2Z_3, Z_4Z_5, Z_5Z_6, Z_7Z_8, Z_8Z_9, X_1X_2X_3X_4X_5X_6, X_4X_5X_6X_7X_8X_9\}$$

□

5.8.2 The Five-Qubit Code

Definition 5.27: The five-qubit code C_5 is defined to be the linear subspace of $\mathcal{H}^{\otimes 5}$ stabilized by the group $\langle X\otimes Z\otimes Z\otimes X\otimes I, I\otimes X\otimes Z\otimes Z\otimes X, X\otimes I\otimes X\otimes Z\otimes Z, Z\otimes X\otimes I\otimes X\otimes Z\rangle$.

■

Lemma 5.14: $C_5 = \mathsf{span}\left\{|\mathbf{0}\rangle_5, |\mathbf{1}\rangle_5\right\}$, where,

$$\begin{aligned}|\mathbf{0}\rangle_5 :=& \frac{1}{4}\big(\,|00000\rangle + |10010\rangle + |10100\rangle \\ &- |11011\rangle - |00110\rangle - |11000\rangle \\ &- |11101\rangle - |00011\rangle - |11110\rangle \\ &- |01111\rangle - |10001\rangle - |01100\rangle \\ &- |10111\rangle + |00101\rangle + |01010\rangle + |01001\rangle\big)\,, \end{aligned} \tag{43}$$

and,

$$\begin{aligned}|\mathbf{1}\rangle_5 :=& \frac{1}{4}\,(\,|11111\rangle + |01101\rangle + |10110\rangle \\ &+ |01011\rangle - |00100\rangle - |11001\rangle \\ &- |00111\rangle - |00010\rangle - |00001\rangle \\ &- |10000\rangle - |11100\rangle - |10011\rangle \\ &- |01000\rangle - |01110\rangle + |10101\rangle + |11010\rangle)\,. \end{aligned} \tag{44}$$

□

Theorem 5.17: Similar to Shor code, any noise consisting of single-qubit errors is correctable in the five-qubit code.

□

Chapter 6

A GENERALIZATION OF QUANTUM NON-LOCAL GAMES

6.1 A Brief Overview of Quantum Non-Local Games

Fix a Hilbert space $\mathcal{H} \cong \mathbb{C}^d$ for some positive integer d.

Definition 6.1: *Let n be a positive integer, $\{Q_k\}_k$ a collection of finite sets indexed by $\{0, \cdots, n-1\}$, and let $\alpha_k := |Q_k|$ for each k. For each $k \in \mathbb{Z}_n = \{0, \cdots, n-1\}$ let $\mathcal{M}^{(k)} = \left\{M_1^{(k)}. \cdots, M_{\alpha_k}^{(k)}\right\}$ be a set of (local) POVM measurements in the Hilbert space $\mathcal{H}^{\otimes n}$, so that each $M_j^{(k)}$ is a measurement acting effectively on the j-th location in the n-fold tensor product of the Hilbert space $\mathcal{H}$, with the set of results R_{kj}. Let $\pi : \prod_{k=0}^{n-1} Q_k \to [0,\, 1]$ be a probability distribution, and let $V : \prod_{k=0}^{n-1} Q_k \times \prod_{k=0}^{n-1} \bigcup_{j=1}^{\alpha_k} R_{kj} \to \{0,1\}$ be a predicate function. Let $|\Psi\rangle \in \mathcal{H}^{\otimes n}$. The tuple $\mathcal{G} = \left(|\Psi\rangle, \{Q_k\}_k, \left\{\mathcal{M}^{(k)}\right\}_k, \pi, V\right)$ is called a "quantum non-local game".*

For each $k \in \mathbb{Z}_n$ let $f_k : Q_k \to \mathcal{M}^{(k)}$ be a function. The tuple $S := (\mathcal{G}, f_0, \cdots, f_{n-1})$ is called an "n-player quantum strategy for the quantum game $\mathcal{G}$".

■

We now describe the practical interpretation of a quantum strategy as defined above. There assumed to be two types of agents involved in the game. There is a referee provided with the collection of finite sets $\{Q_k\}_k$ and the probability distribution $\pi : \prod_{k=0}^{n-1} Q_k \to [0,\, 1]$, alongside with the predicate function $V : \prod_{k=0}^{n-1} Q_k \times \prod_{k=0}^{n-1} \bigcup_{j=1}^{\alpha_k} R_{kj} \to \{0,1\}$. In addition, there are n players labeled by the elements of $\mathbb{Z}_n$. For each k, the k-th player is provided merely by the set of measurements $\mathcal{M}^{(k)}$.

For each k, the set Q_k is considered to be the set of possible questions that the referee can send to the k-th player. On the other hand $\bigcup_{j=1}^{\alpha_k} R_{kj}$ is considered to be the set of

possible answers by which the k-th player can respond to the question sent by the referee. The referee randomly chooses a tuple of questions $(q_0, \cdots, q_{n-1}) \in \prod_{k=0}^{n-1} Q_k$ with respect to the probability distribution π, and sends q_k to the k-th player. Followingly, the k-th player has to respond to the question of the referee with one answer among the set of possible answers $\bigcup_{j=1}^{\alpha_k} R_{kj}$.

Prior to the start of the game, all players are assumed to be provided with a shared state $|\Psi\rangle \in \mathcal{H}^{\otimes n}$. A quantum strategy consists of choices of functions $f_0, \ldots, f_{n-1}$ which determines the nature of the response of players to the questions they receive; upon receiving the question q_k, the k-th player performs the measurement $f_k(q_k)$ on the shared quantum state $|\Psi\rangle$ and sends the observed outcome r_k back to the referee. Note that according to the probabilistic nature of quantum measurements, the response of players are not deterministic in general. Ultimately, the referee calls the predicate function V to infer the value $V(q_0, \cdots, q_{n-1}, r_1, \cdots, r_{n=1})$, and accepts if this value is 1 and rejects otherwise. If the referee accepts, then the players are said to win the game.

The players aim at agreeing upon a prior strategy that maximizes the likelihood of winning the game.

6.2 Multi-Layer Quantum Non-Local Games

The notions of quantum non-local games and strategies as introduced in the previous section can be generalized by taking into account an arbitrary number of teams of players which do not play simultaneously, but instead successively with different shared states generally. So the teams are labeled by an ordered finite set $\{0, \cdots, N-1\}$ with the standard ordering $0 < \cdots < N-1$. In addition, in this generalized form the existence of a tuple $\mathcal{U} := (U_1, \cdots, U_{N-1})$ of unitary operations in $L(\mathcal{H}^{\otimes n})$ is assumed. Also we relax the constraint of the equality of the number of players of teams to the number n, so that the number of players of each team can be any number in $\{1, \cdots, n\}$. Furthermore, the location in the n-fold tensor product of $\mathcal{H}$ accessible to each player of each team is assumed to be specified prior to the start of the game.

In the generalized form, the referee is provided tuples of questions for each team, alongside with corresponded probability distributions. More precisely, for each $l \in \mathbb{Z}_N$, let η_l be the number of players of the l-th team whose player are labeled by the set $\mathbb{Z}_{\eta_l}$. The referee is assumed to be provided with the collection of question-sets $\bigcup_{l=0}^{N-1} \left\{Q_k^l\right\}_{k=1}^{\eta_l}$, where Q_k^l is considered to be the set of possible questions that can be sent only to the player number k of the team number l. Let $\alpha_{l,k} := \left|Q_k^l\right|$. The referee is also assumed to be provided with probability distributions $\pi^l : \prod_{k=1}^{\eta_l} Q_k^l \to [0,\, 1]$. The referee sends randomly each player of each team a question according to the probability distributions π^l-s.

Furthermore the player number k of the team number l is assumed to have access to the set of measurements $\mathcal{M}_k^l = \left\{M_1^{(l,k)}.\cdots, M_{\alpha_{l,k}}^{(l,k)}\right\}$ with $R_{l,k,j}$ being the set of all outcomes of the measurement $M_1^{(l,k)}$. Moreover, the team number 0 is considered to be the first team to start the game whose players share an initial state $|\Psi_0\rangle$ in the Hilbert space $\mathcal{H}^{\otimes n}$. In addition, the referee is assumed to have access to a predicate function $V : \prod_{l=0}^{N-1}\prod_{k=1}^{\eta_l} Q_k^l \times \prod_{l=1}^{N}\prod_{k=1}^{\eta_l}\bigcup_{j=1}^{\alpha_{l,k}} R_{l,k,j} \to \{0,1\}$.

