OPTIMALITY IN STABILIZER TESTING

MSc Thesis *(Afstudeerscriptie)*

written by

Raja Oktovin Parhasian Damanik
(born October 6th, 1992 in Medan, Indonesia)

under the supervision of **Dr Michael Walter**, and submitted to the Board of Examiners in partial fulfillment of the requirements for the degree of

MSc in Logic

at the *Universiteit van Amsterdam.*

Date of the public defense:
July 9th, 2018

Members of the Thesis Committee:
Dr Maris Ozols
Dr Christian Schaffner
Dr Michael Walter
Prof Dr Ronald de Wolf (Chair)

INSTITUTE FOR LOGIC, LANGUAGE AND COMPUTATION

Abstract

Stabilizer states are important in quantum information, computation, and error correction. Stabilizer tester is a quantum algorithm that, given an access to several copies a quantum state, tests whether the state is a stabilizer state or far from it. It was an open question whether it is possible to obtain a stabilizer testing algorithm that is efficient and whose power is independent of the number of qubits. The question was answered in [GNW17] which provides a test that is perfectly complete, transversal, and independent of the number of qubits and only requires 6 copies of the state.

This thesis is about optimizing stabilizer testing. There are two main results in this thesis. The first is about stabilizer testing with few copies. We attempt to answer whether there exists a stabilizer testing algorithm that is perfectly complete and independent of the number of qubits given less than 6 copies of the state. We prove a no-go theorem for 4 copies; that it is not possible if the algorithm only has access to 4 copies. The second main result is about stabilizer testing with many copies. One run of the 6-copy stabilizer testing algorithm can give a type-II error with high probability. One can reduce the error by just repeating the 6-copy algorithm many times. We attempt to investigate whether there exists a protocol that is more efficient than the one that just repeats the 6-copy algorithm many times. The answer is affirmative.

Contents

Chapter 1

Introduction

1.1 Motivation

Stabilizer states are quantum states that are useful in measurement based quantum computation [RBB03], quantum error correction [Got97], and many other areas in quantum information. Stabilizer states, even though can be produced by relatively simple quantum operation, can be very highly entangled. Entanglement is one of the sources of difficulty in processing quantum mechanical systems using classical computer since the classical description of the state of the quantum objects grows exponentially in terms of the number of qubits. Hence, it might be also hard to learn whether a state is a stabilizer state classically. On the other hand, stabilizer states are the states that can be produced by a class of quantum circuit called stabilizer circuit. This quantum circuit can be simulated efficiently using classical computer [AG04].

It is known that, given an access to copies of an unknown stabilizer state $|\psi\rangle$ of n qubits, $|\psi\rangle$ can be identified with $O(n)$ copies [AG08]. By identifying, we mean knowing which stabilizer state $|\psi\rangle$ is. Also, from an information theoretic argument, at least $\Omega(n)$ copies are required [Hol73]. It was an open question whether there exists a stabilizer testing whose parameters do not depend on the number of qubits n [MdW16]. By testing, we mean knowing whether a state $|\psi\rangle$ of n qubits is a stabilizer state or far from any of them.

It is proved later that there exists a stabilizer testing algorithm whose error is independent of the number of qubits which require 6 copies of the state [GNW17]. The algorithm uses a very simple quantum algorithm, namely Bell sampling, that is used in quantum teleportation.

In this thesis, we are interested in studying the optimality of the algorithm in [GNW17] and how to do stabilizer testing optimally with more copies. We are interested to find out whether 6 copies are indeed optimal in a sense that there exists no stabilizer testing algorithm that is independent of the number of qubits which only uses less than 6 copies of the state that we are testing. Moreover, the stabilizer testing algorithm in [GNW17] has perfect completeness but can make type-II error with high probability. To reduce the error, we can design a protocol that repeats the 6-copy algorithm. Such protocol will require $6m$ copies where m is the number of repetitions. It was not known whether there is a better protocol for stabilizer testing in terms of the number of copies that is used to reach desirable accuracy and we want to investigate this.

1.2 Main contributions

There are two main contributions of this thesis.

The first contribution is showing that 5 copies are necessary to have a dimension independent stabilizer testing algorithm. It is known that 6 copies are sufficient [GNW17] for a dimension independent stabilizer testing. Of course, there is a gap, but the proof strategy that we explain might be useful to close this gap. The key idea of the result is to do analysis on average case and relate it to the concept of quantum t-design. More precisely, if random t copies of stabilizer states are close a quantum t-design, then the stabilizer testing algorithm satisfying such desired property cannot exist.

The second contribution is an analysis of some protocols that, given access to many copies of the state, can be used to further reduce the error probability of stabilizer testing. A natural protocol for this is an independent and identical repetition of the 6-copy algorithm from [GNW17]. We investigate whether there exists a better protocol to reduce the error than this protocol. We study some protocols that use same primitives as the 6-copy algorithm, namely Bell sampling and Weyl measurements. The answer is affirmative. Aside from that, our analysis gives an insight to how the 6-copy algorithm actually works – we show that one should invest more copies on Bell samplings to obtain better confidence on the stabilizer testing result.

1.3 Organization of the thesis

Chapter 2 contains some preliminaries about some notions and facts that are relevant to the thesis. If there is an argument regarding the mathematics that is not clear in the content, we should look at this chapter.

Chapter 3 is about stabilizer testing with 6 copies in [GNW17]. We will briefly analyze the algorithm and discuss some of its properties. In the last section, we give some alternative proof to the lemmas and theorems used in the analysis. The technique that we use in the new proof can be used to analyze protocols for stabilizer testing in Chapter 5 later.

Chapter 4 contains one of our main mathematical results, namely the no-go theorem for 4 copies. We will formalize what we mean by no-go theorem for dimension independent stabilizer testing with perfect completeness here. Throughout the chapter we will develop some useful lemmas, such as a lemma about the probability that a random pure quantum state is in the neighborhood of a set of quantum states with respect to trace distance, lemma about quantum t-design and its relation to our no-go theorem, and finally some techniques in representation theory to show that show that random 4-copies of stabilizer states is close to a quantum 4-design.

Chapter 5 contains our other main results, namely about efficiency of protocols for stabilizer testing that can be used to reduce the error. Since the 6-copy algorithm makes a type-II error with high probability in a difficult case, we need to reduce the error. For example, we can use a protocol that repeats the 6-copy algorithm. We show that we can do stabilizer testing in more efficient way in this chapter.

Finally, in Chapter 6, we mention our main results and their significance and some interesting directions for further research.

Chapter 2

Preliminaries

In this section, we review briefly some notions from the quantum information formalism that are relevant to this thesis.

2.1 Quantum computation and information

We mainly follow the development of the notions in quantum computation and information from [dW18] and [Wal18].

Given a real or complex matrix

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

of size $m \times n$, we denote

$$A^\dagger = \begin{pmatrix} \overline{a_{11}} & \overline{a_{21}} & \dots & \overline{a_{m1}} \\ \overline{a_{12}} & \overline{a_{22}} & \dots & \overline{a_{m2}} \\ \vdots & \vdots & \ddots & \vdots \\ \overline{a_{1n}} & \overline{a_{2n}} & \dots & \overline{a_{mn}}. \end{pmatrix}$$

If $|u\rangle \in \mathbb{C}^d$ is written in coordinates as

$$|\phi\rangle = \begin{pmatrix} u_1 \\ u_2 \\ \dots \\ u_d \end{pmatrix},$$

we denote $\langle u| = |u\rangle^\dagger = \begin{pmatrix} \overline{u_1} & \overline{u_2} & \dots & \overline{u_d} \end{pmatrix}$. We define

$$\langle u|v\rangle = \langle u|\,|v\rangle = \sum_{i=1}^{d} \overline{u_i}\cdot v_i$$

which will be our standard inner product.

A *Hilbert space* $\mathcal{H}$ is a real or complex inner product space with norm defined by $\|u\| = \sqrt{\langle u|u\rangle}$ for every $u \in \mathcal{H}$. Every quantum mechanical system corresponds to a Hilbert space $\mathcal{H}$. In this thesis, we only finite-dimensional Hilbert space, for example $\mathcal{H} = \mathbb{C}^d$ for some positive integer $d > 1$.

A *(pure) state* of a quantum mechanical system $\mathbb{C}^d$ is a unit vector in the space $\mathbb{C}^d$.

Given two Hilbert space $\mathcal{H}_1$ and $\mathcal{H}_2$ respectively with inner product $\langle \cdot\,|\cdot\rangle_1$ and $\langle \cdot\,|\cdot\rangle_2$, we can define a new Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2$ whose elements are of the form

$$\sum_i \alpha_i \cdot u_1^i \otimes u_2^i$$

where $u_1^i \in \mathcal{H}_1$ and $u_2^i \in \mathcal{H}_2$ for every index i with inner product $\langle \cdot\,|\cdot\rangle$ is defined by

$$\langle u_1 \otimes u_2 | v_1 \otimes v_2\rangle = \langle u_1|v_1\rangle_1 \langle u_2|v_2\rangle_2$$

whenever $u_1, v_1 \in \mathcal{H}_1$ and $u_2, v_2 \in \mathcal{H}_2$. Given two quantum mechanical systems A and B, the joint quantum system for A and B is $\mathcal{H}_A \otimes \mathcal{H}_B$.

The simplest quantum mechanical system that we will use is *qubit*, which is described by two-dimensional Hilbert space $\mathcal{H} = \mathbb{C}^2$. The standard computational basis for $\mathbb{C}^2$ is denoted by

$$|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

which can be seen as the quantum analogue of classical bit 0 and 1, respectively. Some other important states of one qubit are:

$$\begin{aligned} |+\rangle &= \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \quad |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle, \\ |L\rangle &= \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle, \quad |R\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{i}{\sqrt{2}}|1\rangle. \end{aligned}$$

Together with $|0\rangle$ and $|1\rangle$, these states are exactly all the stabilizer states of one qubit.

A system of n qubits corresponds to $\mathbb{C}^2 \otimes \ldots \otimes \mathbb{C}^2 = (\mathbb{C}^2)^{\otimes n}$. A state of n qubits is a unit vector $|\phi\rangle \in (\mathbb{C}^2)^{\otimes n}$ where we use Dirac's bra-ket notation. Moreover, for n qubits, the computational basis is denoted by $|x_1 \ldots x_n\rangle := |x_1\rangle \otimes \ldots \otimes |x_n\rangle$ where $x_i \in \{0, 1\}$ for $i = 1, \ldots, n$.

Not all vectors in joint system $\mathcal{H}_A \otimes \mathcal{H}_B$ is of the form $|\phi\rangle \otimes |\psi\rangle$. Every state that is not in such tensor product form is called *entangled state*. For example, Einstein–Podolsky–Rosen (EPR) pair

$$|\Phi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

is an entangled state in $\mathbb{C}^2 \otimes \mathbb{C}^2$.

A unitary operator U is an operator that satisfies $UU^\dagger = U^\dagger U = I$. Transformation of a state $|\phi\rangle$ to another state in $\mathcal{H}$ is performed by a unitary operator U, namely $|\phi\rangle \mapsto U|\phi\rangle$.

A Hermitian operator O is an operator that satisfies $O = O^\dagger$. Every Hermitian operator O with the spectral decomposition $\sum_x xP_x$ corresponds to a *projective measurement* $\{P_x\}_x$. The probability of outcome x when we measure O on a state $|\psi\rangle$ is $\mathrm{tr}[P_x |\psi\rangle \langle\psi|]$. After the measurement, $|\psi\rangle$ collapses to

$$\frac{P_x |\psi\rangle}{\|P_x |\psi\rangle\|}.$$

More generally, if $\{Q_x\}_x$ is an operator that satisfies $Q_x \geq 0$ (positive semidefinite) and $\sum_x Q_x = I$, then $\{Q_x\}$ is called a *POVM measurement* and each Q_x is called a POVM element.

For a set of pure states $\{|\psi_i\rangle\}_i$ and probability distribution $\{p_i\}_i$, there is a *density operator* ρ for this ensemble which is a state of the form $\rho = \sum_i p_i |\psi\rangle \langle\psi|$. For pure states $|\psi\rangle$, we usually denote $|\psi\rangle \langle\psi|$ as ψ.

Trace distance between two states ρ and σ is denoted

$$T(\rho, \sigma) := \frac{1}{2}\|\rho - \sigma\|_1 = \frac{1}{2}\mathrm{tr}\left[\sqrt{(\rho - \sigma)^\dagger(\rho - \sigma)}\right].$$

Since density operators ρ and σ are Hermitian, the trace distance can be computed using formula

$$T(\rho, \sigma) = \frac{1}{2}\sum_i |\lambda_i|$$

where λ_i are eigenvalues of Hermitian matrix $\rho - \sigma$. Trace distance is a metric, namely for all density operator ρ, σ, τ: (i) $T(\rho, \sigma) \geq 0$ with equality iff $\rho = \sigma$, (ii) $T(\rho, \sigma) + T(\sigma, \tau) \geq T(\rho, \tau)$, (iii) $T(\rho, \sigma) = T(\sigma, \rho)$.

Fidelity of two pure states $|\varphi\rangle$ and $|\psi\rangle$ is given by $|\langle\varphi|\psi\rangle|^2$ and computes the how close the two states φ and ψ is. For pure states, fidelity is also related to the trace distance as follows:

$$T(\varphi, \psi) = \sqrt{1 - |\langle\phi|\psi\rangle|^2}.$$

2.2 Weyl operators

In one qubit system, the Pauli operators are unitary operators defined by

$$\sigma_{00} = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$
$$\sigma_{01} = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$
$$\sigma_{11} = Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},$$
$$\sigma_{10} = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Note that each Pauli operator P is a unitary, namely $PP^\dagger = P^\dagger P = I$, and a Hermitian, namely $P = P^\dagger$. Moreover, the Pauli operators that are not identity anti-commute, i.e. they satisfy $XY = -YX$, $YZ = -ZY$, and $ZX = -XZ$.

In an n-qubit system, for $\mathbf{x} = (\mathbf{p}, \mathbf{q}) \in \mathbb{Z}_2^n \oplus \mathbb{Z}_2^n$, a *Weyl operator* $W_{\mathbf{x}} = W_{(\mathbf{p},\mathbf{q})}$ is an operator of the form

$$W_{\mathbf{x}} = \sigma_{p_1 q_1} \otimes \cdots \otimes \sigma_{p_n q_n} \tag{2.1}$$

where $\mathbf{p} = (p_1, \ldots, p_n)$ and $\mathbf{q} = (q_1, \ldots, q_n)$ for some $p_i, q_i \in \{0, 1\}$. Since Pauli operators are Hermitian, clearly every Weyl operator is also Hermitian. It is clear that there are 4^n Weyl operators of n qubits.

We define function $\pi : \mathbb{Z}_2^n \oplus \mathbb{Z}_2^n \mapsto \mathbb{Z}_2$ as $\pi : \mathbf{x} \mapsto \mathbf{p} \cdot \mathbf{q}$ for any $\mathbf{x} = (\mathbf{p}, \mathbf{q}) \in \mathbb{Z}_2^n \oplus \mathbb{Z}_2^n$. We also define bilinear map $[\cdot\,, \cdot]$ as

$$[\mathbf{x}, \mathbf{y}] = \mathbf{p}_x \cdot \mathbf{q}_y + \mathbf{p}_y \cdot \mathbf{q}_x$$

for any $\mathbf{x} = (\mathbf{p}_x, \mathbf{q}_x)$ and $\mathbf{y} = (\mathbf{p}_y, \mathbf{q}_y)$.

We can see that for any $\mathbf{x} \in \mathbb{Z}_2^n \oplus \mathbb{Z}_2^n$,

$$\overline{W_{\mathbf{x}}} = (-1)^{\pi(\mathbf{x})} W_{\mathbf{x}}. \tag{2.2}$$

We also have that for every $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_2^n \oplus \mathbb{Z}_2^n$,

$$W_{\mathbf{x}} W_{\mathbf{y}} = (-1)^{[\mathbf{x},\mathbf{y}]} W_{\mathbf{y}} W_{\mathbf{x}}. \tag{2.3}$$

Another useful fact about Weyl operator is that the trace of any Weyl operator of n qubits must be either 0 or 2^n. The later case holds if and only if the Weyl operator is the identity operator.

The scaled Weyl operators

$$\{2^{-n/2} W_{\mathbf{x}} : \mathbf{x} \in \mathbb{Z}_2^n \oplus \mathbb{Z}_2^n\}$$

forms an orthonormal basis with respect to the Hilbert-Schmidt inner product $\langle A, B\rangle = \mathrm{tr}[A^\dagger B]$. Hence, any operator B on $(\mathbb{C}^2)^{\otimes n}$ can be written as a linear combination of the scaled Weyl operators and we denote $c_B(\mathbf{x})$ as the coefficient of $2^{-n/2} W_{\mathbf{x}}$ of this. We see that

$$c_B(\mathbf{x}) = 2^{-n/2} \mathrm{tr}[W_{\mathbf{x}} B]. \tag{2.4}$$

If B is a Hermitian operator (e.g. a pure state $B = |\psi\rangle \langle\psi| = \psi$), $c_B(\mathbf{x})$ is a real number. For any operator A and B, we also have that

$$\mathrm{tr}[A^\dagger B] = \sum_{\mathbf{x}} \overline{c_A(\mathbf{x})} c_B(\mathbf{x}) \tag{2.5}$$

If we take A and B as the pure state $|\psi\rangle \langle\psi|$, it follows that

$$p_\psi(\mathbf{x}) := c_\psi(\mathbf{x})^2 = 2^{-n} |\langle\psi|W_{\mathbf{x}}|\psi\rangle|^2 = 2^{-n} \mathrm{tr}[W_{\mathbf{x}} \psi W_{\mathbf{x}} \psi] \tag{2.6}$$

is a probability distribution over $\mathbf{x} \in \mathbb{Z}_2^n \oplus \mathbb{Z}_2^n$ since by equation 2.5, $p_\psi(\mathbf{x}) := c_\psi(\mathbf{x})^2$ sum to 1. We call this the *characteristic distribution* of $|\psi\rangle$. We do not know if this probability distribution has immediate physical interpretation, except via Theorem 3.10.

2.3 Unitary, Pauli, and Clifford group

The set of all unitary operators on $\mathbb{C}^d$ forms a group and we call it the *unitary group* and we denote it by $U(d)$.

In an n-qubit system, the *Pauli group* $\mathcal{P}_n$ is defined by,

$$\mathcal{P}_n = \{\pm 1, \pm i\} \times \{W_{\mathbf{x}} : \mathbf{x} \in \mathbb{Z}_2^n \oplus \mathbb{Z}_2^n\}.$$

In other words, it is the group that is generated by n-fold tensor products of Pauli operators of one qubit. The number of elements of the Pauli group is 4^{n+1}.

The *Clifford group* $\mathcal{C}_n$ of n qubits is a set of unitary operators U on $(\mathbb{C}^2)^{\otimes n}$ such that $UPU^\dagger \in \mathcal{P}_n$ for all $P \in \mathcal{P}_n$. Note that $\mathcal{P}_n \subseteq \mathcal{C}_n$. The number of elements of the Clifford group is

$$|\mathcal{C}_n| = 2^{n^2+2n} \prod_{i=1}^{n} (4^i - 1).$$

For the proof, we refer to [AG04]. For $n > 1$, $\mathcal{C}_n$ is generated by the following operators:

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \text{ and } \quad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

acting on arbitrary qubit or pair of qubits. For $n = 1$, CNOT gate is omitted.