The players of each team are supposed to adopt a mapping the set of possible questions to the set of available measurements. That is, the k-th player of the l-th team is assumed to be equipped with a function $f_k^l : Q_k^l \to \mathcal{M}_k^l$. At the first step, the game is played by the team number 0 exactly in the same way as described in the previous section. Upon receiving a random tuple of questions $\left(q_1^0, \cdots, q_{\eta_0}^0\right)$ the k-th player of the team number 0 performs the measurement $f_k^0\left(q_k^0\right)$ on the state $|\Psi_0\rangle$ and obtains the result r_k^0 and sends it back to the referee.

The measurements of the players of the team number 0 alter the state $|\Psi_0\rangle$, and in accordance with the observed outcomes $\left(r_1^0, \cdots, r_{\eta_0}^0\right)$ the state $|\Psi_0\rangle$ collapses to a state $|\Psi'_0\rangle$. Note that similar to the observed outcomes, the state to which the initial state collapses after the measurements of the 0-th team, is not determined with certainty prior to the initiation of the game by this team, because of the probabilistic nature of quantum measurements.

After the termination of the first round of the game by team number 0, the second round takes place by players of the team number 1. Again at this round everything

is similar to the single-team case with the shared state now being $U_1 |\Psi'_0\rangle$, an the players of this team act by performing their measurements according to the strategy they adopt and the received questions.

In general, the game play flows successively through the teams completely similar to what is described for the case of the transfer of it from team 0 to the team 1. Since there are in general an arbitrary number of teams involved in the game that cannot play simultaneously, we will refer to this form of generalizing the notion of quantum non-local games as "multi-layer quantum non-local games", since each team is conceived of playing at a certain layer of the game. A precise algorithmic description of such a game can be stated inductively as follows.

Definition 6.2: *The tuple* $\mathcal{G} = \left(|\Psi_0\rangle, \bigcup_{l=0}^{N-1} \left\{ Q_k^l \right\}_{k=1}^{\eta_l}, \bigcup_{l=0}^{N-1} \left\{ \mathcal{M}^{(l,k)} \right\}_{k=1}^{\eta_l}, \left(\pi^0, \cdots, \pi^l\right), V, \mathcal{U} \right)$ *is called a "multi-layer quantum non-local game".*

For each $l \in \mathbb{Z}_n$ *and* $k \in \{1, \cdots, \eta_l\}$ *let* $f_k^l : Q_k^l \to \mathcal{M}^{(l,k)}$ *be a function.*

The tuple $\mathcal{S} := \left(\mathcal{G}, f_1^0, \cdots, f_{\eta_0}^0, \cdots, f_1^{N-1}, \cdots, f_{\eta_{N-1}}^{N-1} \right)$ *is called an "*l*-team (*l*-layer) quantum strategy for the quantum game* $\mathcal{G}$*".*

The strategy $\mathcal{S}$ *is played in practice according to the following algorithm.*

For every $l \in \mathbb{Z}_N$*, let the shared state of the team number* l*, when the game play is passed to its players, be denoted by* $\left|\Psi^{(l)}\right\rangle$*, and let* $\left|\Psi'^{(l)}\right\rangle$ *denote the state to which* $\left|\Psi^{(l)}\right\rangle$ *collapses after the termination of* l*-th team playing.*

- *Fix* $\left|\Psi^{(0)}\right\rangle$ *be an initially given state* $|\Psi_0\rangle$*.*
- *For every* $l \in \{1, \cdots, N-1\}$*, let* $\left|\Psi^{(l)}\right\rangle = U_l \left|\Psi'^{(l-1)}\right\rangle$*.*
- *The referee sends questions* $\left(q_1^l, \cdots, q_{\eta_l}^l\right)$ *to the players of teams according to the probability distribution* π^l*, for every* $l \in \mathbb{Z}_N$*.*
- *The players of the* l*-th team respond to the questions they received when their round starts, by performing the measurements according to their adopted strategies, that is the measurements* $\left\{ f_k^l \left(q_k^l\right) \right\}_{k=1}^{\eta_l}$ *and sending back the referee the tuple of observed outcomes* $\left(r_1^l, \cdots, r_{\eta_l}^l\right)$*.*

- *The referee calls the predicate function V after receiving all the answers from the players of all teams to obtain the value* $V\left(q^0, 1, \cdots, q^0_{\eta_0}, \cdots, q^l, 1, \cdots, q^l_{\eta_l}, r^0, 1, \cdots, r^0_{\eta_0}, \cdots, r^l, 1, \cdots, r^l_{\eta_l}\right)$*, accepts if this value is* 1 *and rejects otherwise.*

■

Chapter 7

QUANTUM LINEARITY TESTING OF BOOLEAN FUNCTIONS

7.1 Background

7.1.1 Algebraic Property Testing

Given a pair of non-empty finite sets X and Y, we denote by $\mathsf{F}(X, Y)$ the set of all functions from X to Y. A property $\mathcal{P}$ in the class of functions $\mathsf{F}(X, Y)$ is defined to be a subset of $\mathsf{F}(X, Y)$, and for any $f \in \mathcal{P}$ it is said that "f satisfies the property $\mathcal{P}$ in the class of functions $\mathsf{F}(X, Y)$". The task of determining whether an arbitrary function f satisfies the property $\mathcal{P}$ or not is generally referred to as a "function property testing" problem. Moreover, if the class of functions $\mathsf{F}(X, Y)$ is provided with a metric $\mathrm{d} : \mathsf{F}(\mathrm{X}, \mathrm{Y}) \times \mathsf{F}(\mathrm{X}, \mathrm{Y}) \to [0, 1]$, a measure of distance from $\mathcal{P}$ can be defined for each $f \in \mathsf{F}(X, Y)$, accordingly. This can be defined as the map $dist_{\mathcal{P}} : \mathsf{F}(X, Y) \to \mathbb{R}^{+}$ such that,

$$\forall\, f \in \mathsf{F}(X, Y) \colon\ dist_{\mathcal{P}}\,(f) \stackrel{\text{def}}{=} \inf\{\mathrm{d}\,(\mathrm{f}, \mathrm{g}) \mid \mathrm{g} \in \mathcal{P}\}\,. \tag{1}$$

Then a function $f \in \mathsf{F}(X, Y)$ is said to be "ε-far from $\mathcal{P}$ relative to the metric d" if $\mathrm{dist}_{\mathcal{P}}\,(f) > \varepsilon$, and "$\varepsilon$-close to $\mathcal{P}$ relative to the metric d" if $\mathrm{dist}_{\mathcal{P}}\,(f) \leq \varepsilon$.

Taken to consider the property-testing problem, in general, as a computational task, any function $f \in \mathsf{F}(X, Y)$ can be considered as a computational agent (which is also called the oracle f) that generates the value $f\,(x)$ at the output when receives an arbitrary $x \in X$. The act of extracting an output from this agent upon calling it by an arbitrary input is generally referred to as a "query to the agent (or simply the function) f". A computationl algorithm $\mathbf{T}$ that decides whether an arbitrary function $f \in \mathsf{F}(X, Y)$ belongs to $\mathcal{P}$ or not, by a number of queries to f is generally called a "function property tester". Typically, function property testers that have

been developed in various areas are not completely deterministic in the sense of rejecting (or accepting) an arbitrary $f \in \mathsf{F}(X, Y)$ with certainty when $f \notin \mathcal{P}$ (or $f \in \mathcal{P}$). So, inherently their decision is probabilistic. But the problem is that not every algorithm with any probability of rejecting (or accepting) an arbitrary function f makes sense as a reliable decision task. Hence the following definition is agreed upon in the literature.

Definition 7.1: An algorithm $\mathbf{T}$ is called a "$\mathcal{P}$-tester in $\mathsf{F}(X, Y)$" if there exist maps $q : (0,1) \to \mathbb{Z}^+$ and $\delta : (0,1) \to (0,1)$ such that given a function $f \in \mathsf{F}(X, Y)$ which is ε-far from $\mathcal{P}$, $\mathbf{T}$ accepsts f with certainty if $f \in \mathcal{P}$ and rejects it with probability at least $\delta(\varepsilon)$ by making at most $q(\varepsilon)$ queries to the oracle f.

■

Furthermore, the property $\mathcal{P}$ is said to be a "testable property in $\mathsf{F}(X, Y)$" if there exists a $\mathcal{P}$-tester in $\mathsf{F}(X, Y)$.

When the sets X and Y are equipped with some algebraic structures, then a property $\mathcal{P}$ may be defined based on an algebraic feature of functions in $\mathsf{F}(X, Y)$, and thereby is taken to be equal to the set of all functions possessing this the desired feature. For example, if X and Y are assumed to be endowed with linear stuctures that make them as vector spaces, then the set of all linear function from X to Y is actually a property in $\mathsf{F}(X, Y)$, and any tester for this property is called a "linearity-test". Generally, the task of such function property testing problems where the property under consideration is defined via some algebraic structures on X and Y, go under the name of "algebraic property testing". In the following subsection we review the linearity test and affine-linearity test in a particular case.

7.1.2 Linearity Test

Let $\mathbb{F}_2$ denote the binary field $\{0, 1\}$ of characteristic 2 (endowed with its usual addition and multiplication operations modulo 2), and let n be an arbitrary integer. Let $\mathcal{L}(\mathbb{F}_2^n, \mathbb{F}_2)$ denote the set of all linear maps from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, and hence a property $\mathcal{P}$ of functiopns from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. In this particular case we pose a metric on the set

of all functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, as

$$\forall\ (x,\, y) \in \mathsf{F}(\mathbb{F}_2^n,\, \mathbb{F}_2) \times \mathsf{F}(\mathbb{F}_2^n,\, \mathbb{F}_2)\colon\ \mathrm{d}\,(\mathrm{f}, \mathrm{g}) \stackrel{\mathrm{def}}{=} \frac{1}{2^{\mathrm{n}}} |\{\mathrm{x} \in \mathbb{F}_2^{\mathrm{n}} \mid \mathrm{f}\,(\mathrm{x}) \neq \mathrm{g}\,(\mathrm{x})\}|, \quad (2)$$

based on which arbitrary functions are provided with a measure of distance from $\mathcal{L}\,(\mathbb{F}_2^n, \mathbb{F}_2)$, as described above.

There is a famous linearity tester in this case, called the "BLR-linearity test", which is defined as follows [19].

Definition 7.2: The BLR-linearity-test is defined to be the following algorithm.

1. Select each x and y in $\mathbb{F}_2^n$ randomly with uniform probability.

2. Query the oracle f three times to obtain $f\,(x)$, $f\,(y)$, and $f\,(x+y)$.

3. Accept if $f\,(x+y) = f\,(x) + f\,(y)$, and reject otherwise.

■

The above algorithm is actually a linearity tester based on the above definition, according to a theorem which we just state without giving the proof.

Theorem 7.1: Let f be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ with distance ε from $\mathcal{L}\,(\mathbb{F}_2^n, \mathbb{F}_2)$. The BLR-linearity-test accepts f with certainty if $\varepsilon = 0$, and rejects it with a probability in $[\varepsilon,\, 5\varepsilon]$.

□

The proof of this theorems that validate the BLR linearity test, rely on the results of the theory of classical Fourier analysis.

7.1.3 Affine Linearity Test

Let $\mathbb{F}_2$ denote the binary field $\{0, 1\}$ of characteristic 2 (endowed with its usual addition and multiplication operations modulo 2), and let n be an arbitrary integer. Let $\mathcal{AL}\,(\mathbb{F}_2^n, \mathbb{F}_2)$ denote the set of all affine linear maps from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, and hence a property $\mathcal{P}$ of functiopns from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. We recall that a function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is called an "affine linear map" if

$$\forall\, x, y, z \in \mathbb{F}_2^n\colon\ f\,(x+y+z) = f\,(x) + f\,(y) + f\,(z)\,, \quad (3)$$

or equivalently

$$\forall\, x, y \in \mathbb{F}_2^n \colon\ f(x+y) = f(0) + f(x) + f(y)\,. \tag{4}$$

There is a famous affine linearity tester in this case, called the "BLR-affine-linearity test", which is defined as follows [19].

Definition 7.3: The BLR-linearity-test is defined to be the following algorithm.

1. Select each x, y, and z in $\mathbb{F}_2^n$ randomly with uniform probability.

2. Query the oracle f four times to obtain $f(x)$, $f(y)$, $f(z)$, and $f(x+y)$.

3. Accept if $f(x+y+z) = f(x) + f(y) + f(z)$, and reject otherwise.

■

This test can be equivalently stated as the following.

Proposition 7.1: The BLR-linearity-test is equivalent to the following algorithm.

1. Select each x, y in $\mathbb{F}_2^n$ randomly with uniform probability.

2. Query the oracle f three times to obtain $f(x)$, $f(y)$, and $f(x+y)$.

3. Accept if $f(x+y) = f(0) + f(x) + f(y)$, and reject otherwise.

□

This algorithm works with a reject probability as follows.

Theorem 7.2: Let f be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ with distance ε from $\mathcal{AL}(\mathbb{F}_2^n, \mathbb{F}_2)$. The BLR-affine-linearity-test accepts f with certainty if $\varepsilon = 0$, and rejects it with a probability in $[\varepsilon,\, 6\varepsilon]$.

□

The proof of this theorems that validate the BLR linearity test, rely on the results of the theory of classical Fourier analysis.

7.2 Implementin Boolean Functions with Quantum Gates

Let n be a positive integer, and let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function. The quantum counterpart of f is defined to be the unitary operator $U_f \in \mathrm{U}\left(\mathcal{H}^{\otimes n}\right)$ such that

$$\forall\, x \in \mathbb{F}_2^n \colon\ U_f \left|x\right\rangle = (-1)^{f(x)} \left|x\right\rangle . \tag{5}$$

The construction of the U_f gate can be achieved by implementing the gate $\tilde{U}_f \in \mathrm{U}\left(\mathcal{H}^{\otimes n+1}\right)$ defined as

$$\forall\, x \in \mathbb{F}_2^n \colon\ \forall\, y \in \mathbb{F}_2 \colon\ \tilde{U}_f \left|x\right\rangle \otimes \left|y\right\rangle := \left|x\right\rangle \otimes \left|x \oplus f\left(y\right)\right\rangle , \tag{6}$$

where $\oplus$ denotes the addition mod 2. Considering that,

$$\tilde{U}_f \left|x\right\rangle \otimes \left|-\right\rangle = (-1)^{f(x)} \left|x\right\rangle \otimes \left|-\right\rangle , \tag{7}$$

where by definition,

$$\left|-\right\rangle := \frac{1}{\sqrt{2}} \left(\left|0\right\rangle - \left|1\right\rangle\right), \tag{8}$$

by setting the second single-qubit register to $\left|-\right\rangle$ and discard it in the output, it is possible then to implement U_f.

7.3 A Quantum-Circuit-Based Algorithm for Linearity Testing

Let n be a positive integer, and let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function. Define the unitary gate D_f as

$$H^{\otimes n} U_f H^{\otimes n}, \tag{9}$$

and define,

$$\left|\Psi\right\rangle := D_f \left|0\right\rangle^{\otimes n} . \tag{10}$$

For every $x \in \mathbb{F}_2^n$ define the Boolean function $g_x : \mathbb{F}_2^n \to \mathbb{F}_2$ as,

$$\forall\, y \in \mathbb{F}_2^n \colon\ g_x\left(y\right) \stackrel{\mathrm{def}}{=} 1 \oplus \delta_{x,y}. \tag{11}$$

Let $\mathcal{M}$ denote the measurement in computational-basis, that is $\{|x\rangle\langle x| \mid x \in \mathbb{F}_2^n\}$. For every $x \in \mathbb{F}_2^n$ define the unitary gate G_x as,

$$\begin{aligned} G_x &:= (2|\Psi\rangle\langle\Psi| - I_n) U_{g_x} \\ &= D_f \left[(2|\psi\rangle\langle\psi| - I_n)\right] D_f U_{g_x}, \end{aligned} \tag{12}$$

where $|\psi\rangle$ is the equally-weighted superposition of computational-basis states,

$$|\psi\rangle := \frac{1}{2^n} \sum_{x \in \mathbb{F}_2^n} |x\rangle . \tag{13}$$

It can be easily verified that [3],

$$(2|\psi\rangle\langle\psi| - I_n) = H^{\otimes n} (2|0\rangle\langle 0| - I_n) H^{\otimes n}, \tag{14}$$

and that $2|0\rangle\langle 0| - I_n$ is the unitary operator such that $|x\rangle \mapsto -(-1)^{\delta_{x,0}} |x\rangle$. Therefore G_x is efficiently implementable.