2.4 Haar measure and quantum state t-design

There exists a measure $d\psi$ on the set of all pure quantum states in $\mathbb{C}^d$ that satisfies

$$\int f(|\psi\rangle\langle\psi|) d\psi = \int f(U|\psi\rangle\langle\psi| U^\dagger) d\psi$$

for all unitary $U \in U(d)$ and all integrable function f. Indeed, it can be shown that there exists a unique probability measure $d\psi$ satisfying such property. We call this measure $d\psi$ the *uniform probability measure* on the set of pure quantum states, or sometimes also called *Haar measure.*

A set of quantum states $\{|\psi_i\rangle\}_i$ in $\mathbb{C}^d$ is a *quantum state t-design* if

$$\sum_i (|\psi_i\rangle\langle\psi_i|)^{\otimes t} = \int_\psi (|\psi\rangle\langle\psi|)^{\otimes t} d\psi$$

where the integral is over the Haar measure. If a set of quantum states forms a quantum t-design, then it is difficult for a quantum computer to distinguish between the two cases whether it is given a random t copies of a state in such a set or given a random t copies of a pure quantum states. Note that the right hand side is proportional to the orthogonal projection to $\mathrm{Sym}^t(\mathbb{C}^d)$ as we will mention later in equation 2.7.

2.5 Representation theory

In Chapter 4, we will use some techniques in representation theory. Here, we briefly discuss some basic representation theory. For a more detailed explanation of some facts that we mention here, we refer to [Ser12] or [Wal18].

Let G be a group with identity element 1. A *representation* of G is a Hilbert space $\mathcal{H}$ together with a set of unitary operators $\{R_g : g \in G\}$ on $\mathcal{H}$ such that for all $g, h \in G$, $R_g R_h = R_{gh}$. It follows that R_1 is an identity on $\mathcal{H}$ and $R_{g^{-1}} = R_g^{-1}$. In this thesis, we will mainly use Hilbert space with finite dimension.

Let us study some interesting representations. Let S_n be the set of bijections $\pi : \{1, \ldots, n\} \to \{1, \ldots, n\}$. Note that for any d, the Hilbert space $(\mathbb{C}^d)^{\otimes t}$ is a representation of S_t where for each $\pi \in S_t$, we have a unitary operator R_π that permutes the tensor factor

$$R_\pi : |\phi_1\rangle \otimes \ldots \otimes |\phi_t\rangle \mapsto |\phi_{\pi^{-1}(1)}\rangle \otimes \ldots \otimes |\phi_{\pi^{-1}(t)}\rangle .$$

The Hilbert space $(\mathbb{C}^d)^{\otimes t}$ is also a representation of the unitary group $U(d)$ where for each $U \in U(d)$, we assign unitary operator R_U

$$R_U : |\phi_1\rangle \otimes \ldots \otimes |\phi_t\rangle \mapsto U |\phi_1\rangle \otimes \ldots \otimes U |\phi_t\rangle .$$

We now define *symmetric subspace* $\mathrm{Sym}^t(\mathbb{C}^d)$ of $(\mathbb{C}^d)^{\otimes t}$ as

$$\mathrm{Sym}^t(\mathbb{C}^d) = \{|\phi\rangle \in (\mathbb{C}^d)^{\otimes t} : (\forall \pi \in S_n) R_\pi |\phi\rangle = |\phi\rangle\}.$$

For a more thorough discussion about symmetric subspace and proofs of some statements below about symmetric subspace, we refer to [Har13].

The dimension of $\mathrm{Sym}^t(\mathbb{C}^d)$ is $\binom{t+d-1}{n}$ and

$$\Pi^{(t)}_{\mathrm{sym}} = \frac{1}{n!} \sum_{\pi \in S_t} R_\pi .$$

is the orthogonal projector onto $\mathrm{Sym}^t(\mathbb{C}^d)$. It is also known that

$$\int (|\psi\rangle \langle\psi|)^{\otimes t} d\psi = \binom{t+d-1}{t}^{-1} \Pi^{(t)}_{\mathrm{sym}} \tag{2.7}$$

where the integral is over the Haar measure.

Note that $\mathrm{Sym}^t(\mathbb{C}^d)$ is a representation for S_n as well as for $U(d)$. This is because for every $\pi \in S_t$ and every $U \in U(d)$, R_π and $U^{\otimes t}$ commute. Since the Clifford group $\mathcal{C}_n$ is a subgroup of unitary group $U(2^n)$, any representation of $U(2^n)$ is also representation for $\mathcal{C}_n$. In particular, $\mathrm{Sym}^t((\mathbb{C}^2)^{\otimes n})$ is also a representation for $\mathcal{C}_n$.

Given Hilbert space $\mathcal{H}$, a subspace $\mathcal{H}_1$ is called an *invariant subspace* if for every $g \in G$ and $|\psi\rangle \in \mathcal{H}_1$, we have $R_g |\psi\rangle \in \mathcal{H}_1$.

We say that $\mathcal{H}$ is an *irreducible representation* if the only invariant subspaces of $\mathcal{H}$ are $\{0\}$ and $\mathcal{H}$ itself. If $\mathcal{H}_1 \subseteq \mathcal{H}$ is a representation of G, $\mathcal{H}_2 := \mathcal{H}_1^{\perp}$ is also a representation of G. Then, we can write $\mathcal{H}$ as a decomposition of two invariant subspaces $\mathcal{H} = \mathcal{H}_1 \oplus \mathcal{H}_2$. This means that every operator R_g can be written as a block diagonal matrix

$$\begin{pmatrix} R_g^1 & 0 \\ 0 & R_g^2 \end{pmatrix}$$

where R_g^1 is the restriction of R_g in $\mathcal{H}_1$ and R_g^2 is the restriction of R_g in $\mathcal{H}_2$.

An *intertwiner* $J : \mathcal{H}_1 \to \mathcal{H}_2$ is an operator such that $JR_g^1 = R_g^2 J$ for all $g \in G$. If the intertwiner is invertible, namely

$$JR_g^1 J^{-1} = R_g^2,$$

for all $g \in G$, then the two representations are *equivalent*. If there is no such intertwiner, the two representations are *inequivalent*. If $\mathcal{H}_1 = \mathcal{H}_2$ and $R_g^1 = R_g^2$, J is called *self-intertwiner*.

Now, any finite representation $\mathcal{H}$ can be decomposed into

$$\mathcal{H} = \bigoplus_i \mathcal{H}_i \otimes \mathbb{C}^{m(i)}$$

where $\mathcal{H}_1, \ldots, \mathcal{H}_k$ correspond to irreducible representations that are pairwise inequivalent and $m(i)$ is the multiplicity of $\mathcal{H}_i$ appearing in the decomposition. *Schur's lemma* states that any self-intertwiner J of such $\mathcal{H}$ is of the form

$$J = \bigoplus_i I_{\mathcal{H}_i} \otimes M_i$$

where $I_{\mathcal{H}_i}$ is the identity on $\mathcal{H}_i$ and M_i is an operator on $\mathbb{C}^{m(i)}$.

2.6 Stabilizer states

We now review some notions about stabilizer states [Got97]. We mainly follow the development of the notions related to stabilizer states as in [GNW17].

2.6.1 Stabilizer formalism

A subset $S \subseteq \mathcal{P}_n$ is *stabilizer group* if it is a subgroup of Pauli group which does not contain $-I$. Every stabilizer group is Abelian. Note that

$$P_S = \frac{1}{|S|} \sum_{P \in S} P \tag{2.8}$$

is a projector onto a subspace that we call the *stabilizer code* V_S associated to S. The dimension of V_S will be

$$\mathrm{tr}[P_S] = \frac{1}{|S|}\sum_{P\in S}\mathrm{tr}[P] = \frac{2^n}{|S|}.$$

If $|S| = 2^n$, there will be a unique $+1$ eigenvector (up to a scalar) of all $P \in S$. We call such eigenvector of a maximal stabilizer group S a *(pure) stabilizer state* and we denote it as $|S\rangle$. The projector P_S will be the one-dimensional projector $|S\rangle\langle S|$

As an example, there are 6 stabilizer states of 1 qubits, namely $|0\rangle, |1\rangle, |+\rangle, |-\rangle, |L\rangle$, and $|R\rangle$. There are 30 stabilizer states of 2 qubits. We denote by $\mathrm{Stab}(n)$ the set of all stabilizer states of n qubits. The number of stabilizer states of n qubits is given by the formula

$$|\mathrm{Stab}(n)| = 2^n\prod_{i=1}^{n}(2^i+1). \tag{2.9}$$

For the proof, we refer to [AG04]. This fact will be useful later in Chapter 4 to show that the size of the some small neighborhood of stabilizer states with respect to the trace distance is arbitrarily small for large n.

2.6.2 Stabilizer states and Lagrangian subspaces

For any subspace $N \subseteq \mathbb{Z}_2^n \oplus \mathbb{Z}_2^n$, we denote $N^\perp = \{\mathbf{y} \in \mathbb{Z}_2^n \oplus \mathbb{Z}_2^n : (\forall\mathbf{x})[\mathbf{x},\mathbf{y}] = 0\}$ and $\dim N$ as the dimension of N. For any subspace N of $\mathbb{Z}_2^n \oplus \mathbb{Z}_2^n$, we have that $\dim N + \dim N^\perp = 2n$. We call a subspace N *isotropic* if $N \subseteq N^\perp$ and *Lagrangian* if $N = N^\perp$.

For any isotropic subspace N of $\mathbb{Z}_2^n \oplus \mathbb{Z}_2^n$, we can find a Lagrangian subspace containing it. If N is a proper subset of $N^\perp$, there exists an element $\mathbf{a}$ of $N^\perp$ that is not in N. Define another subspace N_1 that contains N as its subspace and $\mathbf{a}$ as its element. Since $[\mathbf{a},\mathbf{a}] = [\mathbf{a},\mathbf{x}] = 0$ for all $\mathbf{x} \in N$, $N_1 \subseteq N_1^\perp$.

If S is a stabilizer group, we can write

$$S = \{(-1)^{f(\mathbf{x})}W_{\mathbf{x}} : \mathbf{x} \in M\}$$

for some subset $M \subseteq \mathbb{Z}_2^n \oplus \mathbb{Z}_2^n$ and function $f : M \to \mathbb{Z}_2$. In this way, $|S\rangle$ is a $(-1)^{f(x)}$ eigenvector of $W_{\mathbf{x}}$. Moreover, if $|S| = 2^n$, M must have size 2^n. Moreover, if $\mathbf{x},\mathbf{y} \in M$, then $\mathbf{x}+\mathbf{y} \in M$ and since S is Abelian, for all $\mathbf{x},\mathbf{y} \in M$, we have $[\mathbf{x},\mathbf{y}] = 0$. Hence, M is a Lagrangian subspace of $\mathbb{Z}_2^n \oplus \mathbb{Z}_2^n$.

Moreover, for any Lagrangian subspace M of $\mathbb{Z}_2^n \oplus \mathbb{Z}_2^n$, there always exist functions $f : M \to \mathbb{Z}_2$ such that $\{(-1)^{f(x)}W_{\mathbf{x}} : \mathbf{x} \in M\}$ is a stabilizer group. Let us denote $|M, f\rangle$

the stabilizer state corresponding to this stabilizer group. Moreover, other such function f must be of the form $f + \delta$ where $\delta(\mathbf{x}) = [\mathbf{x}, \mathbf{z}]$ for some $\mathbf{z} \in \mathbb{Z}_2^n \oplus \mathbb{Z}_2^n$ and it can be checked that any function of such form also induces a stabilizer group. For any such δ, we also have $|M, f + \delta\rangle = W_{\mathbf{z}} |M, f\rangle$.

2.6.3 Characteristic distribution of stabilizer states

Writing a stabilizer state $|S\rangle$ as $|M, f\rangle$ allows us to write the projector

$$|S\rangle \langle S| = \frac{1}{2^n} \sum_{\mathbf{x} \in M} (-1)^{f(\mathbf{x})} W_{\mathbf{x}}$$

as in the equation 2.8. Hence, by the formula 2.4, we have

$$c_S(\mathbf{x}) = \begin{cases} 2^{-n/2}(-1)^{f(\mathbf{x})} & \text{if } \mathbf{x} \in M \\ 0 & \text{otherwise.} \end{cases}$$

Hence, the characteristic distribution $p_S(\mathbf{x})$ for stabilizer state $|S\rangle = |M, f\rangle$ is given by

$$p_S(\mathbf{x}) = \begin{cases} 2^{-n} & \text{if } \mathbf{x} \in M, \\ 0 & \text{otherwise,} \end{cases}$$

that is a uniform distribution whose support is the set M. Moreover, if $|\psi\rangle = |M, f\rangle$ is a stabilizer state, then

$$\overline{\psi} = \overline{|\psi\rangle \langle\psi|} = \sum_{\mathbf{x}} (-1)^{\pi(\mathbf{x}) + f(\mathbf{x})} W_{\mathbf{x}}$$

so $|\overline{\psi}\rangle$ is also a stabilizer state and $|\overline{\psi}\rangle = |M, g\rangle$ for some function g. Consequently, $|\overline{\psi}\rangle = W_{\mathbf{z}} |\psi\rangle$ for some $\mathbf{z}$.

Chapter 3

Stabilizer testing

We say that a state $|\psi\rangle$ of n qubits is *ε-far from any stabilizer states* if

$$\max_{S \in \mathrm{Stab}(n)} |\langle S|\psi\rangle|^2 \leq 1 - \varepsilon^2.$$

We will usually write the expression on the left hand side as $\max_S |\langle S|\psi\rangle|^2$. *Stabilizer testing algorithm* (or *stabilizer tester*) is a quantum algorithm that, given t copies of a state $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$, accepts if $|\psi\rangle$ is a stabilizer state and rejects with non-zero probability if it is ε-far from any stabilizer states.

The definition of stabilizer testing algorithm above must depend on ε but in many contexts of our discussion this is not a problem.

In this chapter, we study a stabilizer testing algorithm from [GNW17] that uses 6 copies of $|\psi\rangle$. In Section 3.1, we write down the algorithm and mention its important properties. In Section 3.2, we discuss some primitives that are used in the algorithm and their properties. In Section 3.3, we give a brief analysis of the algorithm. In Section 3.4, we will look into some parts of the proof and modify them. We show that we can obtain the same analysis without proving the so-called Bell difference sampling theorem. We will use this modification for analyzing stabilizer testing protocol in Chapter 5.

3.1 A 6-copy algorithm

We write the 6-copy algorithm that we can use for stabilizer testing in Algorithm 1 and its high-level circuit is given in Figure 3.1. There are two non-classical primitives namely Bell sampling and Weyl measurement which will be discussed in another section. The second and fourth steps of the algorithm can be done classically.

Algorithm 1: Stabilizer testing algorithm with 6 copies.

```
Input: 6 copies of a state $|\psi\rangle$ of $n$ qubits.
    1. Perform Bell sampling twice on two independent copies of $|\psi\rangle^{\otimes 2}$ each. Let the two sampling outcomes be $\mathbf{x}$ and $\mathbf{y}$; each is an element of $\mathbb{Z}_2^n \oplus \mathbb{Z}_2^n$.
    2. Compute the sum (difference) $\mathbf{z} := \mathbf{x} - \mathbf{y} = \mathbf{x} + \mathbf{y}$.
    3. Perform Weyl $W_{\mathbf{z}}$ measurement on two independent copies of $|\psi\rangle$ twice.
    4. Accept iff both Weyl $W_{\mathbf{z}}$ measurement outcomes agree.
```

As we will see, the algorithm is perfectly complete, transversal, and independent of the number of qubits. By being perfectly complete, we mean that if the state $|\psi\rangle$ is a stabilizer state, the algorithm will accept with probability 1. In this case, the algorithm never makes an error. By being transversal, we mean the algorithm factorizes into qubits of $|\psi\rangle$ or pair of qubits in $|\psi\rangle^{\otimes 2}$. This is the nature of Bell sampling and Weyl measurement. By being independent of the number of qubits, we mean that the error of our algorithm does not depend on n. Thus, if we want to reduce the error it does not depend on the number of qubits of our states. This means that the algorithm tests the *stabilizerness* property of quantum state regardless of the number of qubits.

3.2 Bell sampling and Weyl measurement

3.2.1 Bell sampling

Bell states are useful in the task of quantum teleportation [BBC+93] and many other tasks in quantum information. They are states that are obtained from applying one of the four Pauli operators to one of the two qubits of an EPR pair:

$$
\begin{aligned}
|\Phi_{00}\rangle &= (\sigma_{00} \otimes I)\,|\Phi_{00}\rangle = \frac{1}{\sqrt{2}}\,|00\rangle + \frac{1}{\sqrt{2}}\,|11\rangle \\
|\Phi_{01}\rangle &= (\sigma_{01} \otimes I)\,|\Phi_{00}\rangle = \frac{1}{\sqrt{2}}\,|01\rangle + \frac{1}{\sqrt{2}}\,|10\rangle \\
|\Phi_{10}\rangle &= (\sigma_{10} \otimes I)\,|\Phi_{00}\rangle = \frac{1}{\sqrt{2}}\,|00\rangle - \frac{1}{\sqrt{2}}\,|11\rangle \\
|\Phi_{11}\rangle &= (\sigma_{11} \otimes I)\,|\Phi_{00}\rangle = \frac{1}{\sqrt{2}}\,|01\rangle - \frac{1}{\sqrt{2}}\,|10\rangle\,.
\end{aligned}
$$

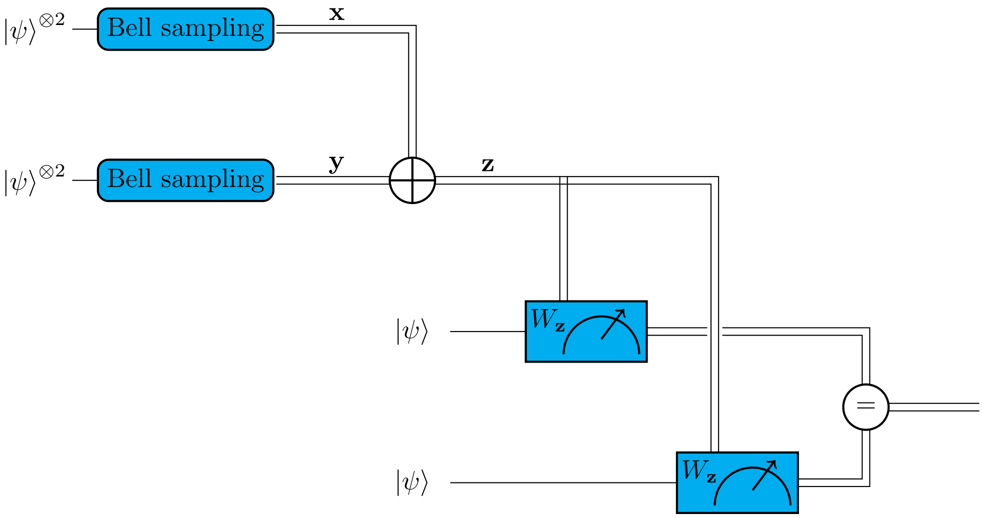

Figure 3.1: A high-level circuit for the 6-copy algorithm. A single line indicates quantum data while double lines indicate that the data is classical. Bell sampling is a primitive that can be performed using CNOT gate, Hadamard gate, and performing measurement in computational basis.

They form an orthonormal basis of $(\mathbb{C}^2)^{\otimes 2}$. Hence, they correspond to a projective measurement $\{|\Phi_{\mathbf{x}}\rangle\langle\Phi_{\mathbf{x}}|\}_{\mathbf{x}\in\mathbb{Z}_2^2}$ on $(\mathbb{C}^2)^{\otimes 2}$.