For every Boolean function $g : \mathbb{F}_2^n \to \mathbb{F}_2$, let $S_g := g^{-1}(1)$, and define,

$$\begin{aligned} |X_g\rangle &:= \frac{1}{\sqrt{\sum_{x \in S_g} |\langle x|\Psi\rangle|^2}} \left[\sum_{x \in S_g} |x\rangle\langle x|\right] |\Psi\rangle , \\ |Y_g\rangle &:= \frac{1}{\sqrt{\sum_{x \in \mathbb{F}_2^n \setminus S_g} |\langle x|\Psi\rangle|^2}} \left[\sum_{x \in \mathbb{F}_2^n \setminus S_g} |x\rangle\langle x|\right] |\Psi\rangle , \end{aligned} \tag{15}$$

and,

$$\begin{aligned} u_g &:= \sqrt{\sum_{x \in S_g} |\langle x|\Psi\rangle|^2}, \\ v_g &:= \sqrt{\sum_{x \in \mathbb{F}_2^n \setminus S_g} |\langle x|\Psi\rangle|^2}. \end{aligned} \tag{16}$$

Then,

$$|\Psi\rangle = u_g |X_g\rangle + v_g |Y_g\rangle . \tag{17}$$

By defining

$$\begin{aligned} u_g &=: \sin\theta_g, \\ v_g &=: \cos\theta_g, \end{aligned} \tag{18}$$

it is straightforward to verify the following proposition.

Proposition 7.2: For every positive integer r, and for every $x \in \mathbb{F}_2^n$,

$$G_x^r \left|\Psi\right\rangle = \sin\left[(2r+1)\,\theta_{g_x}\right] \left|X_{g_x}\right\rangle + \cos\left[(2r+1)\,\theta_{g_x}\right] \left|Y_{g_x}\right\rangle . \tag{19}$$

□

Definition 7.4: For every $x \in \mathbb{F}_2^n$, let t_x be the positive integer such that $r = t_x$ minimizes $\left|(2r+1)\,\theta_{g_x} - \frac{\pi}{2}\right|$ among all integer values r.

■

Now we consider the following quantum algorith that attempts to decide wether a given Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is linear or not.

Algorithm 7.1:

1. Measure $\left|\Psi\right\rangle$ by $\mathcal{M}$ and denote by $x \in \mathbb{F}_2^n$ the observed outcome.
2. Get the state $\left|\Phi_x\right\rangle := G_x^{t_x} \left|\Psi\right\rangle$.
3. Measure $\left|\Phi_x\right\rangle$ by $\mathcal{M}$ and denote by $y \in \mathbb{F}_2^n$ the observed outcome.
4. Accept if $y = x$, and reject otherwise.

■

As what is shown in [18], if a given Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is ϵ-far from the set of all linear functions with $0 < \epsilon < \frac{1}{2}$, then [algorithm 7.1] rejects with a probability greater than $\frac{2}{3}$, that is with probability $\mathcal{O}(1)$. On the other hand, the query complexity of [algorithm 7.1] is the number of iterations of aunitary gate G_x for some $x \in \mathbb{F}_2^n$, that is the number t_x. oreover, according to [definition 7.4] it is not difficult to show that $t_x = \mathcal{O}\left(\frac{1}{\sqrt{\epsilon}}\right)$.
So, this quantum algorithm is superior to the famous classical (BLR) linearity testing which requires a query complexity $\mathcal{O}\left(\frac{1}{\epsilon}\right)$ to reject a Boolen function ϵ-far from the set of linear functions with probability $\mathcal{O}(1)$ [19].

7.4 Representing Boolean Functions by Measurements

Let $\mathbb{F}_2$ denote the finite field with two elements $\{0, 1\}$, with 0 and 1 as its neutral additive and multiplicative elements, respectively. Let n be a positive integer, $\mathcal{F}_n$ denote the set of all functions $f : \mathbb{F}_2^n \to \mathbb{F}_2$, which are called Boolean functions. Let $\mathcal{H}_2$ denote the Hilbert space of a single qubit system. For every non-negative integers m and l, we will denote by $\mathcal{BM}^1[l,\, m]$ the set of all projective measurements M with two outcomes on the Hilbert space $\mathcal{H}_2^{\otimes l} \otimes \mathcal{H}_2^{\otimes m}$ such that $M = \{P_0 \otimes I_m, P_1 \otimes I_m\}$, where I_m denotes the identity operator on $\mathcal{H}_2^{\otimes m}$ and P_0 and P_1 are projections in $\mathcal{H}_2^{\otimes l}$ with $P_0P_1 = P_1P_0 = 0$ and $P_0 + P_1 = I_l$. Similarly, we will denote by $\mathcal{BM}^2[l,\, m]$ the set of all projective measurements M with two outcomes on the Hilbert space $\mathcal{H}_2^{\otimes l} \otimes \mathcal{H}_2^{\otimes m}$ such that $M = \{I_l \otimes P_0, I_l \otimes P_1\}$, where P_0 and P_1 are projections in $\mathcal{H}_2^{\otimes m}$ with $P_0P_1 = P_1P_0 = 0$ and $P_0 + P_1 = I_m$. We will also simply denote by $\mathcal{BM}_l$ the set $\mathcal{BM}^1[l,\, 0] = \mathcal{BM}^2[0,\, l]$. We will refer to elements of $\mathcal{BM}^1[l,\, m]$ or $\mathcal{BM}^2[m,\, l]$ as binary projecive measurements. For a fixed l, we consider the measurements $\{P_0 \otimes I_m, P_1 \otimes I_m\} \in \mathcal{BM}^1[l,\, m]$, $\{I_l \otimes P_0, I_l \otimes P_1\} \in \mathcal{BM}^2[m,\, l]$, and $\{P_0, P_1\} \in \mathcal{BM}_l$ to be equivalent. Thus $\mathcal{BM}^1[l,\, m]$, $\mathcal{BM}^2[m,\, l]$, and $\mathcal{BM}_l$ are canonically identified for all m.

Let $\{|0\rangle, |1\rangle\}$ be the standard orthonormal basis of $\mathcal{H}_2$. Then consequently the set of states $\{|k_1\rangle \otimes \cdots \otimes |k_n\rangle \mid k_1, \cdots, k_n \in \{0, 1\}\}$ is an orthonormal basis of $\mathcal{H}_2^{\otimes n}$ which is considered to be its standard basis. We will simply denote by $|k_1, \cdots, k_n\rangle$ the basis element $|k_1\rangle \otimes \cdots \otimes |k_n\rangle$. Based on the choice of the standard basis for $\mathcal{H}_2^{\otimes n}$, there is a natural correspondence between the set of all Boolean functions, $\mathcal{F}_n$, and the set of all binary projective measurements, $\mathcal{BM}_n$, by associating a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ with the binary projective measurement $M_f = \{P_0, P_1\}$, where,

$$P_0 := \sum_{k \in f^{-1}(0)} |k\rangle\langle k|, \tag{20}$$

$$P_1 := \sum_{k \in f^{-1}(1)} |k\rangle\langle k|. \tag{21}$$

So binary projective measurements can be considered as representations of Boolean functions. We define two measurements on $\mathcal{H}_2^{\otimes n} \otimes \mathcal{H}_2^{\otimes n}$ equivalent to M_f as,

$$M_f^1 := \{P_0 \otimes I_n, P_1 \otimes I_n\}, \tag{22}$$

$$M_f^2 := \{I_n \otimes P_0, I_n \otimes P_1\}. \tag{23}$$

7.5 Linearity Testing via Quantum Measurements

Let $f \in \mathcal{F}_n$, and suppose that initially a quantum system with Hilbert space $\mathcal{H}_2^{\otimes n} \otimes \mathcal{H}_2^{\otimes n}$ is prepared in the state

$$\left|\Psi^0\right\rangle := \frac{1}{2^n} \sum_{j \in \mathbb{F}_2^n} \sum_{k \in \mathbb{F}_2^n} |j\rangle \otimes |k\rangle. \tag{24}$$