Now, in the system of $2\cdot n$ qubits, we denote n EPR pairs as

$$|\Phi^+\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{q}\in\mathbb{Z}_2^n} |\mathbf{q}\rangle \otimes |\mathbf{q}\rangle$$

where $|\mathbf{q}\rangle = |q_1, \ldots, q_n\rangle$ is a state in a computational basis corresponding to the components of $\mathbf{q} \in \mathbb{Z}_2^n$. We illustrate this in Figure 3.2. For $\mathbf{x} \in \mathbb{Z}_2^n \oplus \mathbb{Z}_2^n$, applying a Weyl operator $W_{\mathbf{x}}$ to the first n qubits, we will obtain n pairs of Bell states, which we denote as

$$|W_{\mathbf{x}}\rangle = (W_{\mathbf{x}} \otimes I)\,|\Phi^+\rangle\,.$$

Projective measurement $\{|W_{\mathbf{x}}\rangle\langle W_{\mathbf{x}}|\}_{\mathbf{x}\in\mathbb{Z}_2^n\oplus\mathbb{Z}_2^n}$ is known as *Bell sampling* [Mon17, ZPDF16]. Moreover, given a state $|\psi\rangle$ of n qubits, performing Bell sampling on $|\psi\rangle^{\otimes 2}$ is just performing projective measurement in the Bell basis on n corresponding pairs of qubits from each copy. This means that Bell sampling transversal.

Let us denote by $t_\psi(\mathbf{x})$ the probability of obtaining an outcome $\mathbf{x}$ from performing Bell

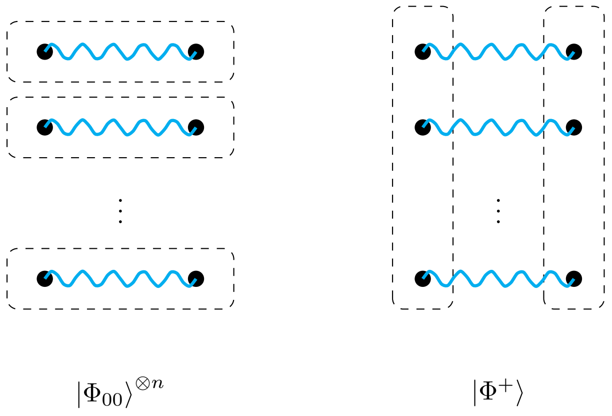

Figure 3.2: Two ways of looking at n EPR pairs based on the order of the qubit systems. More precisely, there exists a unitary J that permutes the tensor factors such that $|\Phi^+\rangle = J\,|\Phi_{00}\rangle^{\otimes n}$.

sampling on $|\psi\rangle^{\otimes 2}$, namely

$$t_\psi(\mathbf{x}) = |\,\langle W_\mathbf{x}|\,(|\psi\rangle \otimes |\psi\rangle)|^2.$$

We call t_ψ the *Bell sampling distribution* of a pure state $|\psi\rangle$. We prove the following formula for t_ψ.

Proposition 3.1 (Bell sampling distribution [Mon17]). *For any pure state ψ of n qubits, we have that*

$$t_\psi(\mathbf{x}) = 2^{-n}|\,\langle\psi|W_\mathbf{x}|\overline{\psi}\rangle\,|^2.$$

Proof. The proof uses transpose trick:

$$\begin{aligned}
&\mathrm{tr}[|W_\mathbf{x}\rangle\,\langle W_\mathbf{x}|\,\psi^{\otimes 2}] = \langle\Phi^+|\,(I\otimes W_\mathbf{x})\psi^{\otimes 2}(I\otimes W_\mathbf{x})\,|\Phi^+\rangle\\
&= \langle\Phi^+|\,(\psi\otimes W_\mathbf{x}\psi W_\mathbf{x})\,|\Phi^+\rangle = \langle\Phi^+|\,(I\otimes W_\mathbf{x}\psi W_\mathbf{x}\overline{\psi})\,|\Phi^+\rangle\\
&= \mathrm{tr}[|\Phi^+\rangle\,\langle\Phi^+|\,(I\otimes W_\mathbf{x}\psi W_\mathbf{x}\overline{\psi})] = 2^{-n}\sum_\mathbf{q}\mathrm{tr}[|\mathbf{q}\rangle\,\langle\mathbf{q}|\,W_\mathbf{x}\psi W_\mathbf{x}\overline{\psi}] = 2^{-n}\mathrm{tr}[W_\mathbf{x}\psi W_\mathbf{x}\overline{\psi}],
\end{aligned}$$

where the first equation is because trace is cyclic and the definition of $|W_\mathbf{x}\rangle$, the third equation is by the so called transpose trick and the fact that for pure state ψ, $\psi^\top = \overline{\psi}$, the fourth equation is again because trace is cyclic, and fifth equation is by the definition of $|\Phi^+\rangle$. It is now easy to see that

$$\mathrm{tr}[W_\mathbf{x}\psi W_\mathbf{x}\overline{\psi}] = |\,\langle\psi|W_\mathbf{x}|\overline{\psi}\rangle\,|^2.$$

□

3.2.2 Weyl measurement

Pauli operators X, Y, and Z have spectral decompositions as follows:

$$\begin{aligned} X &= \left|+\right\rangle\left\langle+\right| - \left|-\right\rangle\left\langle-\right| \\ Y &= \left|L\right\rangle\left\langle L\right| - \left|R\right\rangle\left\langle R\right| \\ Z &= \left|0\right\rangle\left\langle 0\right| - \left|1\right\rangle\left\langle 1\right| . \end{aligned}$$

So, measuring Pauli operators X, Y, and Z will give us an outcome that is their eigenvalues, namely $+1$ or -1.

For every $\mathbf{x} = (\mathbf{p}, \mathbf{q}) \in \mathbb{Z}_2^n \oplus \mathbb{Z}_2^n$, a Weyl operator $W_\mathbf{x}$ on n qubits is just an n-fold tensor product of Pauli operators

$$W_\mathbf{x} = \sigma_{p_1 q_1} \otimes \ldots \otimes \sigma_{p_n q_n}.$$

We define *Weyl measurement* as measuring some Weyl operator $W_\mathbf{x}$ on a state of n qubits. Weyl measurement has two possible outcomes $+1$ and -1. The projectors that correspond to the outcome $+1$ and -1 of Weyl $W_\mathbf{x}$ measurement are

$$\frac{I - W_\mathbf{x}}{2} \text{ and } \frac{I + W_\mathbf{x}}{2},$$

respectively. Performing Weyl $W_\mathbf{x}$ measurement can also be thought as measuring Pauli $\sigma_{p_i q_i}$ to the i-th qubit of $|\psi\rangle$. Hence, together with Bell sampling they perform transversal tests.

If we want to test whether a state $|\psi\rangle$ is an eigenvector of a Weyl operator $W_\mathbf{x}$, we can measure $W_\mathbf{x}$ on $|\psi\rangle$ several times and accept if and only if all the measurement outcomes agree. We call this procedure *Weyl eigenvector test*. Let ℓ be the number of repetitions of the Weyl measurement on ℓ independent copies of $|\psi\rangle$. Given a state $|\psi\rangle$ of n qubits and $\mathbf{x} \in \mathbb{Z}_2^n \oplus \mathbb{Z}_2^n$, we denote by $w_{\psi,\ell}(\mathbf{x})$ the probability that the Weyl $W_\mathbf{x}$ eigenvector test with ℓ repetitions accepts $|\psi\rangle$. Note that $w_{\psi,\ell}$ is not a probability distribution over $\mathbb{Z}_2^n \oplus \mathbb{Z}_2^n$.

Proposition 3.2. *Let $|\psi\rangle$ be a state of n qubits, $\ell > 1$ be a positive integer and $\mathbf{x} \in \mathbb{Z}_2^n \oplus \mathbb{Z}_2^n$. Then the probability that Weyl $W_\mathbf{x}$ eigenvector test with ℓ repetition accepts $W_\mathbf{x}$ is given by*

$$w_{\psi,\ell}(\mathbf{x}) = \left(\frac{1 + \sqrt{2^n p_\psi(\mathbf{x})}}{2}\right)^\ell + \left(\frac{1 - \sqrt{2^n p_\psi(\mathbf{x})}}{2}\right)^\ell .$$

where $p_\psi(\mathbf{x})$ is the probability distribution in 2.6. Consequently, $w_{\psi,\ell}(x) = f_\ell(2^n p_\psi(\mathbf{x}))$ for some polynomial f_ℓ with non-negative coefficients. If we fix n as a constant, we also have that $w_{\psi,\ell}$ is a polynomial with non-negative coefficients in $p_\psi(\mathbf{x})$.

Proof. The probability can be computed immediately by computing

$$\operatorname{tr}\left[\left(\frac{I+W_{\mathbf{x}}}{2}\right)^{\ell}\psi^{\otimes 2\ell}\right]+\operatorname{tr}\left[\left(\frac{I-W_{\mathbf{x}}}{2}\right)^{\ell}\psi^{\otimes 2\ell}\right].$$

The consequence can be checked by expanding the expression

$$f_\ell(t)=\left(\frac{1+\sqrt{t}}{2}\right)^{\ell}+\left(\frac{1-\sqrt{t}}{2}\right)^{\ell}=2^{-\ell}\sum_{i=0}^{\ell}(\sqrt{t})^i+(-\sqrt{t})^i=2^{-\ell}\sum_{0\le i\le \ell/2}t^{2i}.$$

□

In particular, if $|\psi\rangle$ is an eigenvector of $W_{\mathbf{x}}$ then $c_\psi(\mathbf{x})=2^{-\frac{n}{2}}\operatorname{tr}[W_{\mathbf{x}}\psi]=\pm 1$ and hence the probability above will be 1. Algorithm 1 uses Weyl eigenvalue test with $\ell=2$ repetitions. For $\ell=2$, the probability of being accepted by Weyl eigenvector test is

$$w_{\psi,2}(\mathbf{x})=\frac{1+2^n p_\psi(\mathbf{x})}{2}.$$

3.3 Brief analysis

We begin by showing that Algorithm 1 has perfect completeness, i.e. accepts stabilizer state with probability 1.

Proposition 3.3 (Perfect completeness of Algorithm 1 [GNW17])**.** *If $|\psi\rangle\in Stab(n)$, Algorithm 1 accepts $|\psi\rangle$ with probability* 1*.*

Proof. Suppose $|\psi\rangle$ is a stabilizer state of n qubits. We can write $|\psi\rangle=|M,f\rangle$ for some Lagrangian subspace $M\subseteq\mathbb{Z}_2^n\oplus\mathbb{Z}_2^n$ and function $f:\mathbb{Z}_2^n\oplus\mathbb{Z}_2^n\to\mathbb{Z}_2$ as mentioned in Section 2.6. There exists $\mathbf{z}\in\mathbb{Z}_2^n\oplus\mathbb{Z}_2^n$ such that $\overline{|\psi\rangle}=W_{\mathbf{z}}|\psi\rangle$. This $\mathbf{z}$ depends on $|\psi\rangle$, which is unknown. From Proposition 3.1, performing Bell sampling on $|\psi\rangle^{\otimes 2}$ will give an outcome $\mathbf{x}$ with probability

$$t_\psi(\mathbf{x})=2^{-n}|\langle\psi|W_{\mathbf{x}+\mathbf{z}}|\psi\rangle|^2=p_\psi(\mathbf{x}+\mathbf{z}).$$

Hence we obtain an $\mathbf{x}$ such that $\mathbf{x}+\mathbf{z}\in M$ but $\mathbf{x}$ is not necessarily in M. If we do Bell sampling twice on two independent copies of $|\psi\rangle^{\otimes 2}$, we will obtain two outcomes $\mathbf{x}$ and $\mathbf{y}$ where $\mathbf{x}+\mathbf{z},\mathbf{y}+\mathbf{z}\in M$. Note that $\mathbf{x}$ and $\mathbf{y}$ are not necessarily in M, but we know that $\mathbf{x}+\mathbf{z}+\mathbf{y}+\mathbf{z}=\mathbf{x}+\mathbf{y}$ must be in M since M is a subspace. We know that $|\psi\rangle$ is a $(-1)^{f(\mathbf{x}+\mathbf{y})}$ eigenvector of $W_{\mathbf{x}+\mathbf{y}}$. Hence, $|\psi\rangle$ will be accepted by eigenvector test corresponding to Weyl operator Weyl $W_{\mathbf{x}+\mathbf{y}}$ with probability 1. □

Note that if $|\psi\rangle$ is a stabilizer state with real amplitude, namely $\overline{|\psi\rangle} = |\psi\rangle$, we have

$$t_\psi(\mathbf{x}) = 2^{-n} |\langle\psi|W_\mathbf{x}|\overline{\psi}\rangle|^2 = 2^{-n} |\langle\psi|W_\mathbf{x}|\psi\rangle|^2 = p_\psi(\mathbf{x}) \tag{3.4}$$

so we know the outcome of Bell sampling comes from the set M.

Suppose $|\psi\rangle$ is ε-far from any stabilizer states. The idea of the proof is to connect three quantities, namely the probability that the algorithm accepts $|\psi\rangle$, the characteristic distribution p_ψ, and $\max_S |\langle S|\psi\rangle|^2$. In this thesis, we mainly explore some new relations between the first two quantities and just use the result about the last two quantities. The following lemma shows the relation of the last two quantities.

Lemma 3.5 ([GNW17])**.** *Let $|\psi\rangle$ be a pure state of n qubits. Let $M_0 \subseteq \mathbb{Z}_2^n \oplus \mathbb{Z}_2^n$ such that*

$$M_0 = \left\{\mathbf{x} : 2^n \cdot p_\psi(\mathbf{x}) > \frac{1}{2}\right\}. \tag{3.6}$$

Then,

$$\max_{S \in Stab(n)} |\langle S|\psi\rangle|^2 \geq \sum_{\mathbf{x} \in M_0} p_\psi(\mathbf{x}). \tag{3.7}$$

Proof. We refer the to the proof in [GNW17]. □

For the analysis of the first two quantities, a new primitive called *Bell difference sampling* is introduced in [GNW17]. Bell difference sampling is defined as performing Bell sampling twice on two independent copies of the states we are testing and take the difference of the two outcomes. In Algorithm 1, this is the combination of steps 1 and 2.

If $|\psi\rangle = |M, f\rangle$ is a stabilizer state, the outcome of Bell difference sampling on four copies of $|\psi\rangle$ will be a sample $\mathbf{z}$ from and only from the set M, which contains the supports of the characteristic distribution of $|\psi\rangle$. The elements of M correspond to Weyl operators that stabilize $|\psi\rangle$. If $|\psi\rangle$ is not a stabilizer state, it is not clear how Bell sampling distribution t_ψ is related to the characteristic distribution of $|\psi\rangle$. Let us denote by $q_\psi(\mathbf{a})$ the probability of obtaining outcome $\mathbf{a}$ from performing Bell difference sampling on four copies of $|\psi\rangle$. We call q_ψ the *Bell difference sampling distribution.* Also, the POVM element that corresponds to outcome $\mathbf{a}$ from Bell difference sampling is given by

$$\Pi_\mathbf{a} = \sum_\mathbf{x} |W_\mathbf{x}\rangle\langle W_\mathbf{x}| \otimes |W_{\mathbf{x}+\mathbf{a}}\rangle\langle W_{\mathbf{x}+\mathbf{a}}|, \tag{3.8}$$

and the probability is

$$q_\psi(\mathbf{a}) = \sum_\mathbf{x} t_\psi(\mathbf{x}) t_\psi(\mathbf{x}+\mathbf{a}). \tag{3.9}$$

Bell difference sampling theorem is a beautiful theorem that relates t_ψ and p_ψ.

Theorem 3.10 (Bell difference sampling theorem [GNW17])**.** *Let ψ be a pure state of n qubits. The probability of obtaining an outcome* $\mathbf{a}$ *from Bell difference sampling is given by*

$$q_\psi(\mathbf{a}) = \sum_{\mathbf{x}} t_\psi(\mathbf{x}) t_\psi(\mathbf{x}+\mathbf{a}) = \sum_{\mathbf{x}} p_\psi(\mathbf{x}) p_\psi(\mathbf{x}+\mathbf{a}). \tag{3.11}$$

Proof. We refer to [GNW17] for the proof. We will provide an alternative proof in the next section. □

It is not true in general that for any $\mathbf{a}_1, \dots, \mathbf{a}_m$,

$$\sum_{\mathbf{x}} t_\psi(\mathbf{x}) t_\psi(\mathbf{x}+\mathbf{a}_1) \dots t_\psi(\mathbf{x}+\mathbf{a}_m) = \sum_{\mathbf{x}} p_\psi(\mathbf{x}) p_\psi(\mathbf{x}+\mathbf{a}_1) \dots p_\psi(\mathbf{x}+\mathbf{a}_m).$$

Now, we prove that it rejects non-stabilizer state with non-zero probability.

Proposition 3.12 ([GNW17])**.** *Let ψ be a state of n qubits that is ε-far from any stabilizer states. Then Algorithm 1 accepts ψ with probability at most $1 - \frac{1}{4}\varepsilon^2$.*

Proof. We can see that the POVM that corresponds to accepting a state $|\psi\rangle$ is given by

$$\Pi_{\text{accept}} = \sum_{\mathbf{a}} \Pi_{\mathbf{a}} \otimes \frac{I^{\otimes 2} + W_{\mathbf{x}}^{\otimes 2}}{2} \tag{3.13}$$

where $\Pi_{\mathbf{a}}$ is a POVM element defined in equation 3.8 corresponding to outcome $\mathbf{a}$ of Bell difference sampling. Then, the probability of accepting $|\psi\rangle$ is

$$\begin{aligned} p_{\text{accept}} &= \operatorname{tr}[\Pi_{\text{accept}} \psi^{\otimes 6}] = \frac{1}{2} \sum_{\mathbf{a}} q_\psi(\mathbf{a})(1 + 2^n p_\psi(\mathbf{a})) \\ &= \frac{1}{2} \sum_{\mathbf{a}} \sum_{\mathbf{x}} p_\psi(\mathbf{x}) p_\psi(\mathbf{x}+\mathbf{a})(1 + 2^n p_\psi(\mathbf{a})) = \frac{1}{2} \sum_{\mathbf{x}} p_\psi(\mathbf{x})(1 + 2^n \sum_{\mathbf{a}} p_\psi(\mathbf{x}+\mathbf{a}) p_\psi(\mathbf{a})) \\ &\le \frac{1}{2} \sum_{\mathbf{x}} p_\psi(\mathbf{x})(1 + 2^n \sum_{\mathbf{a}} p_\psi(\mathbf{a})^2) = \frac{1}{2} \sum_{\mathbf{a}} p_\psi(\mathbf{a})(1 + 2^n p_\psi(\mathbf{a})), \end{aligned}$$

where the third equation is by Theorem 3.10, the inequality is by the Cauchy Schwarz inequality. By Markov's inequality, we have

$$\sum_{\mathbf{a} \in M_0} p_\psi(\mathbf{a}) \ge 1 - 2 \sum_{\mathbf{a}} p_\psi(\mathbf{a})(1 - 2^n p_\psi(\mathbf{a})) = 1 - 4(1 - p_{\text{accept}})$$

which works because $p_\psi(\mathbf{a}) \le 2^{-n}$. It follows that if ψ is ε-far from any stabilizer states, using Lemma 3.7, we obtain

$$1 - \varepsilon^2 \ge \max_S |\langle S|\psi\rangle|^2 \ge \sum_{\mathbf{a} \in M_0} p_\psi(\mathbf{a}) \ge 1 - 4(1 - p_{\text{accept}}),$$

and hence $p_{\text{accept}} \le 1 - \frac{1}{4}\varepsilon^2$. □

3.4 Another perspective

We prove some facts in the analysis above in a different way. First, we prove Theorem 3.10, namely Bell difference sampling theorem, in different way. Second, we also prove

$$p_{\text{accept}} \leq \frac{1}{2}\sum_{\mathbf{a}} p_\psi(\mathbf{a})(1 + 2^n p_\psi(\mathbf{a})).$$

in a different way; without using the Bell difference sampling theorem. We use the same method later in Chapter 5 to analyze some protocol for stabilizer testing with many copies that is more efficient than just repeating Algorithm 1.

All the propositions below aim to write p_ψ and t_ψ in terms of $c_\psi(\mathbf{x})$. The behaviour of the computation is also very similar, namely using Lemma 3.14.

Lemma 3.14. *Let* $\mathbf{x} \in \mathbb{Z}_2^n \oplus \mathbb{Z}_2^n$. *Then*

$$\sum_{\mathbf{y} \in \mathbb{Z}_2^n \oplus \mathbb{Z}_2^n} (-1)^{[\mathbf{x},\mathbf{y}]} = \begin{cases} 2^n & \textit{if } \mathbf{x} = 0, \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. Follows from the fact that for any $\mathbf{x} \in \mathbb{Z}_2^n \oplus \mathbb{Z}_2^n$, the function $\varphi : \mathbb{Z}_2^n \oplus \mathbb{Z}_2^n \to \mathbb{Z}_2$

$$\varphi(\mathbf{y}) = (-1)^{[\mathbf{x},\mathbf{y}]}$$

is a homomorphism; and it is a trivial homomorphism if and only if $\mathbf{x} = \mathbf{0}$. □

We first write p_ψ and t_ψ in terms of p_ψ.

Proposition 3.15. *For any pure state* ψ *of* n *qubits,*

$$p_\psi(\mathbf{x}) = 2^{-n}\sum_{\mathbf{y}} p_\psi(\mathbf{y})(-1)^{[\mathbf{x},\mathbf{y}]}$$
$$t_\psi(\mathbf{x}) = 2^{-n}\sum_{\mathbf{y}} p_\psi(\mathbf{y})(-1)^{\pi(\mathbf{y})+[\mathbf{x},\mathbf{y}]}.$$

Proof. The first equation can be obtained from the following computation:

$$\begin{aligned} p_\psi(\mathbf{x}) &= 2^{-n}\mathrm{tr}[W_{\mathbf{x}}\psi W_{\mathbf{x}}\psi] = 2^{-2n}\sum_{\mathbf{y},\mathbf{z}} c_\psi(\mathbf{y})c_\psi(\mathbf{z})\mathrm{tr}[W_{\mathbf{x}}W_{\mathbf{y}}W_{\mathbf{x}}W_{\mathbf{z}}] \\ &= 2^{-2n}\sum_{\mathbf{y},\mathbf{z}} c_\psi(\mathbf{y})c_\psi(\mathbf{z})(-1)^{[\mathbf{x},\mathbf{y}]}\mathrm{tr}[W_{\mathbf{y}}W_{\mathbf{z}}] = 2^{-n}\sum_{\mathbf{y}} c_\psi(\mathbf{y})^2(-1)^{[\mathbf{x},\mathbf{y}]}. \end{aligned}$$

The second equation can be obtained from the following computation:

$$\begin{aligned} t_\psi(\mathbf{x}) &= 2^{-n}\mathrm{tr}[W_{\mathbf{x}}\psi W_{\mathbf{x}}\overline{\psi}] = 2^{-2n}\sum_{\mathbf{y},\mathbf{z}} c_\psi(\mathbf{y})c_\psi(\mathbf{z})(-1)^{\pi(\mathbf{z})}\mathrm{tr}[W_{\mathbf{x}}W_{\mathbf{y}}W_{\mathbf{x}}W_{\mathbf{z}}] \\ &= 2^{-2n}\sum_{\mathbf{y},\mathbf{z}} c_\psi(\mathbf{y})c_\psi(\mathbf{z})(-1)^{\pi(\mathbf{z})}(-1)^{[\mathbf{x},\mathbf{z}]}\mathrm{tr}[W_{\mathbf{y}}W_{\mathbf{z}}] = 2^{-n}\sum_{\mathbf{y}} c_\psi(\mathbf{y})^2(-1)^{\pi(\mathbf{y})+[\mathbf{x},\mathbf{y}]}. \end{aligned}$$

□

Now, we prove the Bell difference sampling theorem in a different way.

Proof of Theorem 3.10. We simply compute

$$\sum_{\mathbf{x}} p_\psi(\mathbf{x})p_\psi(\mathbf{x}+\mathbf{a}) = 2^{-2n}\sum_{\mathbf{y},\mathbf{z}} p_\psi(\mathbf{y})p_\psi(\mathbf{z})(-1)^{[\mathbf{a},\mathbf{z}]}\sum_{\mathbf{x}}(-1)^{[\mathbf{x},\mathbf{y}+\mathbf{z}]} = \sum_{\mathbf{y}} p_\psi(\mathbf{y})^2(-1)^{[\mathbf{a},\mathbf{y}]}.$$

and

$$\sum_{\mathbf{x}} t_\psi(\mathbf{x})t_\psi(\mathbf{x}+\mathbf{a}) = 2^{-2n}\sum_{\mathbf{y},\mathbf{z}} p_\psi(\mathbf{y})p_\psi(\mathbf{z})(-1)^{\pi(\mathbf{y})+\pi(\mathbf{z})+[\mathbf{a},\mathbf{z}]}\sum_{\mathbf{x}}(-1)^{[\mathbf{x},\mathbf{y}+\mathbf{z}]} = \sum_{\mathbf{y}} p_\psi(\mathbf{y})^2(-1)^{[\mathbf{a},\mathbf{y}]}$$

where in the last step we use Lemma 3.14. □

Next, we prove the relation between probability of accepting a state $|\psi\rangle$ of n qubits with the characteristic distribution p_ψ. First we prove the following lemma.

Lemma 3.16. *Let ψ be an arbitrary pure state of n qubits. Then,*

$$\sum_{\mathbf{a}} t_\psi(\mathbf{x}+\mathbf{a})p_\psi(\mathbf{a}) \le \sum_{\mathbf{a}} p_\psi(\mathbf{a})^2.$$

Proof. We compute

$$\sum_{\mathbf{a}} t_\psi(\mathbf{x}+\mathbf{a})p_\psi(\mathbf{a}) = 2^{-2n}\sum_{\mathbf{a},\mathbf{y},\mathbf{z}} p_\psi(\mathbf{x})p_\psi(\mathbf{z})(-1)^{\pi(\mathbf{y})+[\mathbf{x},\mathbf{y}]+[\mathbf{a},\mathbf{y}+\mathbf{z}]} = \sum_{\mathbf{y}}(-1)^{\pi(\mathbf{y})+[\mathbf{x},\mathbf{y}]}p_\psi(\mathbf{y})^2,$$

and the inequality immediately follows. □

But then some steps in the proof can be slightly changed as follows. Note that our argument does not require the Bell difference sampling theorem.

Alternative proof to Proposition 3.12. We only modify the step of the proof for

$$p_{\text{accept}} = \sum_{\mathbf{a}} q_\psi(\mathbf{a})(1+2^n p_\psi(\mathbf{a})) \le \sum_{\mathbf{a}} p_\psi(\mathbf{a})(1+2^n p_\psi(\mathbf{a})).$$

To prove this, we observe that

$$\begin{aligned}
\sum_{\mathbf{a}} q_\psi(\mathbf{a})(1+2^n p_\psi(\mathbf{a})) &= \sum_{\mathbf{a}}\sum_{\mathbf{x}} t_\psi(\mathbf{x})t_\psi(\mathbf{x}+\mathbf{a})(1+2^n p_\psi(\mathbf{a})) \\
&= \sum_{\mathbf{x}} t_\psi(\mathbf{x})\left(1+2^n\sum_{\mathbf{a}} t_\psi(\mathbf{x}+\mathbf{a})p_\psi(\mathbf{a})\right) \\
&\le \sum_{\mathbf{x}} t_\psi(\mathbf{x})\left(1+2^n\sum_{\mathbf{a}} p_\psi(\mathbf{a})^2\right) \\
&= 1+2^n\sum_{\mathbf{a}} p_\psi(\mathbf{a})^2 \\
&= \sum_{\mathbf{a}} p_\psi(\mathbf{a})(1+2^n p_\psi(\mathbf{a}))
\end{aligned}$$

where in the inequality we use Lemma 3.16. □

Chapter 4

Dimension independent stabilizer testing no-go theorem for t copies

There are several no-go theorems that are known in theory of quantum computing, such as the quantum no-cloning theorem [WZ82, Die82] or the quantum no-deleting theorem [PB00]. A no-go theorem is usually a mathematical theorem about impossibility of a certain condition to happen.

In this chapter, we will discuss the impossibility of finding a stabilizer tester whose power is independent of the number of qubits with small amount of copies. More precisely, we ask for the minimal number of copies of a state such that we can find a stabilizer testing algorithm that is independent of the number of qubits of the state. It is known that the upper bound is 6 [GNW17]. The main result of this chapter is to show that we have a lower bound of 5. We present this in terms of no-go theorem for 4 copies.

An operator P on $\mathbb{C}^d$ is called a *(binary) POVM element in* $\mathbb{C}^d$ if P and $I - P$ is a positive semi-definite operator on $\mathbb{C}^d$.

Definition 4.1 (Dimension independent stabilizer testing algorithm with perfect completeness for t copies)**.** *Let t be a positive integer. A sequence of operators $\{\Pi^{(n)}\}_n$, where for each n, $\Pi^{(n)}$ is a binary POVM element on $((\mathbb{C}^2)^{\otimes n})^{\otimes t}$, is called a* stabilizer testing algorithm with perfect completeness for t copies *if there exists a function $f : [0,1] \to [0,1]$ such that $f(\varepsilon) = 1$ iff $\varepsilon = 0$ and such that for every positive integer n:*

(i) for any $|S\rangle \in Stab(n)$, $tr[\Pi^{(n)}(|S\rangle\langle S|)^{\otimes t}] = 1$, and

(ii) for any $|\phi\rangle \in (\mathbb{C}^2)^{\otimes n}$ that is ε-far from any stabilizer states (of n qubits),

$$tr[\Pi^{(n)}(|\phi\rangle\langle\phi|)^{\otimes t}] \leq f(\varepsilon).$$

The sequence $\{\Pi^{(n)}\}$ is called dimension independent stabilizer testing algorithm with perfect completeness *if there exists such function f that does not depend on n.*

In this thesis, we will only discuss stabilizer testing algorithm with perfect completeness, namely the algorithm accepts a stabilizer state with probability 1, as stated in Condition (i). We believe that similar result holds for any stabilizer testing algorithm that can be used for stabilizer testing with high accuracy. The algorithm can only make a type-II error, that is when it accepts a state that is far from any stabilizer states.

Note that if our algorithm has perfect completeness, we can run the algorithm many times to obtain a small error probability. The number of times we repeat the algorithm depends on our knowledge of how often the algorithm accepts a state that is far from any stabilizer states. Condition (ii) from our definition states that we know that the probability of it accepts a state that is ε-far from any stabilizer states cannot be larger than $f(\varepsilon)$. Note that if $f(\varepsilon)$ gets larger as n gets larger, the number of times we need to run the algorithm to obtain a small error probability will be larger as well. If $f(\varepsilon)$ does not depend on n, the number of repetitions is not dependent on n as well. This is good since then we can think that the algorithm really just tests whether a state is a stabilizer state regardless of the number of qubits.

We now define the no-go theorem for t copies.

Definition 4.2 (No go theorem for t copies)**.** *The* no-go theorem for t copies *is a theorem that states there exists no dimension independent stabilizer testing algorithm with perfect completeness for t copies.*

It is clear that no-go theorem for 6 copies does not hold since we can use $\{\Pi_n\}_n$ from equation 3.13 with bound for type-II error $f(\varepsilon) = 1 - \frac{1}{4}\varepsilon^2$. Our main result in this chapter is the no-go theorem for 4 copies. We list the task of investigating whether the no-go theorem for 5 copies as a further research in Chapter 6.

To prove the no-go theorem for 4 copies, we will start by proving an inequality about the neighborhood of some quantum states in Section 4.1 and apply it for the case of stabilizer states. We show a connection between our no-go theorem and the notion of quantum designs in Section 4.2 and prove the no-go theorem for 3 copies. In Section 4.3, we prove a no-go

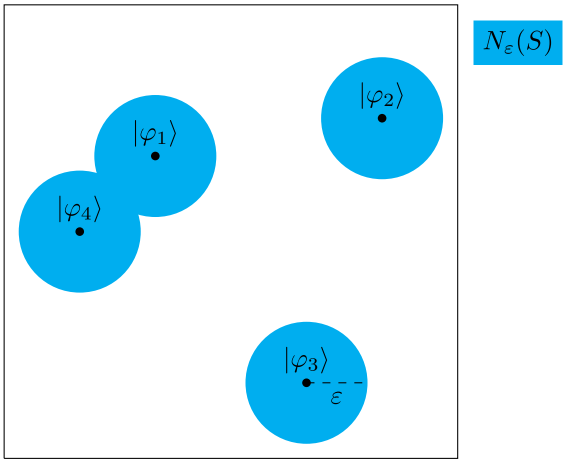

Figure 4.1: Illustration of an ε-neighborhood of a set of states $S = \{|\varphi_1\rangle, |\varphi_2\rangle, |\varphi_3\rangle, |\varphi_4\rangle\}$.

theorem for 4 copies. We describe a strategy to prove the no-go theorem for 5 copies in Section 4.4.

4.1 Neighborhood of quantum states

4.1.1 Quantum state neighborhood bound

Definition 4.3 (ε-neighborhood of a state). *Let $|\varphi\rangle \in (\mathbb{C}^2)^{\otimes n}$ be a pure state of n qubits. We define the* ε-neighborhood of $|\varphi\rangle$ *as*

$$N_\varepsilon(\varphi) = \{|\psi\rangle \in (\mathbb{C}^2)^{\otimes n} : |\langle\varphi|\psi\rangle|^2 \geq 1 - \varepsilon^2\}.$$

Then, by definition, we have that $N_\varepsilon(|\varphi\rangle) = \{|\psi\rangle \in (\mathbb{C}^2)^{\otimes n} : T(|\varphi\rangle, |\psi\rangle) \leq \varepsilon\}$ is a ball centered at $|\varphi\rangle$ of radius ε, where T is a trace distance. The complement $N_\varepsilon(|\varphi\rangle)^C$ is the set of all states of n qubits that are ε-far from $|\varphi\rangle$.

It is natural to define what we mean by an ε-neighborhood of a set of states is. If we are given a set of states, instead of only one state, it is natural to call a state close to such a set if it is close to some state in the set. Figure 4.1 is an illustration for an ε-neighborhood for a set of states.

Definition 4.4 (ε-neighborhood of a set of states). *Let $S \subseteq (\mathbb{C}^2)^{\otimes n}$ be a set of pure states* *of n qubits. We define the* ε-neighborhood of S *as*

$$N_\varepsilon(S) = \bigcup_{\varphi \in S} N_\varepsilon(\varphi).$$

Suppose we are given a state $|\varphi\rangle$ and a real number $\varepsilon > 0$. As ε goes to 0, there should be less and less states in the ε-neighborhood $N_\varepsilon(\varphi)$ of $|\varphi\rangle$. We want a quantitative version of this via the notion of probability. We can ask the following similar question: If we pick a state $|\psi\rangle$ randomly according to the Haar-measure, what is the probability that it lies in the neighborhood of $|\varphi\rangle$? The main result of this section is the following theorem which gives us an upper bound of picking a state that is in an ε-neighborhood of $|\varphi\rangle$.

Theorem 4.5 (State neighborhood bound)**.** *Let $\varepsilon > 0$ be a real number such that $\varepsilon^2 < \frac{1}{2}$ and $|\varphi\rangle \in (\mathbb{C}^2)^{\otimes n}$ be a pure state of n qubits. Then, the probability of a Haar random pure state $\psi \in (\mathbb{C}^2)^{\otimes n}$ is in $N_\varepsilon(\varphi)$ can be bounded as follows:*

$$\mathbb{P}_\psi[\psi \in N_\varepsilon(\varphi)] \leq \left(2e\cdot \varepsilon^2\right)^{2^n-1}.$$

We first prove some lemmas.

Lemma 4.6. *Let $\varepsilon \in (0,1)$, then the inequality*

$$(1-\varepsilon^2)^{\frac{1}{\varepsilon^2}-1} \geq \frac{1}{e}$$

holds. Consequently, if ℓ is the largest integer such that $\ell \leq \frac{1}{\varepsilon^2}$, then $(1-\varepsilon^2)^{\ell-1} \geq \frac{1}{e}$.

Proof. For $\varepsilon \in (0,1)$, we have that $\frac{1}{\varepsilon^2} - 1 > 0$ and hence

$$0 < \frac{1}{(1-\varepsilon^2)^{\frac{1}{\varepsilon^2}-1}} = \left(1 + \frac{1}{\frac{1}{\varepsilon^2}-1}\right)^{\frac{1}{\varepsilon^2}-1} \leq e$$

where we use the inequality $(1+1/x)^x \leq e$ for $x > 0$, and hence it follows that $(1-\varepsilon^2)^{\frac{1}{\varepsilon^2}-1} \geq \frac{1}{e}$. Now, the second statement follows since if $\ell \leq \frac{1}{\varepsilon^2}$, we have

$$(1-\varepsilon^2)^{\ell-1} \geq (1-\varepsilon^2)^{\frac{1}{\varepsilon^2}-1} \geq \frac{1}{e}.$$

□

Lemma 4.7. *Let $|\phi\rangle \in (\mathbb{C}^2)^{\otimes n} \cong \mathbb{C}^{2^n}$. Then*

$$\mathbb{E}_\psi[|\langle\phi|\psi\rangle|^{2t}] = \binom{2^n+t-1}{t}^{-1}.$$

Proof. Note that

$$\begin{aligned}
\mathbb{E}_\psi[|\langle\phi|\psi\rangle|^{2t}] &= \mathbb{E}_\psi[\langle\phi|^{\otimes t}|\psi\rangle^{\otimes t}\langle\psi|^{\otimes t}|\phi\rangle^{\otimes t}] \\
&= \langle\phi|^{\otimes t}\,\mathbb{E}_\psi[|\psi\rangle^{\otimes t}\langle\psi|^{\otimes t}]\,|\phi\rangle^{\otimes t} \\
&= \langle\phi|^{\otimes t}\left(\int |\psi\rangle^{\otimes t}\langle\psi|^{\otimes t}\,d\psi\right)|\phi\rangle^{\otimes t} \\
&= \langle\phi|^{\otimes t}\binom{2^n+t-1}{t}^{-1}\Pi_{\mathrm{sym}}^{(t)}|\phi\rangle^{\otimes t} \\
&= \binom{2^n+t-1}{t}^{-1}\langle\phi|^{\otimes t}|\phi\rangle^{\otimes t} \\
&= \binom{2^n+t-1}{t}^{-1},
\end{aligned}$$

where the second last equality follows from the fact that $|\phi\rangle^{\otimes t} \in \mathrm{Sym}^t((\mathbb{C}^2)^{\otimes n})$. □

We are now ready to prove our main theorem in this section.

Proof of Theorem 4.5. By Markov's inequality, we have

$$\mathbb{P}[\psi \in N_\varepsilon(\varphi)] = \mathbb{P}[|\langle\varphi|\psi\rangle|^2 \geq 1-\varepsilon^2] \leq \frac{\mathbb{E}[|\langle\varphi|\psi\rangle|^{2t}]}{(1-\varepsilon^2)^t},$$

for an arbitrary $t > 0$. We can upper bound $\mathbb{E}[|\langle\varphi|\psi\rangle|^{2t}]$ for any positive integer t as follows:

$$\mathbb{E}[|\langle\phi|\psi\rangle|^{2t}] = \binom{t+2^n-1}{t}^{-1} = \prod_{k=1}^{2^n-1}\frac{k}{t+k} \leq \left(\frac{2^n-1}{t+2^n-1}\right)^{2^n-1},$$

where the first equality is by Lemma 4.7, the second equality is by definition of binomials, and the last inequality follows from the fact that for $t > 0$, the function $f(x) = \frac{x}{t+x}$ is increasing.