Now suppose that the quantum system initially prepared in the state Ψ_0 goes under two successive measurements M_f^1 and M_f^2. Let us first consider the outcome of the measurement M_f^1 on Ψ_0. If the result 0 is observed the state of the system will change to the state

$$\left|\Psi_0^1\right\rangle := P_0 \otimes I_n \left|\Psi_0\right\rangle = \frac{1}{2^n} \left(\sum_{j \in f^{-1}(0)} |j\rangle \right) \otimes \left(\sum_{k \in \mathbb{F}_2^n} |k\rangle \right), \tag{25}$$

and if the result 1 is observed the state of the system will change to the state

$$\left|\Psi_1^1\right\rangle := P_1 \otimes I_n \left|\Psi_0\right\rangle = \frac{1}{2^n} \left(\sum_{j \in f^{-1}(1)} |j\rangle \right) \otimes \left(\sum_{k \in \mathbb{F}_2^n} |k\rangle \right). \tag{26}$$

The probability of observing the results 0 and 1 are

$$\mathcal{P}^1(0) = \langle \Psi_0 | P_0 \otimes I_n | \Psi_0 \rangle = \frac{|f^{-1}(0)|}{2^n}, \tag{27}$$

$$\mathcal{P}^1(1) = \langle \Psi_0 | P_1 \otimes I_n | \Psi_0 \rangle = \frac{|f^{-1}(1)|}{2^n}. \tag{28}$$

Now suppose that after the collapse of the state $|\Psi_0\rangle$ to one of the states $\mathcal{P}_0^1$ or $\mathcal{P}_1^1$, following the measurement M_f^1, the quantum system is measured by the measurement M_f^2. Then there are four possibilities for the state of the system following the second measurement, corresponded to the four possible ordered pair of results of

these two successive measurements, that is (0, 0), (0, 1), (1, 0), (1, 1). We denote these states by $\left|\Psi^2_{0,0}\right\rangle$, $\left|\Psi^2_{0,1}\right\rangle$, $\left|\Psi^2_{1,0}\right\rangle$, $\left|\Psi^2_{1,1}\right\rangle$, respectively. Clearly,

$$\left|\Psi^2_{r,s}\right\rangle = I_n \otimes P_s \left|\Psi^1_r\right\rangle = \frac{1}{2^n}\left(\sum_{j\in f^{-1}(r)} |j\rangle\right) \otimes \left(\sum_{k\in f^{-1}(s)} |k\rangle\right), \quad r,s \in \{0,1\}. \tag{29}$$

We denote by $\mathcal{P}^2(s|r)$ the probability of observing the outcome s for the measurement M^2_f conditioned on observing the outcome r for the measurement M^1_f, for $r, s = 0, 1$. Clearly,

$$\mathcal{P}^2(s|r) = \left\langle \Psi^1_r \right| I_n \otimes P_s \left| \Psi^1_r \right\rangle = \frac{|f^{-1}(s)|}{2^n}, \quad r,s = 0,1. \tag{30}$$

So denoting by $\mathcal{P}(r, s)$ the probability of the occurrence of the result $(r,\ s)$ for this pair of successive measurements, we have,

$$\mathcal{P}(r,s) = \mathcal{P}^2(s|r)\mathcal{P}^1(r) = \frac{|f^{-1}(s)|}{2^n}\frac{|f^{-1}(r)|}{2^n}, \quad r,s = 0,1. \tag{31}$$

So after performing M^1_f and M^2_f successively on the state $|\Psi_0\rangle$, the state of the quantum system collapses to one of the states $\left|\Psi^2_{r,s}\right\rangle$ with the the probability $\mathcal{P}(r, s)$. At this stage suppose that the attained state $\left|\Psi^2_{r,s}\right\rangle$ goes under the measurement $M_{2n} = \{|j\rangle\langle j| \otimes |k\rangle\langle k| \ \mid j,k \in \mathbb{F}_2^{2n}\}$ of the computational basis of the Hilbert-space $\mathcal{H}_2^{\otimes n} \otimes \mathcal{H}_2^{\otimes n}$. Let $\mathcal{P}(j,k|r,s)$ denote the probability of observing the outcome jk for the measurement M_{2n} conditioned on observing the outcome (r, s) for the pair of successive measurements (M^1_f, M^2_f) performed on the initial state $|\Psi_0\rangle$. It can be easily seen that,

$$\forall\, j,k \in \mathbb{F}_2^n\colon\ \mathcal{P}(j,k|r,s) = \frac{1}{|f^{-1}(r)|}\frac{1}{|f^{-1}(s)|}, \quad r,s \in \{0,1\}. \tag{32}$$

So starting with the state $|\Psi_0\rangle$ and following the three successive measurements performed on the quantum system, the final state of the system at the output of these measurements can be any of the states $|j\rangle \otimes |k\rangle$ of the computational basis of $\mathcal{H}_2^{\otimes n} \otimes \mathcal{H}_2^{\otimes n}$. Given $j, k \in \mathbb{F}_2^n$, the probability that this process collapses the initial state $|\Psi_0\rangle$ to the state $|j\rangle \otimes |k\rangle$ is,

$$\mathcal{P}_{jk} = \mathcal{P}(j,k|r,s)\mathcal{P}(r,s) = \frac{1}{2^{2n}}. \tag{33}$$

So it can be equivalently stated that this process chooses a pair of elements of the computational basis $\{|k\rangle \mid k \in \mathbb{F}_2^n\}$ of $\mathcal{H}_2^{\otimes n}$ independently and each with respect to the uniform probability.

Now assume that another set of n registers (qubit spaces) is added to the previous quantum system (or it is safe to assume that they were present from the first, playing no role until this stage) to form a system with the Hilbert space $\mathcal{H}_2^{\otimes n} \otimes \mathcal{H}_2^{\otimes n} \otimes \mathcal{H}_2^{\otimes n}$. Furthermore, assume that the final set of n-registers is initialized to the state $|\mathbf{0}\rangle$, where $\mathbf{0}$ denotes the neutral additive element of $\mathbb{F}_2^n$. So at this stage the state of the quantum system is $|j\rangle \otimes |k\rangle \otimes |\mathbf{0}\rangle$ for some $j, k \in \mathbb{F}_2^n$. Now suppose that the quantum modulo-2 addition operation $\tilde{\oplus} : \mathcal{H}_2^{\otimes 3n} \to \mathcal{H}_2^{\otimes 3n}$ is acted on the current state $|j\rangle \otimes |k\rangle \otimes |\mathbf{0}\rangle$ whose output is,

$$|\Phi\rangle := \tilde{\oplus}\,|j\rangle \otimes |k\rangle \otimes |\mathbf{0}\rangle = |j\rangle \otimes |k\rangle \otimes |j \oplus k\rangle\,, \tag{34}$$

where $\oplus$ denotes the addition operation of the vector space $\mathbb{F}_2^n$.

Finally suppose that the state $|\Phi\rangle$ is measured by the measurement $M_f^3 := \{I_n \otimes I_n \otimes P_0, I_n \otimes I_n \otimes$

It is trivial that the result of this measurement determines the value $f(j \oplus k)$ with absolute certainty. In other words the result of this measurement must be $f(j \oplus k)$ with probability 1.

Now we propose an algorithm named **QBLR**.

The **QBLR** Algorithm:

1. Prepare the initial state $|\Psi_0\rangle \in \mathcal{H}_2^{\otimes n} \otimes \mathcal{H}_2^{\otimes n}$.

2. Put $|\Psi_0\rangle$ into the process of successive measurements M_f^1, M_f^2, M_{2n}, and record the results of the measurements M_f^1 and M_f^2, denoted by R_1 an R_2, respectively.

3. Add a further collection of n-registers to the system at the output of stage 2 and initialize this collection of added registers to $|\mathbf{0}\rangle$.

4. Act the quantum modulo-2 addition operation on the state achieved in stage 3.

5. Measure the output of the state of the stage 4 by the measurement M_f^3 and record the result of this measurement denoted by R_3.

6. Accept if $R_3 = R_1 \oplus R_2$, an reject otherwise.

The proof of the following proposition is trivial according to what has been discussed before the statement of the algorithm.

Proposition 7.3: The **QBLR** algorithm selects a pair of states $|j\rangle$ and $|k\rangle$ among the computational basis of $\mathcal{H}_2^{\otimes n}$ independently and each with the uniform probability. $R_1 = f(j)$, $R_2 = f(k)$, and $R_3 = f(j \oplus k)$. The algorithm accepts if $f(j \oplus k) = f(j) + f(k)$, and rejects otherwise.

□

The proposition above shows that this quantum algorithm is equivalent to the classical BLR test, and hence has the same success probability in deciding the linearity of a given Boolean function as that of the BLR test. But the point of introducing this method is not quantum advantage, but an example which fits into the generalized framework for quantum non-local games that we introduced in the previous chapter, alongside with the introduction of implementing Boolean functions by quantum measurements rather than quantum gates.