Now, if we take $t = (2^n-1)(\ell-1)$ where ℓ is the largest integer less than or equal to $1/\varepsilon^2$ we have

$$\mathbb{P}[\psi \in N_\varepsilon(\varphi)] \leq \frac{1}{(1-\varepsilon^2)^t}\left(\frac{2^n-1}{t+2^n-1}\right)^{2^n-1} = \frac{1}{(1-\varepsilon^2)^{(\ell-1)(2^n-1)}}\frac{1}{\ell^{2^n-1}} \leq \left(\frac{e}{\ell}\right)^{2^n-1},$$

where in the last inequality, we use Lemma 4.6. Now, if $\varepsilon^2 < \frac{1}{2}$, then since ℓ is the largest integer that is less than or equal to $1/\varepsilon^2$,

$$\mathbb{P}[\psi \in N_\varepsilon(\varphi)] \leq \left(\frac{e}{\ell}\right)^{2^n-1} \leq \left(\frac{e}{\frac{1}{\varepsilon^2}-1}\right)^{2^n-1} \leq \left(2e\cdot\varepsilon^2\right)^{2^n-1}.$$

□

We can also bound the probability of picking a state $|\psi\rangle$ over Haar-measure that falls into the ε-neighborhood of a set S that is finite.

Corollary 4.8. *Let $\varepsilon > 0$ be a real number such that $\varepsilon^2 < \frac{1}{2}$ and S be a finite set of pure states of n qubits. Then the probability that a Haar random pure state $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ is in $N_\varepsilon(S)$ can be bounded as follows:*

$$\mathbb{P}[\psi \in N_\varepsilon(S)] \leq |S| \cdot \left(2e \cdot \varepsilon^2\right)^{2^n - 1}.$$

Proof. By the union bound,

$$\mathbb{P}[\psi \in N_\varepsilon(S)] \leq \sum_{\varphi \in S} \mathbb{P}[\psi \in N_\varepsilon(\varphi)] \leq |S| \cdot \left(2e \cdot \varepsilon^2\right)^{2^n - 1}.$$

□

4.1.2 Application: Neighborhood of stabilizer states

We discuss an application of the state neighborhood bound in case of S being the set of stabilizer states of n qubits. We will use this fact as an ingredient to prove some no-go theorems for stabilizer testing later.

Lemma 4.9. *There exists $\varepsilon_0 > 0$ such that*

$$\lim_{n \to \infty} \mathbb{P}[\psi \in N_{\varepsilon_0}(\mathit{Stab}(n))] = 0.$$

Proof. Recall that

$$|\mathrm{Stab}(n)| = 2^n \prod_{i=1}^{n} (2^i + 1) \leq 2^n \prod_{i=1}^{n} 2^{i+1} \leq 2^{\frac{1}{2}(n^2+5n)}.$$

Let us take $\varepsilon_0 = \sqrt{1/12}$, then by Corollary 4.8,

$$\mathbb{P}[|\psi\rangle \in N_{\varepsilon_0}(\mathrm{Stab}(n))] \leq 2^{\frac{1}{2}(n^2+5n)} \left(\frac{e}{6}\right)^{2^n - 1} \leq 2^{\frac{1}{2}(n^2+5n)} 2^{-2^n+1}.$$

Hence, as n goes to infinity, the probability goes to 0. □

4.2 Quantum t-designs and no-go theorem

For positive integers n and t, let us denote by $\varrho_{n,t}$ the uniform average of the t-th tensor power of states in $(\mathbb{C}^2)^{\otimes n}$. More precisely,

$$\varrho_{n,t} = \int (|\psi\rangle\langle\psi|)^{\otimes t} d\psi$$

where the integration is over the Haar measure. Similarly, we denote by $\sigma_{n,t}$ the uniform average of the t-th tensor power of states in $\mathrm{Stab}(n)$, the set of stabilizer states of n qubits. More precisely,

$$\sigma_{n,t} = \frac{1}{|\mathrm{Stab}(n)|} \sum_{|S\rangle \in \mathrm{Stab}(n)} (|S\rangle \langle S|)^{\otimes t}.$$

It is known that stabilizer states form a quantum t-design for $t = 2$ and $t = 3$ [KG15].

We show that the fact that stabilizer states constitute a uniform t-design implies a no-go theorem for t copies.

Theorem 4.10 (No-go theorem for 3 copies)**.** *There exists no dimension independent stabilizer testing algorithm with perfect completeness given* 3 *copies.*

Proof. Suppose, for the sake of contradiction, there exists a dimension independent stabilizer testing algorithm $\{\Pi^{(n)}\}_n$. From the first condition (i), we know that $\mathrm{tr}[\Pi^{(n)}\sigma_{n,t}] = 1$. But then since $\sigma_{n,t} = \varrho_{n,t}$, we deduce $\mathrm{tr}[\Pi^{(n)}\varrho_{n,t}] = 1$. But note that for any ε, by linearity of trace,

$$\mathrm{tr}[\Pi^{(n)}\varrho_{n,t}] = \int_{N_\varepsilon(\mathrm{Stab}(n))} \mathrm{tr}[\Pi^{(n)}(|\psi\rangle \langle\psi|)^{\otimes t}] d\psi + \int_{N_\varepsilon(\mathrm{Stab}(n))^C} \mathrm{tr}[\Pi^{(n)}(|\psi\rangle \langle\psi|)^{\otimes t}] d\psi$$

Note that

$$\int_{N_\varepsilon(\mathrm{Stab}(n))} \mathrm{tr}[\Pi^{(n)}(|\psi\rangle \langle\psi|)^{\otimes t}] d\psi \leq \int_{N_\varepsilon(\mathrm{Stab}(n))} d\psi = p_\varepsilon^{(n)}$$

where $p_\varepsilon^{(n)} = \mathbb{P}[\psi \in N_\varepsilon(\mathrm{Stab}(n))]$. Moreover, by condition (ii) for $\Pi^{(n)}$, we have that

$$\int_{N_\varepsilon(\mathrm{Stab}(n))^C} \mathrm{tr}[\Pi^{(n)}(|\psi\rangle \langle\psi|)^{\otimes t}] d\psi \leq \int_{N_\varepsilon(\mathrm{Stab}(n))^C} f(\varepsilon) d\psi = f(\varepsilon)(1 - p_\varepsilon^{(n)}).$$

It follows that for all positive integer n and all $\varepsilon > 0$, we have

$$1 \leq p_\varepsilon^{(n)} + f(\varepsilon)(1 - p_\varepsilon^{(n)}) = p_\varepsilon^{(n)}(1 - f(\varepsilon)) + f(\varepsilon).$$

By Lemma 4.9, there exists $\varepsilon_0 > 0$ such that $\lim p_{\varepsilon_0}^{(n)} = 0$ for n large and thus we must have $f(\varepsilon_0) = 1$, which is a contradiction.

□

In the proof above, we use the fact that $\sigma_{n,3} = \varrho_{n,3}$. We show that if $\sigma_{n,t}$ is asymptotically close to $\varrho_{n,t}$ as n goes to infinity with respect to the trace distance, then a no-go theorem for t copies will also follow.

Theorem 4.11 (Being asymptotically close to t-design implies no-go theorem for t copies)**.** *Let t be a positive integer such that*

$$\lim_{n\to\infty} \|\sigma_{n,t} - \varrho_{n,t}\|_1 = 0.$$

Then, there exists no dimension independent stabilizer testing algorithm with perfect completeness for t copies.

Proof. Suppose t satisfies the condition above. Let us denote

$$\delta(n) = \mathrm{tr}[\Pi^{(n)}\sigma_{n,t}] - \mathrm{tr}[\Pi^{(n)}\varrho_{(n,t)}].$$

Recall that for $\mathrm{tr}[\Pi^{(n)}\sigma_{n,t}] - \mathrm{tr}[\Pi^{(n)}\varrho_{n,t}] \leq \frac{1}{2}\|\sigma_{n,t} - \varrho_{n,t}\|_1$ for all n, and by the condition in the theorem, we have

$$\lim_{n\to\infty} \delta(n) = 0.$$

By similar reasoning as in Theorem 4.10, we have that for every $\varepsilon > 0$ and every positive integer n,

$$1 - \delta(n) = \mathrm{tr}[\Pi^{(n)}\varrho_{n,t}] \leq p_\varepsilon^{(n)}(1 - f(\varepsilon)) + f(\varepsilon).$$

Now since $\lim_{n\to\infty}\delta(n) = 0$, together with Lemma 4.9, there exists $\varepsilon_0 > 0$ such that $f(\varepsilon_0) = 0$, a contradiction. □

4.3 No-go theorem for 4 copies

In this section, we prove the no-go theorem for 4 copies[1]. According to Theorem 4.11, it suffices to prove that

$$\lim_{n\to\infty} \|\sigma_{n,4} - \varrho_{n,4}\|_1 = 0.$$

There is a formula to compute $\sigma_{n,4}$ in [ZKGG16] and $\sigma_{n,t}$ for any t in [GNW17]. We will use results from [GNW17] since its most general result might be applicable to the no-go theorem for 5 copies as we will discuss briefly in Section 4.4.

To every subspace $T \subseteq \mathbb{Z}_2^t \oplus \mathbb{Z}_2^t$, we consider an operator $r(T)$ on $(\mathbb{C}^2)^{\otimes t}$ defined by

$$r(T) = \sum_{(\mathbf{x},\mathbf{y})\in T} |\mathbf{x}\rangle\langle\mathbf{y}|$$

[1] I would like to thank Michael Walter and Sepehr Nezami for the discussion about the proof strategy.

where $|\mathbf{x}\rangle = |x_1, \ldots, x_t\rangle$ is a computational basis vector corresponding to $\mathbf{x} \in \mathbb{Z}_2^t$. We can also define an operator $R(T)$ on $((\mathbb{C}^2)^{\otimes t})^{\otimes n}$ by $R(T) = r(T)^{\otimes n}$.

We define a bilinear form $\beta : \mathbb{Z}_2^t \oplus \mathbb{Z}_2^t \times \mathbb{Z}_2^t \oplus \mathbb{Z}_2^t \to \mathbb{Z}_2$ defined by

$$\beta((\mathbf{x}, \mathbf{y}), (\mathbf{x}', \mathbf{y}')) = \mathbf{x} \cdot \mathbf{x}' + \mathbf{y} \cdot \mathbf{y}'$$

for all $(\mathbf{x}, \mathbf{y}), (\mathbf{x}', \mathbf{y}') \in \mathbb{Z}_2^t \oplus \mathbb{Z}_2^t$. A subspace $T \subseteq \mathbb{Z}_2^t \oplus \mathbb{Z}_2^t$ is called *Lagrangian subspace with respect to* β if for all $(\mathbf{x}, \mathbf{y}), (\mathbf{x}', \mathbf{y}')$, $\beta((\mathbf{x}, \mathbf{y}), (\mathbf{x}', \mathbf{y}')) = 0$ and $\dim(T) = t$. We define $\Sigma_{t,t}$ as the set of Lagrangian subspaces of $T \subseteq \mathbb{Z}_2^t \oplus \mathbb{Z}_2^t$ with respect to bilinear form β which also satisfy the following condition: for all $(\mathbf{x}, \mathbf{y}) \in T$:

$$\sum_{i=1}^{t} x_i \equiv \sum_{i=1}^{t} y_i \pmod 4,$$

where x_i and y_i are the representatives in $\{0, 1\}$ of the components of $\mathbf{x}$ and $\mathbf{y}$. We define $\Delta = \{(\mathbf{x}, \mathbf{x}) : \mathbf{x} \in \mathbb{Z}_2^t\}$. We have $\Delta \in \Sigma_{t,t}$ and $R(\Delta) = I$. The number of elements of $\Sigma_{t,t}$ is given by

$$|\Sigma_{t,t}| = \prod_{i=0}^{t-2} (2^i + 1). \tag{4.12}$$

We refer to [GNW17] for the proof. For $T \in \Sigma_{t,t}$, $R(T)$ are the basis of the commutants of t-th tensor power of the Clifford group $\mathcal{C}_n$ which is the main result of [GNW17].

With symmetry, we can understand the structure of $\Sigma_{t,t}$ better. We define a natural symmetry group for $\Sigma_{t,t}$. An operator O of $\mathbb{Z}_2^t$ is called *orthogonal* if it satisfies $OO^\top = O^\top O = I$. Define O_t to be the set of orthogonal operators O on $\mathbb{Z}_2^t$ which also satisfy the following condition: for all $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_2^t$ such that $\mathbf{x} = O\mathbf{y}$,

$$\sum_{i=1}^{t} x_i \equiv \sum_{i=1}^{t} y_i \pmod 4.$$

O_t forms a group. It is easy to see that the permutation group $S_t \subseteq O_t$ for all t. Indeed, for $t \leq 5$, $S_t = O_t$. Interestingly, O_6 has more elements than S_6, since S_6 contains the anti-identity operator

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

Next, we define the action of $O \in O_t$ on elements of $\Sigma_{t,t}$. It has left action and right action. The *left action of* O *on* T is defined as follows:

$$OT = \{(O\mathbf{x}, \mathbf{y}) : (\mathbf{x}, \mathbf{y}) \in T\}.$$

Similarly, the *right action of* O *on* T is defined as

$$TO = \{(\mathbf{x}, O^\top \mathbf{y}) : (\mathbf{x}, \mathbf{y}) \in T\}.$$

The action makes sense since for all $O \in O_t$ and $T \in \Sigma_{t,t}$, OT and TO are both in $\Sigma_{t,t}$ again. In addition, the operators $R(T)$ also behave nicely. When $T \in \Sigma_{t,t}$ and $O, O' \in O_t$, we have that

$$R(O)R(T)R(O') = R(OTO'),$$

where

$$R(O) := R(O\Delta) = \left(\sum_{\mathbf{x}} |O\mathbf{x}\rangle \langle \mathbf{x}| \right)^{\otimes n}.$$

Now, $\Sigma_{t,t}$ can be decomposed into disjoint cosets with respect to the left and the right action of O_t:

$$\Sigma_{t,t} = \bigcup_{i=1}^{k} O_t T^{(i)} O_t$$

for some $T^{(i)}$ in $\Sigma_{t,t}$ that has different orbits with respect to left and right action of O_t. We can always choose $T^{(1)} = \Delta$ and note that the orbit $O_t \Delta O_t = O_t \Delta$.

With this decomposition, for small t, we can understand the operators $R(T)$ for $T \in \Sigma_{t,t}$ in a way that it is useful for our computation of $\sigma_{n,t}$. The formula for $\sigma_{n,t}$ is given by:

$$\sigma_{n,t} = \frac{1}{N_t} \sum_{T \in \Sigma_{t,t}} R(T) \tag{4.13}$$

where

$$N_t = 2^n \prod_{i=0}^{t-2} (2^n + 2^i),$$

where the equality in equation 4.13 is up to permutation of tensor factors $((\mathbb{C}^2)^{\otimes t})^{\otimes n} \cong ((\mathbb{C}^2)^{\otimes n})^{\otimes t}$. We refer to [GNW17] for the proof of this statement.

Consider the following subspace of $\mathbb{Z}_2^4 \oplus \mathbb{Z}_2^4$

$$T_4 = \left[\begin{array}{cccc|cccc} 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right] \tag{4.14}$$

where the rows are the basis of T_4 and each row represents a basis element $(\mathbf{x}, \mathbf{y})$ where $\mathbf{x}$ is on the left of the middle line and $\mathbf{y}$ is on the right of the middle line. Every element of T_4 is of the form and only of the form $(\mathbf{x}, \mathbf{x})$ or $(\mathbf{x}, \overline{\mathbf{x}})$ where $x_1 + x_2 + x_3 + x_4 \equiv 0 \pmod 2$. Here, for $\mathbf{x} \in \mathbb{Z}_2^4$, $\overline{\mathbf{x}}$ denotes the string $\mathbb{Z}_2^4$ with all the bits flipped. For example, $\overline{1010} = 0101$.

It is easy to show that $\pi T_4 = T_4 \pi$ for all $\pi \in S_4$, and hence $R(T_4)$ commutes with all operators $R(\pi)$. Moreover, $R(T_4)$ is proportional to a projector operator.

Lemma 4.15. *$R(T_4)^2 = 2^n \cdot R(T_4)$.*

Proof. Since $R(T_4) = r(T_4)^{\otimes n}$, it suffices to show that $r(T_4)^2 = 2 \cdot r(T_4)$. Let $E \subseteq \mathbb{Z}_2^4$ be the set of all $\mathbf{x} \in \mathbb{Z}_2^4$ such that $x_1 + x_2 + x_3 + x_4 \equiv 0 \pmod 2$. We can write

$$r(T_4) = \sum_{\mathbf{x} \in E} |\mathbf{x}\rangle \langle \mathbf{x}| + \sum_{\mathbf{x} \in E} |\mathbf{x}\rangle \langle \overline{\mathbf{x}}|,$$

and hence

$$\begin{aligned} r(T_4)^2 &= \sum_{\mathbf{x},\mathbf{y} \in E} |\mathbf{x}\rangle \langle \mathbf{x}|\mathbf{y}\rangle \langle \mathbf{y}| + \sum_{\mathbf{x},\mathbf{y} \in E} |\mathbf{x}\rangle \langle \mathbf{x}|\mathbf{y}\rangle \langle \overline{\mathbf{y}}| + \sum_{\mathbf{x},\mathbf{y} \in E} |\mathbf{x}\rangle \langle \overline{\mathbf{x}}|\mathbf{y}\rangle \langle \mathbf{y}| + \sum_{\mathbf{x},\mathbf{y} \in E} |\mathbf{x}\rangle \langle \overline{\mathbf{x}}|\mathbf{y}\rangle \langle \overline{\mathbf{y}}| \\ &= \sum_{\mathbf{x} \in E} |\mathbf{x}\rangle \langle \mathbf{x}| + \sum_{\mathbf{x} \in E} |\mathbf{x}\rangle \langle \overline{\mathbf{x}}| + \sum_{\mathbf{x} \in E} |\mathbf{x}\rangle \langle \overline{\mathbf{x}}| + \sum_{\mathbf{x} \in E} |\mathbf{x}\rangle \langle \mathbf{x}| \\ &= 2 \cdot r(T_4), \end{aligned}$$

as desired. □

Observe that $R(T_4)^2 = 2^n \cdot R(T_4)$. There are exactly 4 elements of S_n that stabilizes T_4 and they are the Klein-four group $K_4 \subseteq S_4$, namely $K_4 = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$. The orbit of T_4 with respect to the left and right action of O_t is given by πT_4 for $\pi \in \{\mathrm{id}, (12), (13), (14), (123), (132)\}$ giving in total 6 elements in $S_4 T_4 S_4$. Together with $S_4 \Delta$ which has size 24, this gives the whole $\Sigma_{4,4} = S_4 \Delta \cup S_4 T_4 S_4$ which has size 30 from equation 4.12.

The set of the commutants of the 4-th tensor power of the Clifford group in $((\mathbb{C}^2)^{\otimes n})^{\otimes 4}$ is spanned by

$$\{R(\pi) : \pi \in S_4\} \cup \{R(\pi) R(T_4) : \pi \in S_4\}.$$

Restricted to $\mathrm{Sym}^4((\mathbb{C}^2)^{\otimes n})$, the commutants are spanned by only two operators, namely $I_{\mathrm{Sym}^4((\mathbb{C}^2)^{\otimes n})}$ and $I_{\mathrm{Sym}^4((\mathbb{C}^2)^{\otimes n})}R(T_4)_{\mathrm{Sym}^4((\mathbb{C}^2)^{\otimes n})}$.

Suppose $\mathrm{Sym}^4((\mathbb{C}^2)^{\otimes n})$ can be decomposed as

$$\mathrm{Sym}^4((\mathbb{C}^2)^{\otimes n}) = \bigoplus_i \mathcal{H}_i \otimes \mathbb{C}^{m_i}$$

where the $\mathcal{H}_i$'s are inequivalent irreducible representations of the Clifford group $\mathcal{C}_n$ and m_i are the multiplicities of $\mathcal{H}_i$. By Schur's lemma, the dimension of the intertwiner is given by the formula $\sum_i m_i^2$. Since the dimension of the commutants of 4-th tensor power of the Clifford group $\mathcal{C}_n$ in $\mathrm{Sym}^4((\mathbb{C}^2)^{\otimes n})$ is 2, it follows that $\mathrm{Sym}^4((\mathbb{C}^2)^{\otimes n})$ decomposes into two inequivalent irreducible representations $\mathrm{Sym}^4((\mathbb{C}^2)^{\otimes n}) = \mathcal{H}_1 \oplus \mathcal{H}_2$ with respect to the Clifford group $\mathcal{C}_n$.

Let P_1 and P_2 be the projections onto $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively. Note that

$$\varrho_{n,4} = \beta I_{\mathrm{Sym}^4((\mathbb{C}^2)^{\otimes n})} = \beta P_1 + \beta P_2$$

where

$$\beta^{-1} = \dim(\mathrm{Sym}^4((\mathbb{C}^2)^{\otimes n})) = \frac{(2^n+3)(2^n+2)(2^n+1)2^n}{24}. \tag{4.16}$$

Note that $P_1^2 = P_1, P_2^2 = P_2$, and $P_1P_2 = P_2P_1 = 0$.

Using formula 4.13, we also have

$$\sigma_{n,4} = \beta_1 P_1 + \beta_2 P_2$$

for some β_1, β_2. Then for every positive integer k,

$$\sigma_{n,4}^k = \beta_1^k P_1 + \beta_2^k P_2. \tag{4.17}$$

We will compute β_1 and β_2 as follows. According the formula 4.13, we know that $\sigma_{n,4} = (A+B)/N_4$ where

$$A = \sum_{\pi \in S_4} R(\pi) \tag{4.18}$$

$$B = \sum_{T \in S_4 T_4 S_4} R(T). \tag{4.19}$$

We prove the following facts about operators A and B.

Lemma 4.20. *Let A and B be operators that are defined in equation 4.18 and equation 4.19. Then:*

(i) $A^2 = 24\cdot A$,

(ii) $A\cdot B = B\cdot A = 24\cdot B$, *and*

(iii) $B^2 = 6\cdot 2^n\cdot B$.

Proof. (i) Note that for all $\pi \in S_4$, $R(\pi)A = A$ so $A^2 = 24A$. (ii) Note that for all $\pi \in S_4$, $R(\pi)B = BR(\pi) = B$ so $A\cdot B = B\cdot A = 24\cdot B$. (iii) Note that $R(T_4)^2 = 2^n\cdot R(T_4)$ by Lemma 4.15 and that $R(\pi)R(T_4) = R(T_4)R(\pi)$ for all $\pi \in S_4$. Hence, $B^2 = 6\cdot 2^n\cdot B$ since for □

This way, $(A+B)^k = a_k A + b_k B$ for some $\{a_k\}$ and $\{b_k\}$. It is easy to prove by induction that the sequence $\{a_k\}$ and $\{b_k\}$ satisfy

$$\begin{aligned} a_{k+1} &= 24a_k \\ b_{k+1} &= 24a_k + (24 + 6\cdot 2^n)b_k \end{aligned}$$

with $a_1 = b_1 = 1$. It is also easy to see by induction that $\{a_k\}$ and $\{b_k\}$ have closed formulas

$$\begin{aligned} a_k &= 24^{k-1} \\ b_k &= \frac{(24 + 6\cdot 2^n)^k - 24^k}{6\cdot 2^n}. \end{aligned}$$

Rearranging the term, we obtain

$$\begin{aligned} \sigma_{n,4}^k &= \frac{24^k}{N_4^k} A + \frac{(24 + 6\cdot 2^n)^k - 24^k}{N_4^k\cdot 6\cdot 2^n} B \\ &= \left(\frac{24}{N_4}\right)^k \left(\frac{A}{24} - \frac{B}{6\cdot 2^n}\right) + \left(\frac{24 + 6\cdot 2^n}{N_4}\right)^k \frac{B}{6\cdot 2^n}. \end{aligned}$$

Letting

$$P_1 = \frac{A}{24} - \frac{B}{6\cdot 2^n} \qquad \text{and } P_2 = \frac{B}{6\cdot 2^n},$$

it is easy to verify that P_1 and P_2 are orthogonal projectors. Comparing with equation 4.17, we find

$$\beta_1 = \frac{24}{2^n(2^n+1)(2^n+2)(2^n+4)} \text{ and } \beta_2 = \frac{6}{2^n(2^n+1)(2^n+2)}, \tag{4.21}$$

where the indices are just assigned arbitrarily.

Next, we denote $d_1 = \dim(\mathcal{H}_1)$ and $d_2 = \dim(\mathcal{H}_2)$, we can solve the following system

$$\begin{aligned} \beta_1 d_1 + \beta_2 d_2 &= \mathrm{tr}[\sigma_{n,4}] = 1 \\ d_1 + d_2 &= \dim(\mathrm{Sym}^4((\mathbb{C}^2)^{\otimes n}) = \binom{2^n+3}{4}, \end{aligned}$$

to obtain

$$
\begin{aligned}
d_1 &= \frac{(2^n+4)(2^n+2)(2^n+1)(2^n-1)}{24}, \\
d_2 &= \frac{(2^n+2)(2^n+1)}{6}.
\end{aligned}
$$

Theorem 4.22 ($\sigma_{n,4}$ is asymptotically close to a 4-design)**.** $\lim_{n\to\infty} \|\sigma_{n,4} - \varrho_{n,4}\|_1 = 0$.

Proof. We compute using coefficients that we find in equation 4.16 and equation 4.21. We see that

$$
\begin{aligned}
\|\sigma_{n,4} - \varrho_{n,4}\|_1 &= \|(\beta_1 - \beta^{-1})P_1 + (\beta_2 - \beta^{-1})P_2\|_1 \\
&= |\beta_1 - \beta^{-1}|d_1 + |\beta_2 - \beta^{-1}|d_2 \\
&= 2\left|\frac{1}{2^n} - \frac{4}{2^n(2^n+3)}\right| \\
&\leq 2\cdot \frac{1}{2^n} = 2^{-n+1},
\end{aligned}
$$

and hence the limit is 0 as n gets larger. □

Hence, we have proved a no-go theorem for $t = 4$ copies.

Corollary 4.23 (No-go theorem for 4 copies)**.** *There exists no dimension independent stabilizer testing algorithm with perfect completeness for* 4 *copies.*

4.4 Dimension independent stabilizer testing with 5 copies

We have not found a no-go theorem for 5 copies nor a stabilizer testing algorithm that only use 5 copies of the state. But if one believes that no-go theorem for 5 copies hold, one can try to work with the same proof strategy as before in proving the no-go theorem for 4 copies with the same goal, namely to show that average 5 copies is close to a quantum 5-design with some techniques from representation theory.

There are some similar results that we found in the case of 4 copies and 5 copies. For example, we know that the group of orthogonal operators O_5 in $\mathbb{Z}_2^5$ coincides Moreover, we can decompose $\Sigma_{5,5}$ into two cosets with respect to the left and right action of O_5, namely

$$\Sigma_{5,5} = S_5 \cup S_5 T_5 S_5$$

where

$$T_5 = \left[\begin{array}{ccccc|ccccc} 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{array}\right].$$

Interestingly, we can see that $r(T_5) = r(T_4) \otimes I$ where $T_4 \in \Sigma_{4,4}$ from equation 4.14.

Otherwise, one should be able to find a dimension independent stabilizer testing algorithm with only 5 copies. We leave this open question as a direction for further research in Chapter 6.

Chapter 5

Stabilizer testing protocol

Given access to 6 copies of $|\psi\rangle$ that is ε-far from any stabilizer states, the 6-copy stabilizer testing algorithm in [GNW17] is perfectly complete, i.e. makes only one-sided error, but with possibly high probability. But since the algorithm is perfectly complete, we can do error reduction [AB09]. A natural way to do it is by running the algorithm k times and accept if and only if all k instances accept. This requires $6 \cdot k$ copies and the probability of error will be reduced to $(1 - \varepsilon^2/4)^k$. We attempt to answer the following question.

> **Question** $(*)$**.** If we have access to a large amount of copies of a state ψ, is there a better *protocol* to test whether ψ is a stabilizer state (or ε-far from any stabilizer state) than repeating the 6-copy algorithm several times?

By *protocol*, we mean a new algorithm that is built from some primitives with a set of parameters that determines how the primitives in the algorithm are used. The parameters determine the amount of resources needed as well as the performance of the algorithm.

One obvious protocol would be the one that repeats the 6-copy algorithm k times. This protocol can be described as follows: (1) perform Bell sampling $2k$ times; label the outcomes $\mathbf{x}_0, \ldots, \mathbf{x}_{2k-1}$, (2) compute the Bell differences $\mathbf{a}_i = \mathbf{x}_{2i} + \mathbf{x}_{2i+1}$ for $i = 0, 1, \ldots, k-1$, (3) test whether $|\psi\rangle$ is an eigenvector of $W_{\mathbf{a}_i}$ for every $i = 0, \ldots, k-1$ (by performing Weyl measurement twice on two independent copies of $|\psi\rangle$), and accept iff all tests accept. we will give a family of natural protocols that has three parameters:

- the number of times Bell sampling is performed,
- a specification of how to extract the differences $\mathbf{x} + \mathbf{y}$ of two Bell sampling outcomes,

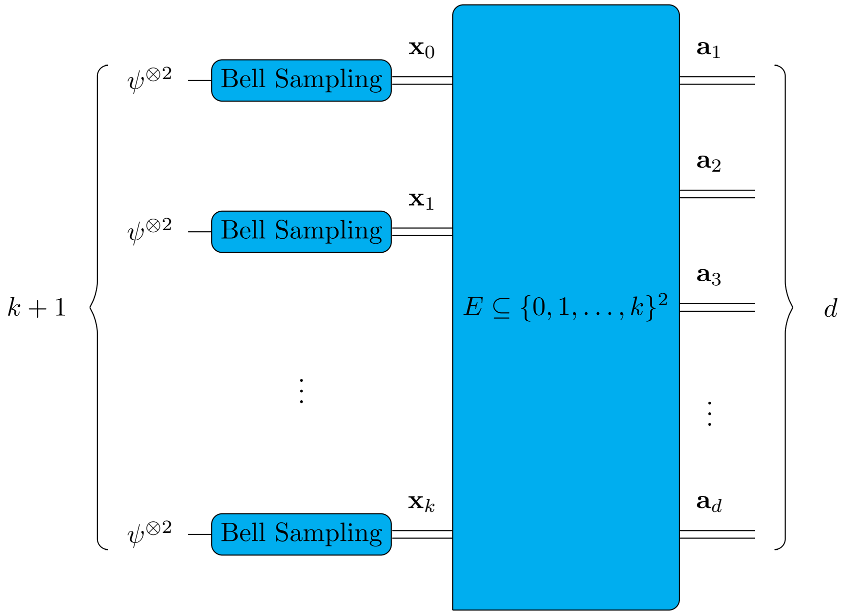

Figure 5.1: A Bell difference extraction parameterized by $k \in \mathbb{N}$ and $E \subseteq [k]^2$, with $|E| = d$.

- the number of Weyl measurements performed for each Weyl $W_{\mathbf{x}+\mathbf{y}}$ test.

We will define this family of stabilizer testing protocols more formally in Section 5.1. In Section 5.2, we will prove a lemma that helps us analyzing the protocols of the form (k, ℓ, E). This lemma is a generalization of Lemma 3.16 that we used in Chapter 3 to prove an alternative analysis of the 6-copy algorithm. In Section 5.3, we analyze some interesting stabilizer testing protocols. We prove an upper bound of the error probability for each protocol which depends on the parameters of the protocol. In Section 5.4, we will use the bound that we have obtained to see how each parameter affects the bound to understand the performance of this family of stabilizer testing protocols and answer the Question $(*)$.

5.1 A natural stabilizer testing protocol

For every positive integer k, let $[k] = \{0, 1, \ldots, k\}$. We define a generalization of Bell difference sampling [GNW17] as follows.

Definition 5.1 (Bell difference extraction)**.** *Let $k \in \mathbb{N}$. Suppose $E \subseteq [k]^2$ is non-empty and $|E| = d$. We define* Bell difference extraction (k, E) *as:*

1. *performing $k+1$ rounds of Bell sampling on $k+1$ independent copies of $|\psi\rangle^{\otimes 2}$, let the outcomes be $\mathbf{x}_0, \ldots, \mathbf{x}_k$, and*

2. *output the differences $\mathbf{x}_i + \mathbf{x}_j$ for all $(i, j) \in E$.*

See Figure 5.1 for an illustration. An example of a Bell difference extraction is the original Bell difference sampling with $k = 1$ and $E = \{(0, 1)\}$. It is desirable that the domain of E covers the whole set $[k]$.

Once we have defined Bell difference extraction, we can define a family of stabilizer testing protocol parameterized by positive integers k and ℓ and a set $E \subseteq [k]^2$.

Definition 5.2 (Stabilizer testing protocol (k, ℓ, E))**.** *Let k and ℓ be positive integers with $\ell > 1$. Suppose $E \subseteq [k]^2$ is non-empty and $|E| = d$. We define* stabilizer testing protocol *(k, ℓ, E) as performing Bell difference extraction (k, E) on $(k+1)$ independent copies of $\psi^{\otimes 2}$ and for each outcome $\mathbf{a}$ of Bell difference extraction, performing eigenvector test corresponding to Weyl operator $W_{\mathbf{a}}$ with parameter ℓ on independent copies of ψ. The protocol accepts iff the every Weyl eigenvector test accepts.*

See Figure 5.2 for an illustration. Note that the number of copies that is used for a protocol (k, ℓ, E) is $2\cdot(k+1) + d\ell$.

It is easy to see that the protocol that just repeats the 6-copy algorithm is the stabilizer testing protocol that is obtained from setting the parameter $\ell = 2$ and $E = \{(2i, 2i+1) : i = 0, 1, \ldots, k-1\}$. Note that in this protocol, k denotes the number of repetitions of the 6-copy algorithm.

If $|\psi\rangle$ is a stabilizer state, then Bell difference extraction will always give an outcome $\mathbf{x} \in \{0, 1\}^{2n}$ such that $W_{\mathbf{x}}$ has $|\psi\rangle$ as an eigenvector. Hence, by similar argument in the analysis of the 6-copy algorithm, we obtain the following lemma.

Lemma 5.3. *For every positive integer k and ℓ with $\ell > 1$, and any non-empty subset $E \subseteq [k]^2$, protocol (k, ℓ, E) accepts any stabilizer state with probability* 1.

If $|\psi\rangle$ is not a stabilizer state, it is not obvious how the parameters k, ℓ, and E will affect the probability that the stabilizer testing protocol (k, ℓ, E) accepts $|\psi\rangle$. We will analyze some interesting examples of stabilizer testing protocol (k, ℓ, E) in Section 5.3.

5.2 Bell sampling distribution bound

We prove the following lemma.

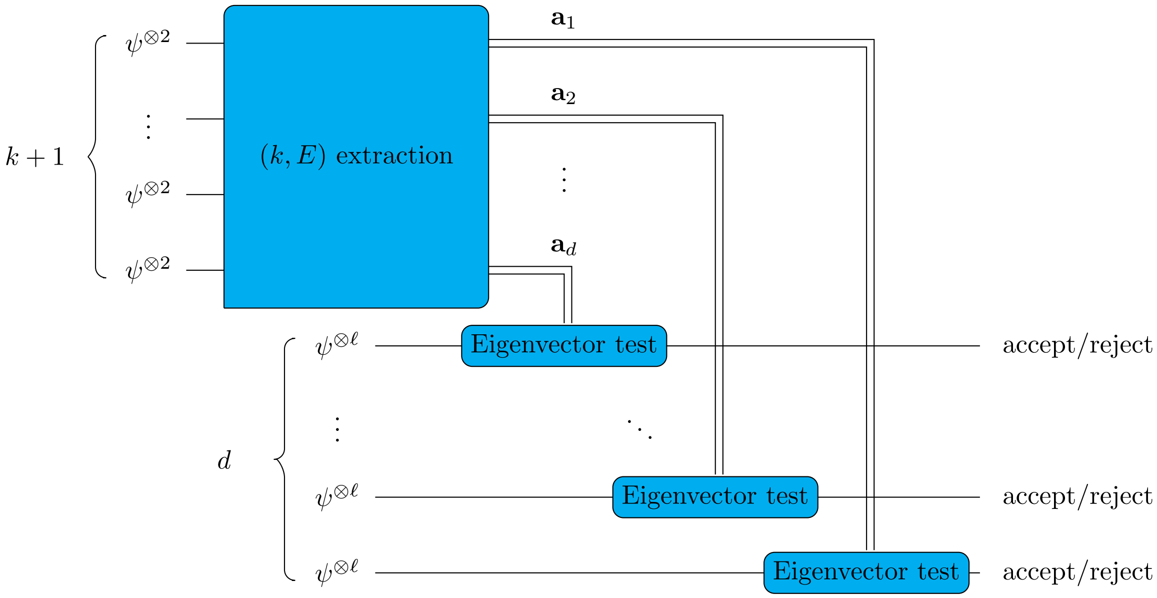

Figure 5.2: A (k, ℓ, E) protocol.

Lemma 5.4. *Let ψ be a pure state of n qubits. For any non-negative integers k and ℓ and any $\mathbf{a}_1, \ldots, \mathbf{a}_{k+\ell} \in \mathbb{Z}_2^n \oplus \mathbb{Z}_2^n$, we have that*

$$\sum_{\mathbf{x}} t_\psi(\mathbf{x}+\mathbf{a}_1) \ldots t_\psi(\mathbf{x}+\mathbf{a}_k) p_\psi(\mathbf{x}+\mathbf{a}_{k+1}) \ldots p_\psi(\mathbf{x}+\mathbf{a}_{k+\ell}) \leq \sum_{\mathbf{x}} p_\psi(\mathbf{x})^{k+\ell}. \tag{5.5}$$

Proof. By Proposition 3.15, the right hand side of the inequality can be rewritten as

$$\begin{aligned}
\text{RHS} &= 2^{-n(k+\ell)} \sum_{\mathbf{x}} \sum_{\mathbf{y}_1, \ldots, \mathbf{y}_{k+\ell}} (-1)^{\sum_{i=1}^{k+\ell} [\mathbf{x}, \mathbf{y}_i]} \prod_{i=1}^{k+\ell} c_\psi(\mathbf{y}_i)^2 \\
&= 2^{-n(k+\ell)} \sum_{\mathbf{y}_1, \ldots, \mathbf{y}_{k+\ell}} \prod_{i=1}^{k+\ell} c_\psi(\mathbf{y}_i)^2 \sum_{\mathbf{x}} (-1)^{[\mathbf{x}, \sum_{i=1}^{k+\ell} \mathbf{y}_i]} \\
&= 2^{-n(k+\ell-2)} \sum_{\mathbf{y}_1 + \cdots + \mathbf{y}_{k+\ell} = 0} \prod_{i=1}^{k+\ell} p_\psi(\mathbf{y}_i),
\end{aligned}$$

while the left hand side can be rewritten as

$$\begin{aligned}\text{LHS} &= 2^{-n(k+\ell)} \sum_{\mathbf{x}} \sum_{\mathbf{y}_1,\dots \mathbf{y}_{k+\ell}} (-1)^{\sum_{i=1}^{k} \pi(\mathbf{y}_i) + \sum_{i=1}^{k+\ell} [\mathbf{x}+\mathbf{a}_i, \mathbf{y}_i]} \prod_{i=1}^{k+\ell} c_\psi(\mathbf{y}_i)^2 \\ &= 2^{-n(k+\ell)} \sum_{\mathbf{y}_1,\dots \mathbf{y}_{k+\ell}} (-1)^{\sum_{i=1}^{k} \pi(\mathbf{y}_i) + \sum_{i=1}^{k+\ell} [\mathbf{a}_i, \mathbf{y}_i]} \prod_{i=1}^{k+\ell} p_\psi(\mathbf{y}) \sum_{\mathbf{x}} (-1)^{[\mathbf{x}, \sum_{i=1}^{k+\ell} \mathbf{y}_i]} \\ &= 2^{-n(k+\ell-2)} \sum_{\mathbf{y}_1+\dots+\mathbf{y}_{k+\ell}=0} (-1)^{\sum_{i=1}^{k} \pi(\mathbf{y}_i) + \sum_{i=1}^{k+\ell} [\mathbf{a}_i, \mathbf{y}_i]} \prod_{i=1}^{k+\ell} c_\psi(\mathbf{y}_i)^2 .\end{aligned}$$

Thus, RHS $\geq$ LHS. □

We discuss some immediate consequences of this inequality. First of all, for the case $k = 0$, the inequality 5.5 becomes

$$\sum_{\mathbf{x}} p_\psi(\mathbf{x} + a_1) \dots p_\psi(\mathbf{x} + \mathbf{a}_\ell) \leq \sum_{\mathbf{x}} p_\psi(\mathbf{x})^\ell$$

which can also be seen as an immediate consequence of rearrangement inequality that we will also discuss later as a lemma in the next section. Interestingly, a similar upper bound also holds for probability distribution t_ψ by taking $l = 0$:

$$\sum_{\mathbf{x}} t_\psi(\mathbf{x} + a_1) \dots t_\psi(\mathbf{x} + \mathbf{a}_k) \leq \sum_{\mathbf{x}} p_\psi(\mathbf{x})^k .$$

It would be nice if we can find a more intuitive explanation of why these inequalities are true which probably requires a better understanding of characteristic distribution of pure states ψ [Woo87].