Chapter 8

CLASSICAL LOW-DEGREE TESTING

8.1 Boolean Polynomials

We will denote by $\mathbb{F}_2$ *the finite field of order* 2*, that is* $\mathbb{F}_2 := \{0, 1\}$ *endowed with the addition and multiplication operations modulo* 2*. Given a set* X*, we will denote by* $\mathcal{P}(X)$ *the set of all subsets of* X*. For any positive integer* n*, we will denote by* $[n]$ *the set* $\{1, \cdots, n\}$*.*

Definition 8.1: Let n be a positive integer. We will denote by $\mathbf{F}_n$ the set of all functions $f : \mathbb{F}_2^n \to \mathbb{F}_2$. Any element of $\mathbf{F}_n$ is called a "Boolean function (in n variates)". Given a Boolean function $f \in \mathbf{F}_n$, we simply write $f = 0$ if for every $x \in \mathbb{F}_2^n$, $f(x) = 0$.
The map $\mathrm{d}_n : \mathbf{F}_n \times \mathbf{F}_n \to \mathbb{Z}^{\geq 0}$ is defined as,

$$\forall\, (f, g) \in \mathbf{F}_n \times \mathbf{F}_n \colon\ \mathrm{d}_n(f, g) \stackrel{\text{def}}{=} \frac{1}{2^n} |\{x \in \mathbb{F}_2^n \mid f(x) \neq g(x)\}|. \tag{1}$$

The map $\mathrm{D}_n : \mathbf{F}_n \times (\mathcal{P}(\mathbf{F}_n) \setminus \{\emptyset\}) \to \mathbb{Z}^{\geq 0}$ is defined as,

$$\forall\, f \in \mathbf{F}_n \colon\ \forall\, A \in \mathcal{P}(\mathbf{F}_n) \setminus \{\emptyset\} \colon\ \mathrm{D}_n(f, A) \stackrel{\text{def}}{=} \min\{\mathrm{d}_n(f, g) \mid g \in A\}. \tag{2}$$

$\mathrm{d}_n(f, g)$ is called the "distance of the Boolean functions f and g", and $\mathrm{D}_n(f, A)$ is called the "distance of f from A".

■

Definition 8.2: Let n be a positive integer, let $f \in \mathbf{F}_n$ and $y \in \mathbb{F}_2^n$. The "directional derivative of f in direction y", is defined as the Boolean function $\mathcal{D}_y(f) : \mathbb{F}_2^n \to \mathbb{F}_2$ such that,

$$\forall\, x \in \mathbb{F}_2^n \colon\ [\mathcal{D}_y(f)](x) := f(x + y) + f(x). \tag{3}$$

■

Definition 8.3: Let n be a positive integer, let $f \in \mathbf{F}_n$ and $y_1, \cdots, y_m \in \mathbb{F}_2^n$ for some positive integer m. We define,

$$\mathcal{D}_{y_1,\cdots,y_m}(f) := \mathcal{D}_{y_1}\left(\mathcal{D}_{y_2}\left(\cdots \mathcal{D}_{y_d}(f)\right)\right). \tag{4}$$

■

Proposition 8.1: Let n be a positive integer, let $f \in \mathbf{F}_n$ and $y_1, \cdots, y_m \in \mathbb{F}_2^n$ for some positive integer m.

$$\forall\, x \in \mathbb{F}_2^n\colon\ \left[\mathcal{D}_{y_1,\cdots,y_m}(f)\right](x) = \sum_{S\subseteq[m]} f\left(x + \sum_{j\in S} y_j\right). \tag{5}$$

□

Proposition 8.2: Let n and d be a positive integers, and let $f \in \mathbf{F}_n$. The following conditions are equivalent.

i. For every $y_1, \cdots, y_{d+1} \in \mathbb{F}_2^n$, $\mathcal{D}_{y_1,\cdots,y_{d+1}}(f) = 0$.

ii. For every $x, y_1, \cdots, y_{d+1} \in \mathbb{F}_2^n$,

$$\sum_{S\subseteq[d+1]} f\left(x + \sum_{j\in S} y_j\right) = 0. \tag{6}$$

iii. There exists a map $a : \mathcal{P}([n]) \to \mathbb{F}_2$ such that for every $x \in \mathbb{F}_2^n$,

$$f(x) = \sum_{\{S\in\mathcal{P}([n])\ |\ |S|\leq d\}} a(S) \prod_{j\in S} x_j. \tag{7}$$

□

Definition 8.4: Let n and d be positive integers. A Boolean function $f \in \mathbf{F}_n$ is called a "Boolean polynomial (in n variates) of degree at most d" if it satisfies any, and hence all, of he conditions stated in [proposition 8.2]. The set of all Boolean polynomials in n variates of degree at most d will be denoted by $\mathbf{P}_d^{(n)}$.

■

Proposition 8.3: Let n and d be positive integers. For every $f \in \mathbf{P}_{d+1}^{(n)}$ and every $y \in \mathbb{F}_2^n$, $\mathcal{D}_y(f) \in \mathbf{P}_d^{(n)}$.

□

8.2 Low-Degree Polynomial Testing

Algorithm 8.1: Let n and d be positive integers. The following algorithm is famous for the $\mathrm{AKKLR}_n(d)$-test.

1. Choose $x, y_1, \cdots, y_{d+1}$ independently and each with respect to the uniform probability on $\mathbb{F}_2^n$.
2. For every $S \in \mathcal{P}([d+1])$, query $f\left(x + \sum_{j \in S} y_j\right)$.
3. If $\sum_{S \subseteq [m]} f\left(x + \sum_{j \in S} y_j\right) = 0$ then accept, otherwise reject.

■

Algorithm 8.2: Let n and d be positive integers with $d < n$. The following algorithm is famous for the $d+1-\mathrm{flat}-\mathrm{test}_n$.

1. Choose randomly a $d+1$-dimensional affine subspace A of $\mathbb{F}_2^n$.
2. Query $f|_A$.
3. If $\sum_{x \in A} f(x) = 0$, that is if $f|_A$ is a degree d polynomial, then accept, otherwise reject.

■

Lemma 8.1: Let n and d be positive integers with $d < n$. Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a boolean function. Let $P_r^{\mathrm{flat}(d+1,n)}(f)$ denote the probability that the $d+1-$

$\text{flat}-\text{test}_n$-test rejects f.

$$P_r^{\text{flat}(d+1,n)}(f) \geq 2^{d+1}\mathrm{D}_n\left(f, \mathbf{P}_d^{(n)}\right)\left[1 - 2^{d+1}\mathrm{D}_n\left(f, \mathbf{P}_d^{(n)}\right)\right]. \tag{8}$$

proof : Obviously, there exists $h \in \mathbf{P}_d^{(n)}$ such that $\mathrm{d}_n(f,h) = \mathrm{D}_n\left(f, \mathbf{P}_d^{(n)}\right)$, that is,

$$\frac{1}{2^n}|\{x \in \mathbb{F}_2^n \mid f(x) \neq h(x)\}| = \mathrm{D}_n\left(f, \mathbf{P}_d^{(n)}\right). \tag{9}$$

Now let $g : \mathbb{F}_2^n \to \mathbb{F}_2$ such that $g := h+1$, that is for every $x \in \mathbb{F}_2^n$, $g(x) = h(x)+1$. Then according to [definition 8.4], it is trivial that $g \in \mathbf{P}_d^{(n)}$. In addition, it is clear that,

$$\begin{aligned}\Pr(f(x) = g(x)) &= \frac{1}{2^n}|\{x \in \mathbb{F}_2^n \mid f(x) = g(x)\}| \\ &= \frac{1}{2^n}|\{x \in \mathbb{F}_2^n \mid f(x) \neq h(x)\}| = \mathrm{D}_n\left(f, \mathbf{P}_d^{(n)}\right).\end{aligned} \tag{10}$$

Let A be a random affine subspace of $\mathbb{F}_2^n$ generated by choosing a random $x \in \mathbb{F}_2^n$ and a random full-rank $n \times (d+1)$ matrix over $\mathbb{F}_2$, and then constructing A as $A := x + M\mathbb{F}_2^{d+1}$, that is,

$$A = \left\{x + My \mid y \in \mathbb{F}_2^{d+1}\right\}. \tag{11}$$

For any $a \in \mathbb{F}_2^{d+1}$, let $\mathbf{E}_a$ denote the event that $f(x+Ma) \neq g(x+Ma)$, and $\mathbf{F}_a$ denote the event that $f(x+Ma) \neq g(x+Ma)$ and for every $b \in \mathbb{F}_2^{d+1} \setminus \{a\}$, $f(x+Mb) = g(x+Mb)$. Note that for any $a \in \mathbb{F}_2^{d+1}$, the sample spaces of the events $\mathbf{E}_a$ and $\mathbf{F}_a$ are subsets of the set of all orderd pairs (x, M) with $x \in \mathbb{F}_2^n$ and M a full-rank $n \times (d+1)$ matrix over $\mathbb{F}_2$.