Another consequence of Bell sampling distribution bound that will be useful later is the following.

Corollary 5.6. *Let Q be a polynomial with non-negative coefficients. For every positive integer k and every $\mathbf{a}_0, \dots, \mathbf{a}_k \in \mathbb{Z}_2^n \oplus \mathbb{Z}_2^n$, we have*

$$\sum_{\mathbf{x}} t_\psi(\mathbf{x} + \mathbf{a}_0) Q(p_\psi(\mathbf{x} + \mathbf{a}_1)) \dots Q(p_\psi(\mathbf{x} + \mathbf{a}_k)) \leq \sum_{\mathbf{x}} p_\psi(\mathbf{x}) Q(p_\psi(\mathbf{x}))^k .$$

Proof. Let $Q(x) = q_0 + q_1 x + \dots + q_m x^m$ where $q_0, \dots, q_m$ are non-negative real numbers. For any non-negative integers $m_1, \dots, m_k$, by applying Lemma 5.4 and by the fact that all the q_i's are non-negative, we have that

$$q_{m_1} \dots q_{m_k} \sum_{\mathbf{x}} t_\psi(\mathbf{x} + \mathbf{a}_0) p_\psi(\mathbf{x} + \mathbf{a}_1)^{m_1} \dots p_\psi(\mathbf{x} + \mathbf{a}_k)^{m_k} \leq \sum_{\mathbf{x}} q_{m_1} \dots q_{m_k} p_\psi(\mathbf{x})^{1+m_1+\dots+m_k} .$$

Summing over all non-negative integers $m_1, \dots, m_k$ that satisfy $m_1, \dots, m_k \leq m$, we obtain the desired result. □

5.3 Stabilizer testing protocols

5.3.1 Protocol with $k = 1$

The only interesting protocol with $k = 1$ is $E = \{(0, 1)\}$.

The probability of accepting a state ψ is

$$p_{\text{accept}} = \sum_{\mathbf{a}} q_\psi(\mathbf{a}) w_{\psi,\ell}(\mathbf{a}),$$

where $q_\psi(\mathbf{a})$ is the probability distribution of obtaining outcome $\mathbf{a}$ from performing Bell difference sampling on $\psi^{\otimes 4}$ and $w_{\psi,\ell}$ is the probability of being accepted by the Weyl eigenvector test with parameter ℓ.

We begin by analyzing protocols with one Bell difference sampling and several Weyl measurement. For every integer $\ell > 1$, we define a function $f_\ell : [0, 1] \to [0, 1]$ defined by

$$f_\ell(t) = \left(\frac{1 + \sqrt{t}}{2}\right)^\ell + \left(\frac{1 - \sqrt{t}}{2}\right)^\ell,$$

for all $t \in [0, 1]$. It is easy to see that f_ℓ is increasing for $t \in [0, 1]$. Indeed, $f_\ell(t)$ is a polynomial in t with non-negative coefficients. See Figure 5.3 for an illustration. Also, recall that for any pure state ψ of n qubits,

$$w_{\psi,\ell}(\mathbf{a}) = f_\ell(2^n p_\psi(\mathbf{a})).$$

Finally, we define a sequence $\{\gamma_\ell\}_{\ell>1}$ as follows:

$$\gamma_\ell = f_\ell(0.5), \text{ for } \ell = 2, 3, 4, \ldots. \tag{5.7}$$

We now prove an upper bound for the probability that this protocol accepts a non-stabilizer state. The proof uses rearrangement inequality.

Lemma 5.8 (Rearrangement Inequality)**.** *Let $x_1, x_2, \ldots, x_n$ and $y_1, \ldots, y_n$ be $2n$ real numbers such that*

$$x_1 \le x_2 \le \cdots \le x_n \text{ and } y_1 \le y_2 \le \cdots \le y_n.$$

For any permutation $\sigma \in S_n$, then

$$x_1 y_{\sigma(1)} + x_2 y_{\sigma(2)} + \cdots + x_n y_{\sigma(n)} \le x_1 y_1 + \cdots + x_n y_n.$$

Theorem 5.9. *Protocol (k, ℓ, E) with $k = 1$ and $E = \{(0, 1)\}$ will accept any state ψ of n qubits that is ε-far from any stabilizer state with probability at most $1 - (1 - \gamma_\ell)\varepsilon^2$.*

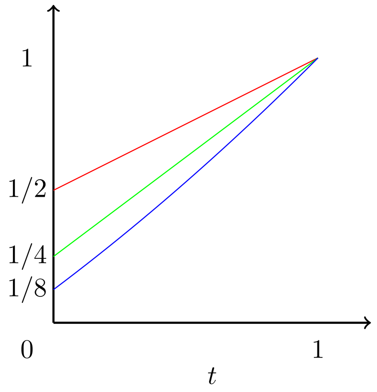

Figure 5.3: A plot of $f_\ell(t)$ with $\ell = 2, 3, 4$ respectively in red, green, and blue.

Proof. Recall that f_ℓ is an increasing function.

$$\begin{aligned} p_{\text{accept}} &= \sum_{\mathbf{a}} q_\psi(\mathbf{a}) f_\ell(2^n p_\psi(\mathbf{a})) = \sum_{\mathbf{x}} \sum_{\mathbf{a}} p_\psi(\mathbf{x}) p_\psi(\mathbf{x}+\mathbf{a}) f_\ell(2^n p_\psi(\mathbf{a})) \\ &= \sum_{\mathbf{x}} p_\psi(\mathbf{x}) \sum_{\mathbf{a}} p_\psi(\mathbf{x}+\mathbf{a}) f_\ell(2^n p_\psi(\mathbf{a})) \\ &\leq \sum_{\mathbf{x}} p_\psi(\mathbf{x}) \sum_{\mathbf{a}} p_\psi(\mathbf{a}) f_\ell(2^n p_\psi(\mathbf{a})) \\ &= \sum_{\mathbf{a}} p_\psi(\mathbf{a}) f_\ell(2^n p_\psi(\mathbf{a})), \end{aligned}$$

where the inequality holds by Lemma 5.8. This lemma can be applied since f_ℓ is an increasing function. Consider the set $M_0 = \{\mathbf{x} \in \{0,1\}^{2n} : 2^n p_\psi(\mathbf{x}) > \frac{1}{2}\}$ again as in the proof for the 6-copy algorithm. By Markov's inequality,

$$1 - \sum_{\mathbf{a} \in M_0} p_\psi(\mathbf{a}) = \mathbb{P}\left[1 - f_\ell(2^n p_\psi(\mathbf{a})) > 1 - f_\ell(1/2)\right] \leq \frac{\mathbb{E}[1 - f_\ell(2^n p_\psi(\mathbf{a}))]}{1 - f_\ell(\frac{1}{2})} \leq \frac{1 - p_{\text{accept}}}{1 - \gamma_\ell},$$

where the first inequality is by Markov's inequality and the second inequality is by our previous observation. Note that the probability is over By a similar argument as in the analysis of the 6-copy algorithm,

$$\max_S |\langle S|\psi\rangle|^2 \geq \sum_{\mathbf{a} \in M_0} p_\psi(\mathbf{a}) \geq 1 - \frac{1 - p_{\text{accept}}}{1 - \gamma_\ell}.$$

Thus, if ψ satisfies $\max_S |\langle S|\psi\rangle|^2 \leq 1 - \varepsilon^2$, we obtain $p_{\text{accept}} \leq 1 - (1 - \gamma_\ell)\varepsilon^2$. □

Hence, the bound that we know will not be smaller than $1 - \varepsilon^2$. Later in Section 5.4, we discuss why we cannot hope for better bound that what we have found.

ℓ	$1-\gamma_\ell$
2	0.250
4	0.469
6	0.613
8	0.718
12	0.850
16	0.920
20	0.958

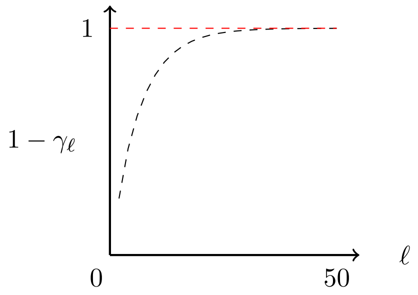

Figure 5.4: The values of of $1-\gamma_\ell$, the constant factor that occurs in the bound of p_{accept} for a protocol with one Bell difference sampling and ℓ Weyl measurements, for $\ell = 2, \dots, 50$. The table shows the values of $1-\gamma_\ell$, the constant factor that occurs in the bound of p_{accept} for a protocol with one Bell difference sampling and ℓ Weyl measurements.

5.3.2 Perfect-matching protocol

A protocol (k, ℓ, E) is a (k,ℓ)-*perfect-matching protocol* if:

1. k is an odd positive integer and
2. $E = \{(2\cdot i, 2\cdot i+1) : i = 0, \dots, (k-1)/2\}$.

For $\ell = 2$, this protocol has a nice interpretation, namely a repetition of the 6-copy algorithm $(k+1)/2$ times. In fact, any (k,ℓ)-perfect-matching protocol is just a protocol that repeats the protocol with $k = 1$. For perfect-matching protocol, we have that $d = |E| = \frac{1}{2}(k+1)$ so the number of copies used is $\frac{1}{2}(k+1)(\ell+4)$. The probability of having outcome $\mathbf{a}_1, \dots, \mathbf{a}_d$ from Bell difference extraction (k, E) on $(\psi^{\otimes 2})^{\otimes(k+1)}$ is $q_\psi(\mathbf{a}_1)q_\psi(\mathbf{a}_2)\dots q_\psi(\mathbf{a}_d)$.

In fact, any (k,ℓ)-perfect-matching protocol is just a protocol that repeats the protocol $(1,\ell)$ protocol and hence we obtain the following bound.

Theorem 5.10. *Let ψ be a pure state of n qubits that is ε-far from any stabilizer state. The probability that (k,ℓ)-perfect-matching protocol accepts ψ is at most*

$$(1-(1-\gamma_\ell)\varepsilon^2)^{(k+1)/2},$$

where γ_ℓ is the constant we define in equation 5.7.

Proof. The probability of accepting is

$$\sum_{\mathbf{a}_1,\dots,\mathbf{a}_d} q_\psi(\mathbf{a}_1)\dots q_\psi(\mathbf{a}_d) w_{\psi,\ell}(\mathbf{a}_1)\dots w_{\psi,\ell}(\mathbf{a}_d) = \left(\sum_{\mathbf{a}} q_\psi(\mathbf{a}) w_{\psi,\ell}(\mathbf{a})\right)^d \le (1-(1-\gamma_\ell)\varepsilon^2)^d,$$

where the inequality is essentially what we proved in Theorem 5.9. □

5.3.3 Complete protocol

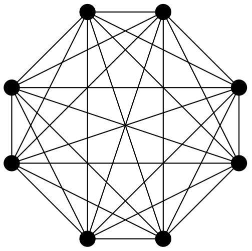

Figure 5.5: Complete protocol can be visualized as a complete graph where each vertex corresponds to a Bell sampling outcome and every edge corresponds to difference of two Bell sampling outcomes that correspond to its two endpoints. In complete protocol, the differences are extracted from every two Bell sampling outcomes.

A protocol (k, ℓ, E) is called (k, ℓ)-*complete protocol* if

$$E = \{(i, j) : 0 \leq i < j \leq k\}.$$

This is a protocol where we try to perform Weyl eigenvector test to all possible differences we can extract from the Bell sampling outcomes. For a complete protocol, we have that $d = |E| = \frac{k(k+1)}{2}$ and thus the number of copies used is $\frac{1}{2}(k+1)(k\ell + 4)$.

We know that the probability that (k, ℓ) complete protocol accept a state $|\psi\rangle$ is given by

$$\sum_{\mathbf{x}_0, \ldots, \mathbf{x}_k} t_\psi(\mathbf{x}_0) \ldots t_\psi(\mathbf{x}_k) \prod_{0 \leq i < j \leq k} w_{\psi,\ell}(\mathbf{x}_i + \mathbf{x}_j).$$

As in previous protocol, we want to have an upper bound of the probability of accepting a non-stabilizer state. Before that we prove a useful lemma.

Lemma 5.11. *Let m and ℓ be positive integers with $\ell > 1$. Let ψ be a state of n qubits that is ε-far from any stabilizer states. For any $\mathbf{a}_1, \ldots, \mathbf{a}_m \in \mathbb{Z}_2^n \oplus \mathbb{Z}_2^n$,*

$$\sum_{\mathbf{x}} t_\psi(\mathbf{x}) w_{\psi,\ell}(\mathbf{x} + \mathbf{a}_1) w_{\psi,\ell}(\mathbf{x} + \mathbf{a}_2) \ldots w_{\psi,\ell}(\mathbf{x} + \mathbf{a}_m) \leq 1 - (1 - \gamma_\ell^m)\varepsilon^2.$$

Proof. Let Q be a polynomial defined by $Q(x) = f_\ell(2^n x)$. Hence, Q is a polynomial with non-negative coefficients and also note that $w_{\psi,\ell}(\mathbf{x}) = Q(p_\psi(\mathbf{x}))$. Now, using Corollary 5.6,

$$\text{LHS} \leq \sum_{\mathbf{x}} p_\psi(\mathbf{x}) Q(p_\psi(\mathbf{x}))^m = \sum_{\mathbf{x}} p_\psi(\mathbf{x}) f_\ell(2^n p_\psi(\mathbf{x}))^m.$$

Now, we use the same strategy as before. For $M_0 = \{\mathbf{a} \in \mathbb{Z}_2^n \oplus \mathbb{Z}_2^n : 2^n p_\psi(\mathbf{a}) > 1/2\}$, we know that

$$\begin{aligned} 1 - \sum_{\mathbf{a} \in M_0} p_\psi(\mathbf{a}) &= \mathbb{P}\left[1 - f_\ell\left(2^n p_\psi(\mathbf{a})\right)^m > 1 - f_\ell(1/2)^m\right] \\ &\leq \frac{1 - \sum_{\mathbf{a}} p_\psi(\mathbf{a}) f_\ell(2^n p_\psi(\mathbf{a}))^m}{1 - f_\ell(\frac{1}{2})^m} \\ &= \frac{1 - \sum_{\mathbf{a}} p_\psi(\mathbf{a}) f_\ell(2^n p_\psi(\mathbf{a}))^m}{1 - \gamma_\ell^m} \end{aligned}$$

where the first equality is because f_ℓ is increasing and the first inequality is by Markov's inequality. Consequently,

$$1 - \varepsilon^2 \geq \max_S |\langle S|\psi\rangle|^2 \geq \sum_{\mathbf{a} \in M_0} p_\psi(\mathbf{a}) \geq 1 - \frac{1 - \sum_{\mathbf{a}} p_\psi(\mathbf{a}) f_\ell(2^n p_\psi(\mathbf{a}))^m}{1 - \gamma_\ell^m}$$

and it follows that

$$\text{LHS} \leq \sum_{\mathbf{a}} p_\psi(\mathbf{a}) f_k(2^n p_\psi(\mathbf{a}))^m \leq 1 - (1 - \gamma_\ell^m)\varepsilon^2.$$

□

Now, it is easy to prove the bound for the probability of accepting an ε-far state for the complete protocol.

Theorem 5.12. *Let ψ be a pure state of n qubits that is ε-far from any stabilizer state. The probability that (k,ℓ)-complete protocol accepts ψ is at most*

$$(1 - (1 - \gamma_\ell)\varepsilon^2)(1 - (1 - \gamma_\ell^2)\varepsilon^2)\ldots(1 - (1 - \gamma_\ell^k)\varepsilon^2).$$

Proof. We need to prove inequality

$$\sum_{\mathbf{x}_0,\ldots,\mathbf{x}_k} t_\psi(\mathbf{x}_0)\ldots t_\psi(\mathbf{x}_k) \prod_{0 \leq i < j \leq k} w_{\psi,\ell}(\mathbf{x}_i + \mathbf{x}_j) \leq \prod_{i=1}^{k} (1 - (1 - \gamma_\ell^i)\varepsilon^2)$$

for every positive integer k and $\ell > 1$. We prove by induction on k.

For $k = 1$, the inequality is true by Theorem 5.9. Suppose the inequality is true for

$k = r$. We prove that the inequality also holds for $k = r + 1$. Note that

$$\begin{aligned}
&\sum_{\mathbf{x}_0,\ldots,\mathbf{x}_{r+1}} t_\psi(\mathbf{x}_0)\ldots t_\psi(\mathbf{x}_{r+1}) \prod_{0\le i<j\le r+1} w_{\psi,\ell}(\mathbf{x}_i+\mathbf{x}_j) \\
&= \sum_{\mathbf{x}_0,\ldots,\mathbf{x}_r} t_\psi(\mathbf{x}_0)\ldots t_\psi(\mathbf{x}_r) \prod_{0\le i<j\le r} w_{\psi,\ell}(\mathbf{x}_i+\mathbf{x}_j) \underbrace{\sum_{\mathbf{x}_{r+1}} t_\psi(\mathbf{x}_{r+1}) \prod_{i=1}^{r} w_{\psi,\ell}(\mathbf{x}_{r+1}+\mathbf{x}_i)}_{\le 1-(1-\gamma_\ell^{r+1})\varepsilon^2} \\
&\le (1-(1-\gamma_\ell^{r+1})\varepsilon^2) \sum_{\mathbf{x}_0,\ldots,\mathbf{x}_r} t_\psi(\mathbf{x}_0)\ldots t_\psi(\mathbf{x}_r) \prod_{0\le i<j\le r} w_{\psi,\ell}(\mathbf{x}_i+\mathbf{x}_j) \\
&\le (1-(1-\gamma_\ell^{r+1})\varepsilon^2) \prod_{i=1}^{r} (1-(1-\gamma_\ell^{i})\varepsilon^2) \\
&= \prod_{i=1}^{r+1} (1-(1-\gamma_\ell^{i})\varepsilon^2),
\end{aligned}$$

where the first inequality follows from Lemma 5.11 and the second inequality follows from induction hypothesis. □

5.3.4 Star protocol

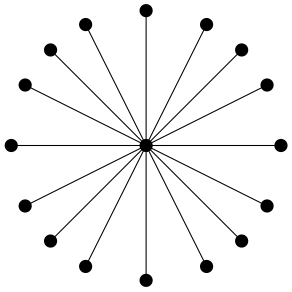

Figure 5.6: Star protocol can be visualized as a star graph where each vertex corresponds to a Bell sampling outcome and every edge corresponds to difference of two Bell sampling outcomes that correspond to its two endpoints. In star graph, there exists a vertex that is a neighbor and the only neighbor of other vertices.