For any $a \in \mathbb{F}_2^{d+1}$, if $(x, M) \in \mathbf{F}_a$, then considering that $\sum_{y\in A} g(x) = 0$ and $f(a) \neq g(a)$,

$$\begin{aligned}\sum_{y\in A} f(x) &= \sum_{y\in A\setminus\{a\}} f(x) + f(a) \\ &= \sum_{y\in A\setminus\{a\}} g(x) + f(a) \\ &= f(a) = g(a) = 1,\end{aligned} \tag{12}$$

and hence $d+1-\text{flat}-\text{test}_n$ rejects f. Therefore,

$$P_r^{\text{flat}(d+1,n)}(f) \geq \Pr\left(\bigcup_{a\in\mathbb{F}_2^{d+1}} \mathbf{F}_a\right). \tag{13}$$

On the other hand, it is obvious that for any pair a, a' of distinct vectors in $\mathbb{F}_2^{d+1}$, $\mathbf{F}_a \cap \mathbf{F}_{a'} = \emptyset$, and hence,

$$\Pr\left(\bigcup_{a\in\mathbb{F}_2^{d+1}} \mathbf{F}_a\right) = \sum_{a\in\mathbb{F}_2^{d+1}} \Pr\left(\mathbf{F}_a\right). \tag{14}$$

Therefore,

$$P_r^{\text{flat}(d+1,n)}(f) \geq \sum_{a\in\mathbb{F}_2^{d+1}} \Pr\left(\mathbf{F}_a\right). \tag{15}$$

On the other hand, for any $a \in \mathbb{F}_2^{d+1}$, clearly,

$$\Pr\left(\mathbf{F}_a\right) \geq \Pr\left(\mathbf{E}_a\right) - \sum_{b\in\mathbb{F}_2^n\setminus\{a\}} \Pr\left(\mathbf{E}_a \cap \mathbf{E}_b\right), \tag{16}$$

and for every $a, b \in \mathbb{F}_2^{d+1}$ such that $a \neq b$,

$$\Pr\left(\mathbf{E}_a \cap \mathbf{E}_b\right) = \Pr\left(\mathbf{E}_a\right)\Pr\left(\mathbf{E}_b\right). \tag{17}$$

□

The following theorem can be proved using the lemma above.

Theorem 8.1: Let d be a positive integer in $\{1, \cdots, n\}$, and let f be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ with distance ε from $\mathbf{P}_d^{(n)}$. AKKLR(d)-test accepts f with certainty if $\varepsilon = 0$, and rejects it with probability at least $c \cdot \min\left\{2^d\epsilon, 1\right\}$ for some absolute positive constant c. [21]

□

8.3 Non-Classical Polynomials and Gowers Norms

Given an Abelian group G and a function $f : G \to \mathbb{C}$, for every $y \in G$, the function $\Delta_y f : G \to \mathbb{C}$ is defined as,

$$\forall\, x \in G\colon\ \left[\Delta_y f\right](x) \stackrel{\text{def}}{=} f\left(x+y\right)\overline{f\left(x\right)}, \tag{18}$$

where $\overline{z}$ denotes the complex-conjugate of $z \in \mathbb{C}$. $\Delta_y f$ is called the "directional derivative of f relative to y".

Definition 8.5: Let G be a finite Abelian group, and let d be a positive integer. For any function $f : G \to \mathbb{C}$, the "Gowers norm of degree d of f", denoted by $|f|_{U^d}$, is defined as [22],

$$\|f\|_{U^d} := \left| \frac{1}{|G|} \left[\sum_{y_1 \in G} \cdots \sum_{y_d \in G} \sum_{x \in G} \left[\Delta_{y_1}, \ldots, \Delta_{y_d} f\right](x) \right] \right|^{\left(\frac{1}{2}\right)^d}. \tag{19}$$

■

When $d = 1$, the Gowers norm is a semi-norm on the vector space of all functions from G to $\mathbb{C}$, but when $d > 1$, the Gowers norm is actually a norm on $\mathsf{F}(G, \mathbb{C})$.
Until now we have taken into account the set of functions $\mathsf{F}(\mathbb{F}_2^n, \mathbb{F}_2)$ (for some positive integer n) to define polynomials. We remind that in the most general case of a finite field $\mathbb{F}_2$, the order of $\mathbb{F}$, that is the number of its elements, equals p^k for a unique choice of prime and positive integers p and k. The charcteristic of a finite field $\mathbb{F}_2$ of order p^k is p, which means the smallest integer m such that $\underbrace{1 + \cdots + 1}_{m} = 0$, equals p (where 1 and 0 denote the multiplicative and additive neutral elements of $\mathbb{F}$). Moreover, $\mathbb{F}$ is called a prime finite field if its order equals a prime number p, in which case we denote it specifically by $\mathbb{F}_p$. We can extend the notion of directional derivatives to the set of functions $\mathsf{F}\big(\mathbb{F}_p^n, G\big)$ for an arbitrary prime number p and an arbitrary positive number n, and a finite Abelian group G. That is, for any function f from $\mathbb{F}_p^n$ to G and any $y \in \mathbb{F}_p^n$, the function $\mathcal{D}_y f : \mathbb{F}_p^n \to G$ is defined as,

$$\forall\, x \in \mathbb{F}_p^n\colon\ \left[\mathcal{D}_y f\right](x) \stackrel{\text{def}}{=} f(x + y) - f(x)\,. \tag{20}$$

Base on this notion of directional derivative, the class of polynomials of degree at most d (for some positive integer d) is defined in the class of functions $\mathsf{F}\big(\mathbb{F}_p^n, G\big)$.

Definition 8.6: A function $P : \mathbb{F}_p^n \to G$ is called a "polynomialf of degree at most d" if for every $y_1, \ldots, y_{d+1}, x \in \mathbb{F}_p^n$,

$$\left[\mathcal{D}_{y_1, \ldots, y_{d+1}} f\right](x) = 0. \tag{21}$$

the class of all polynomials of degree at most d in the class of functions $\mathsf{F}\left(\mathbb{F}_p^n,\, G\right)$ will be denoted by $\mathcal{P}_d\left(\mathbb{F}_p^n, G\right)$. When $\mathbb{F}_p^n$ and the Abelian group G are clearly identified, then simply the class of all polynomials of degree at most d will be denoted by $\mathcal{P}_d$.

■

In the particular case when the Abelian group under consideration is the one-dimensional torus $\mathbb{T}^1 = \mathbb{R}/\mathbb{Z}$, any polynomial in $\mathsf{F}\left(\mathbb{F}_p^n,\, \mathbb{R}/\mathbb{Z}\right)$ is called a "non-classical polynomial".

There is a canonical bijection between $\mathbb{R}/\mathbb{Z}$ and the one-dimensional sphere $S^1 \subseteq \mathbb{C}$, that is a function $\mathbf{e} : \mathbb{R}/\mathbb{Z} \to \mathbb{C}$ as the following. For every $x \in \mathbb{R}/\mathbb{Z}$, choose a representative of $x \in \mathbb{R}$ like x_0, and define,

$$\mathbf{e}\left(x\right) := \exp\left(2\pi i x_0\right). \tag{22}$$

Since the value of $\exp\left(2\pi i x_0\right)$ is independent of the choice of a representative for x, the function $\mathbf{e}$ is well-defined, and $\exp\left(2\pi i x_0\right)$ can be denoted by $\exp\left(2\pi i x\right)$ without causing any confusion. In addition, there is a canonical one-to-one function $\vartheta : \mathbb{F}_p \to \mathbb{C}$ defined as follows. For each $x \in \mathbb{Z}/p\mathbb{Z}$ choose a representative $x_0 \in \mathbb{Z}$, and define,

$$\vartheta\left(x\right) := \exp\left(\frac{2\pi i x_0}{p}\right). \tag{23}$$

Again since the value of $\exp\left(\frac{2\pi i x_0}{p}\right)$ is independent of the choice of a representative for x in $\mathbb{Z}$, the function ϑ is well-defined, and $\exp\left(\frac{2\pi i x_0}{p}\right)$ can be denoted by $\exp\left(\frac{2\pi i x}{p}\right)$ without causing any confusion.

We now define the notion of the standard inner-product on the space of all functions $\mathsf{F}\left(\mathcal{F}_p^n,\, \mathbb{C}\right)$. The inner-product of any pair of functions f and g from $\mathbb{F}_p^n$ to $\mathbb{C}$ is defined to be,

$$\langle f, g\rangle := \frac{1}{p^n} \sum_{x \in \mathbb{F}_p^n} f\left(x\right) \overline{g\left(x\right)}. \tag{24}$$

For any positive integer d, the Gowers uniformity norm of f indicates the extent to which f is correlated to the polynomial phase functions for polynomials of degree at most d. The rigorous description of such correlations are stated in the following theorems which are famous for "direct theorems for Gowers norms".

Theorem 8.2: Let $f \in \mathsf{F}\left(\mathbb{F}_p^n, \mathbb{F}_p\right)$, and let d be a positive integer. For every $P \in \mathcal{P}_d$, that is every polynomial P of degree at most d,

$$|\langle f, \vartheta(P)| \leq \|f\|_{U^{d+1}}. \tag{25}$$

□

Theorem 8.3: Let $f \in \mathsf{F}\left(\mathbb{F}_p^n, \mathbb{C}\right)$, and let d be a positive integer. For every $P \in \mathcal{P}_d$, that is every polynomial P of degree at most d,

$$|\langle f, \mathbf{e}(P)\rangle| \leq \|f\|_{U^{d+1}}. \tag{26}$$

□

The actual usefulness of Gowers uniformity norms in distinguishing polynomials relies on the famous "inverse theorems for Gowers norms" which are stated below.

Theorem 8.4: Let $f \in \mathsf{F}\left(\mathbb{F}_p^n, \mathbb{F}_p\right)$, and let ε be a positive real number.

- If $\|\vartheta(f)\|_{U^2} \geq \varepsilon$, then there exists a polynomial $P : \mathbb{F}_p^n \to \mathbb{F}_p$ of degree 1 such that $|\langle f, \mathbf{e}(P)\rangle| \geq \varepsilon^2$.
- If $\|\vartheta(f)\|_{U^3} \geq \varepsilon$, then there exists a polynomial $P : \mathbb{F}_p^n \to \mathbb{F}_p$ of degree 2 such that $|\langle f, \mathbf{e}(P)\rangle| \geq \delta(p, \varepsilon)$ for some function δ.

□

Theorem 8.5: There exists a map $\delta = \delta(p, d, \varepsilon)$ such that for every function $f : \mathbb{F}_p^n \to \mathbb{C}$ with $\|f\|_{U^{d+1}} \geq \varepsilon$, there exists a non-classical polynomial $P : \mathbb{F}_p^n \to \mathbb{R}/\mathbb{Z}$ of degree at most d that satisfies

$$|\langle f, \mathbf{e}(P)\rangle| \geq \delta(p, d, \varepsilon). \tag{27}$$

□

The statement of the inverse theorem for Gowers norm in the case of non-classical polynomials ncessitates the existence of a function δ without providing further information about any bounds or restrictions on all possible such functions. This fact

impedes the direct usability of the inverse theorem for detecting low-degree polynomial patterns in functions computationally. So any investigation for finding such further information may be crucial for the sake of constructing relevant computational algorithms of low-degree polynomial recognition.

8.4 Directions for Future Research

According to the Gowers inverse theorems, the evaluation of Gowers uniformity norm of degree $d+1$ of a Boolean function is an indicator of the extent of correlatedness of the function with a degree at most d Boolean polynomial. Therefore the construction of fast quantum algorithms to evaluate the Gowers uniformity norms of degree greater than 2 of Boolean functions [24] is capable of opening the way for fast low-degree testing, superior to the classical test.

BIBLIOGRAPHY

[1] A. Yu. Kitaev, A. H. Shen, M. N. Vyalyi, "Classical and Quantum Computation"; 2002, American Mathematical Society

[2] Scott Aaronson, Daniel Gottesman, "Improved Simulation of Stabilizer Circuits", arXiv:quant-ph/0406196

[3] M. A. Nielsen, I. L. Chuang, "Quantum Computation and Quantum Information", 10th Anniversary Edition; 2010, Cambridge University Press

[4] Frank Gaitan, "Quantum Error Correction and Fault Tolerant Quantum Computing"; 2008, CRC Press

[5] Rahul Sarka, Ewout van den Berg, "On sets of commuting and anticommuting Paulis"; arXiv:1909.08123 [quant-ph]

[6] Sergey Bravyi, Alexei Kitaev, "Universal quantum computation with ideal Clifford gates and noisy ancillas"; arXiv:quant-ph/0403025

[7] A. R. Calderbank, E. M Rains, P. W. Shor, N. J. A. Sloane, "Quantum Error Correction via Codes over $GF(4)$"; arXiv:quant-ph/9608006

[8] Daniel Gottesman, "An Introduction to Quantum Error Correction and Fault-Tolerant Quantum Computation"; arXiv:0904.2557 [quant-ph]

[9] Daniel Gottesman, "Stabilizer Codes and Quantum Error Correction"; arXiv:quant-ph/9705052

[10] Daniel Gottesman, "A Class of Quantum Error-Correcting Codes Saturating the Quantum Hamming Bound"; arXiv:quant-ph/9604038

[11] Daniel Gottesman, "The Heisenberg Representation of Quantum Computers"; arXiv:quant-ph/9807006

[12] Daniel Gottesman, "A Theory of Fault-Tolerant Quantum Computation"; arXiv:quant-ph/9702029

[13] Rahul Sarka, Ewout van den Berg, "On sets of commuting and anticommuting Paulis"; arXiv:1909.08123 [quant-ph]

[14] H. Hatami, Isac P. Hatami, S. Lovett, "Higher-order Fourier Analysis and Applications"

[15] J. H. van Lint, "Introduction to Coding Theory", Third Edition; Springer, 1999

[16] C. M. Dawson, M. A. Nielsen, "The Solovay-Kitaev Algorithm"; arXiv:quant-ph/0505030

[17] Adam Bouland, Tudor Giurgica-Tiron, "Efficient Universal Quantum Compilation: An Inverse-free Solovay-Kitaev Algorithm"; arXiv:2112.02040 [quant-ph]

[18] Kaushik Chakraborty, Subhamoy Maitra, "Improved quantum test for linearity of a Boolean function"; arXiv:1306.6195 [quant-ph]

[19] M. Blum, M. Luby, and R. Rubinfeld, "Self-testing/correcting with applications to numerical problems", 1993 In: Proceedings of the 22nd Annual ACM Symposium on Theory of Computing (Bal- timore, MD, 1990). Vol. 47 (3). 549595. doi: 10.1016/0022- 0000(93)90044-W. bibitemHatami Hamed Hatami, Pooya Hatami, Shachar Lovett, "Higher-order Fourier Analysis and Applications"

[20] Noga Alon, Tali Kaufman, Michael Krivelevich, Simon Litsyn, and Dana Ron. Testing Reed-Muller codes. IEEE Trans. Inform. Theory, 51(11):40324039, 2005.

[21] Bhattacharyya, A., S. Kopparty, G. Schoenebeck, M. Sudan, and D. Zuckerman (2010b). Optimal testing of Reed-Muller codes. In: 2010 IEEE 51st Annual

Symposium on Foundations of Computer Science FOCS 2010. IEEE Computer Soc., Los Alamitos, CA. 488497.

[22] W. T. Gowers. A new proof of Szemerédis theorem. Geom. Funct. Anal., 11(3):465588, 2001.

[23] Mark Hillery, and Erika Andersson, "Quantum tests for the linearity and permutation invariance of Boolean function"; arXiv1106.4831v2

[24] C. A. Jothishwaran, Anton Tkachenko, Sugata Gangopadhyay, Constanza Riera, Pantelimon Stanica, "A quantum algorithm to estimate the Gowers U_2 norm and linearity testing of Boolean functions"; arXiv 2006.16523v1