A protocol (k, ℓ, E) is called (k, ℓ)-*star protocol* if

$$E = \{(0, i) : i = 1, \ldots, k\}.$$

For a star protocol, we have that $d = |E| = k$ so the number of copies used is $k(\ell + 2) + 2$. For $\ell = 2$, we obtain the star protocol that we have described in Algorithm 2.

We also denote the outcomes of Bell difference extraction used in a star protocol by $\mathbf{a}_i$ for the difference between two Bell sampling outcomes $\mathbf{x}_0$ and $\mathbf{x}_i$ for $i = 1, \dots, k$. For any pure state ψ, the probability of having outcome $\mathbf{a}_1, \dots, \mathbf{a}_k$ from Bell difference extraction (k, E) on $(\psi^{\otimes 2})^{\otimes(k+1)}$ is

$$\sum_{\mathbf{x}} t_\psi(\mathbf{x}) t_\psi(\mathbf{x} + \mathbf{a}_1) \dots t_\psi(\mathbf{x} + \mathbf{a}_k).$$

We are now ready to prove an upper bound for accepting non-stabilizer state.

Theorem 5.13. *Let ψ be a pure state of n qubits that is ε-far from any stabilizer state. The probability that (k, ℓ)-star protocol accepts ψ is at most*

$$(1 - (1 - \gamma_\ell)\varepsilon^2)^k.$$

Proof. It is routine now to show that the probability of accepting a state ψ using star protocol is given by

$$\begin{aligned}
&\sum_{\mathbf{a}_1, \dots, \mathbf{a}_k} \sum_{\mathbf{x}} t_\psi(\mathbf{x}) t_\psi(\mathbf{x} + \mathbf{a}_1) \dots t_\psi(\mathbf{x} + \mathbf{a}_k) w_{\psi,\ell}(\mathbf{a}_1) \dots w_{\psi,\ell}(\mathbf{a}_k) \\
&= \sum_{\mathbf{x}} t_\psi(\mathbf{x}) \left(\sum_{\mathbf{a}} t_\psi(\mathbf{x} + \mathbf{a}) w_{\psi,\ell}(\mathbf{a}) \right)^k \\
&\leq \sum_{\mathbf{x}} t_\psi(\mathbf{x}) (1 - (1 - \gamma_\ell)\varepsilon^2)^k \\
&= (1 - (1 - \gamma_\ell)\varepsilon^2)^k
\end{aligned}$$

where the inequality follows from Theorem 5.9. □

5.4 Discussion

Every protocol that we have analyzed so far has perfect completeness, i.e. if $|\psi\rangle$ is a stabilizer state, the protocol accepts $|\psi\rangle$ with probability 1. Hence, the protocol makes an error if and only if it accepts non-stabilizer state. If $|\psi\rangle$ is ε-far from any stabilizer state, we have shown that we can upper bound the error probability, i.e. the probability that the protocol accepts $|\psi\rangle$. The bound is parameterized by the parameters of the algorithm, namely k, ℓ, and E.

5.4.1 Bell sampling versus Weyl measurement

Our first result is Theorem 5.9 which states that for $k = 1$, the error probability is bounded by $1 - (1 - \gamma_\ell)\varepsilon^2$. Note that as increasing ℓ does not make this bound arbirarily small.

Indeed, the bound cannot be smaller than $1-\varepsilon^2$. This result suggests that we should not invest too many resources (number of copies) on Weyl measurement. The following theorem shows that there exists a state that makes Weyl measurement not so useful in our protocol; Bell difference extraction is what matters the most.

Theorem 5.14. *Consider the state $|\Psi\rangle = |0\rangle^{\otimes(n-1)} \otimes |\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ where $|\psi\rangle$ is an arbitrary state of one qubit. For any positive integer k and positive integer $\ell > 1$, $|\Psi\rangle$ will be accepted by the protocol (k, ℓ, E) with probability at least 4^{-k}.*

Proof. The stabilizer testing protocols that we propose are transversal and since $|\Psi\rangle$ is a product of n one-qubit states, we can just analyze each qubit independently. The first $n-1$ qubits are $|0\rangle$. Performing Bell sampling on $|0\rangle^{\otimes 2}$ will give us outcome from $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ with probability

$$t_\psi(\mathbf{x}) = \begin{cases} \frac{1}{2} & \text{if } \mathbf{x} = 00, \\ \frac{1}{2} & \text{if } \mathbf{x} = 10, \\ 0 & \text{otherwise.} \end{cases}$$

Recall that $W_{00} = I$ and $W_{01} = Z$. Each of them has $|0\rangle$ as their $+1$ eigenvector so the Weyl measurement on $|0\rangle$ will always give the same outcome, namely $+1$.

For the last qubit, the probability that all the $k+1$ Bell samplings give the same outcome is given by

$$\sum_{\mathbf{x}\in\mathbb{Z}_2\oplus\mathbb{Z}_2} t_\psi(\mathbf{x})^{k+1} \geq 4^{-k} \left(\sum_{\mathbf{x}\in\mathbb{Z}_2\oplus\mathbb{Z}_2} t_\psi(\mathbf{x}) \right)^{k+1} = 4^{-k}.$$

If all the $k+1$ Bell samplings on independent copies of $|\psi\rangle^{\otimes 2}$ give us the same outcome, then all outcomes of the Bell difference extraction will be 00, which corresponds to the identity I. In the case that all Bell sampling outcomes are the same, the algorithm will accept $|\Psi\rangle$ with probability 1 since in particular, I has $|\psi\rangle$ as an $+1$-eigenvector.

Hence, the probability of accepting $|\Psi\rangle$ is at least 4^{-k}. □

5.4.2 Error Exponent

Aside from the stabilizer testing protocol with $k = 1$, we also have discussed some other families of stabilizer testing protocols: (k, ℓ)-perfect-matching protocol, (k, ℓ)-complete protocol, and (k, ℓ)-star protocol. We summarize our result so far about the performance of other interesting stabilizer testing protocols in Table 5.1.

Protocol	Number of copies	Upper bound of the error probability
Perfect-matching protocol	$(k+1)(\ell+4)/2$	$(1-(1-\gamma_\ell)\varepsilon^2)^{\frac{k+1}{2}}$
Complete protocol	$(k+1)(k\cdot\ell+4)/2$	$(1-(1-\gamma_\ell)\varepsilon^2)\ldots(1-(1-\gamma_\ell^k)\varepsilon^2)$
Star protocol	$k(\ell+2)+2$	$(1-(1-\gamma_\ell)\varepsilon^2)^k$

Table 5.1: Performance comparison of some protocols that utilize Bell difference extraction in terms of the number of copies used and also the probability bound of accepting a state that is ε-far from any stabilizer state.

Theorem 5.14 also tells us that to obtain a small error probability, we should invest more copies to be used for Bell samplings. Hence, we will analyze our stabilizer testing protocols by thinking of ℓ as a fixed constant and thinking of the number of copies used for each protocol as a function of k.

Table 5.1 shows how many copies are used in each stabilizer testing protocol and also the bound for error probability of the protocol. To compare the three protocols, we can think of how the upper bound of the error probability as function of the number of copies used by the protocol.

Let us consider an example. For a protocol that repeats the 6-copy algorithm t, the number of copies that is used is $N = 6\cdot t$ and the error probability can be bounded as follows:

$$p_{\text{error}} \leq (1 - \frac{1}{4}\varepsilon^2)^t.$$

We can write

$$p_{\text{error}} \leq \exp\left(N\frac{\ln(1-\frac{1}{4}\varepsilon^2)}{6}\right) = \exp\left(-\frac{1}{24}N\varepsilon^2 + O(\varepsilon^4)\right).$$

Hence, we can see that for the protocol that repeats the 6-copy algorithm the error probability is reduced exponentially with respect to the number of copies used, and the factor $\varepsilon^2/24$ parameterizes how fast the exponential reduction is. It is easy to see that bigger factor will give a faster error reduction.

Given a protocol that uses N copies and makes an error with probability p_{error}, we define *error exponent* of such protocol as

$$E := \lim_{N\to\infty} -\frac{1}{N}\ln p_{\text{error}}.$$

This definition makes sense, since we expect the error probability is exponentially decreasing with respect to the number of copies. If we write $p_{\text{error}} \leq \exp(-N\alpha)$, we will obtain a bound

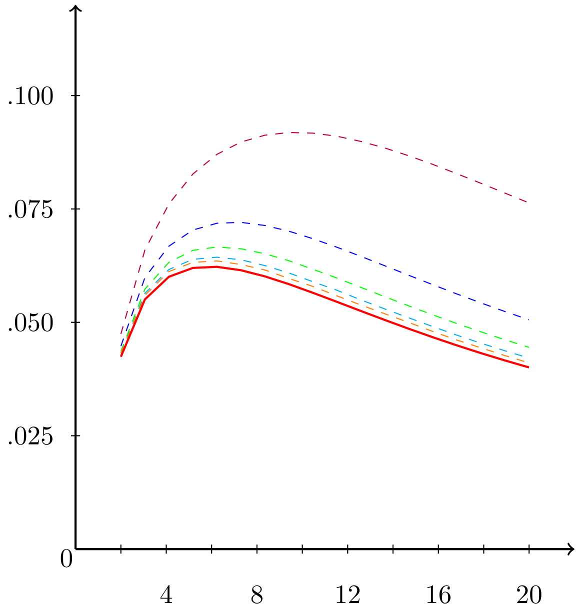

Figure 5.7: We approximate the error exponent of perfect-matching protocol with $\frac{1-\gamma_\ell}{\ell+4}\varepsilon^2$. In the diagram above, we plot $\frac{1}{\varepsilon^2}\cdot\frac{-\ln(1-(1-\gamma_\ell)\varepsilon^2)}{\ell+4}$ for $\varepsilon^2 = 0.8, 0.4, 0.2, 0.1, 0.05$. These functions converge to $\frac{1-\gamma_\ell}{\ell+2}$ as ε goes to 0. Moreover, as ℓ gets larger, the error exponent function $\frac{1-\gamma_\ell}{\ell+4}$ decreases.

of the error exponent $E \geq \alpha$. It is easy to see that bigger error exponent will give faster reduction. For example, for the protocol that repeats the 6-copy algorithm, we will obtain

$$E \geq \lim_{t\to\infty} -\frac{1}{6t}\ln\left((1-\frac{1}{4}\varepsilon^2)^t\right) = \frac{-\ln(1-\frac{1}{4}\varepsilon^2)}{6} = \frac{1}{24}\varepsilon^2 + O(\varepsilon^4).$$

By having a bound for the error exponent of a protocol, we can also judge the number of copies needed to have a small constant error probability bound. Indeed, if $p_{\text{error}} \leq \exp(-N\alpha)$, we can set $N = \Omega(1/\alpha)$ to have a small constant bound for p_{error}.

We can now bound the error exponent of perfect-matching protocol, complete protocol, and star protocol.

Error exponent of (k,ℓ)-perfect-matching protocol

For (k,ℓ)-perfect-matching protocol, we have that $N = (k+1)(\ell+4)/2$ and $p_{\text{error}} \leq (1-(1-\gamma_\ell)\varepsilon^2)^{\frac{k+1}{2}}$. In evaluating the error exponent, we are interested in large N. By Theorem 5.14, we should just fix ℓ. Hence, the error exponent of (k,ℓ)-perfect matching protocol is given by

$$\begin{aligned} E &\geq \lim_{k\to\infty} -\frac{1}{(k+1)(\ell+4)/2} \ln\left((1-(1-\gamma_\ell)\varepsilon^2)^{\frac{k+1}{2}}\right) \\ &= \frac{-\ln(1-(1-\gamma_\ell)\varepsilon^2)}{\ell+4} \\ &= \frac{(1-\gamma_\ell)}{\ell+4}\varepsilon^2 + O(\varepsilon^4). \end{aligned}$$

For small ε, we can approximate the error exponent with $\frac{1-\gamma_\ell}{\ell+4}\varepsilon^2$. See Figure 5.7 as an illustration.

Error exponent of (k,ℓ)-complete protocol

For (k,ℓ)-complete protocol, we have that $N = (k+1)(k\ell+4)/2$ and $p_{\text{error}} \leq (1-(1-\gamma_\ell)\varepsilon^2)\ldots(1-(1-\gamma_\ell^k)\varepsilon^2)$. We can bound the error exponent as follows:

$$\begin{aligned} E &\geq \lim_{k\to\infty} -\frac{1}{(k+1)(k\ell+4)/2}\sum_{i=1}^{k} \ln(1-(1-\gamma_\ell^i)\varepsilon^2) \\ &= \lim_{k\to\infty} \frac{1}{(k+1)(k\ell+4)/2}\sum_{i=1}^{k}(1-\gamma_\ell^i)\varepsilon^2 + O(\varepsilon^4) \\ &= \lim_{k\to\infty} \frac{k-\sum_{i=1}^{k}\gamma_\ell^i}{(k+1)(k\ell+4)/2}\varepsilon^2 + O(\varepsilon^4) \\ &= 0. \end{aligned}$$

Hence, the bound for the error exponent of (k,ℓ)-complete protocol is very weak. This is not surprising since (k,ℓ)-complete protocol due to Theorem 5.14 while complete protocol uses most copies for eigenvector test. Hence, (k,ℓ)-complete protocol is not a good protocol for stabilizer testing.

Error exponent of (k,ℓ)-star protocol

For (k,ℓ)-star protocol, we have that $N = k(\ell+2)+2$ and $p_{\text{error}} \leq (1-(1-\gamma_\ell)\varepsilon^2)^k$. In evaluating the error exponent, we are interested in large N. By Theorem 5.14, we should just fix ℓ. Hence, the error exponent of (k,ℓ)-star protocol is given by

$$\begin{aligned} E &\geq \lim_{k\to\infty} -\frac{1}{k(\ell+2)+2}\ln\left((1-(1-\gamma_\ell)\varepsilon^2)^k\right) \\ &= \lim_{k\to\infty} -\frac{k}{k(\ell+2)+2}\ln(1-(1-\gamma_\ell)\varepsilon^2) \\ &= \frac{1-\gamma_\ell}{\ell+2}\varepsilon^2 + O(\varepsilon^4) \end{aligned}$$

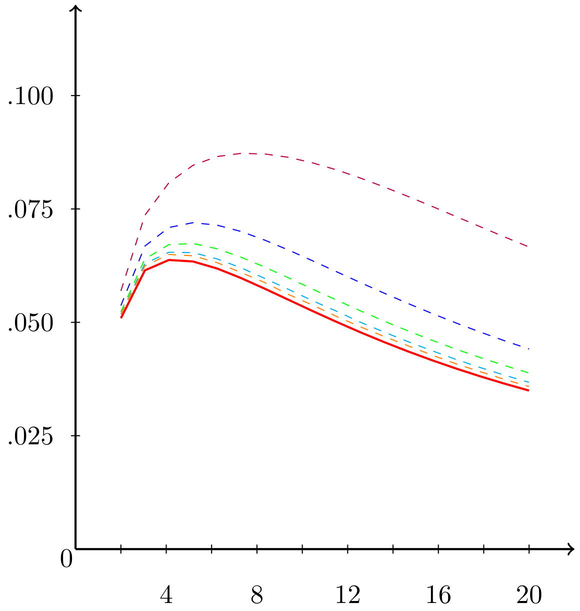

Figure 5.8: We approximate the error exponent of star protocol with $\frac{1-\gamma_\ell}{\ell+2}\varepsilon^2$. In the diagram above, we plot $\frac{1}{\varepsilon^2} \cdot \frac{-\ln(1-(1-\gamma_\ell)\varepsilon^2)}{\ell+2}$ for $\varepsilon^2 = 0.8, 0.4, 0.2, 0.1, 0.05$. These functions converge to $\frac{1-\gamma_\ell}{\ell+2}$ as ε goes to 0. Moreover, as ℓ gets larger, the error exponent function $\frac{1-\gamma_\ell}{\ell+2}$ decreases.

For small ε, we can approximate the error exponent with $\frac{1-\gamma_\ell}{\ell+4}\varepsilon^2$. See Figure 5.8 as an illustration.

5.4.3 Comparison

We have seen that (k, ℓ)-complete protocol is not a good protocol for stabilizer testing. For other two families of protocol, namely (k, ℓ)-perfect-matching protocol and (k, ℓ)-star protocol, we summarize our analysis in terms of error exponent in Table 5.2.

Protocol	Bound for error exponent	Best ℓ	Best error exponent
Perfect-matching protocol	$\varepsilon^2 \cdot \frac{1-\gamma_\ell}{\ell+4}$	6	$0.062\varepsilon^2$
Star protocol	$\varepsilon^2 \cdot \frac{1-\gamma_\ell}{\ell+2}$	4	$0.080\varepsilon^2$

Table 5.2: Performance comparison of some stabilizer testing protocols.

Since $\ell + 4 > \ell + 2$, we can see that in general star protocol will perform better than perfect-matching protocol. Recall that for $\ell = 2$, (k, ℓ)-perfect-matching protocol corre-

```
Algorithm 2: $(k, 2)$-star protocol
  Input: $4k + 2$ copies of the state $|\psi\rangle$.
    1. Perform Bell sampling $k + 1$ times on copies of $|\psi\rangle^{\otimes 2}$, and denote the outcomes by
       $\mathbf{x}_0, \ldots, \mathbf{x}_k$.
    2. Compute $\mathbf{a}_i = \mathbf{x}_0 + \mathbf{x}_i$ for $i = 1, \ldots, k$.
    3. Perform Weyl measurements $W_{\mathbf{a}}$ twice on two independent copies of $|\psi\rangle$ for each
       $\mathbf{a} \in \{\mathbf{a}_i\}_i$ and accept iff every pair of the outcomes agree.
```

sponds to a protocol that just repeats the 6-copy algorithm $t := (k + 1)/2$ times. This protocol will have an error probability bounded by $(1 - \frac{1}{4}\varepsilon^2)^t$ and uses $6 \cdot t$ copies. On the other hand, $(t, 2)$-star protocol will only use $4t + 2$ copies and have an error probability bounded by $(1 - \frac{1}{4}\varepsilon^2)^t$. This means that, with $(t, 2)$-star protocol, we can obtain the same error probability bound by just using $2/3$ number of copies available; giving an affirmative answer to Question $(*)$. For illustration, we write the protocol as Algorithm 2 and the high-level circuit in 5.9.

From Figure 5.7 and Figure 5.8, we can also see that the error exponent is maximized at $\ell = 6$ and $\ell = 4$, respectively. This is compatible with Theorem 5.14 that we should not invest too many copies of eigenvector test.

We can also compare the two protocols by choosing the best ℓ possible for each protocol. We can see from Table 5.2 that the bound for error exponent of $(k, 6)$-perfect-matching protocol is $0.062\varepsilon^2$ and the bound for error exponent of $(k, 4)$-star protocol is $0.080\varepsilon^2$. Hence, if we want to allocate a bit more than 2 copies for each Weyl eigenvector test, star-protocol still provides the better possible error exponent that the perfect-matching protocol.

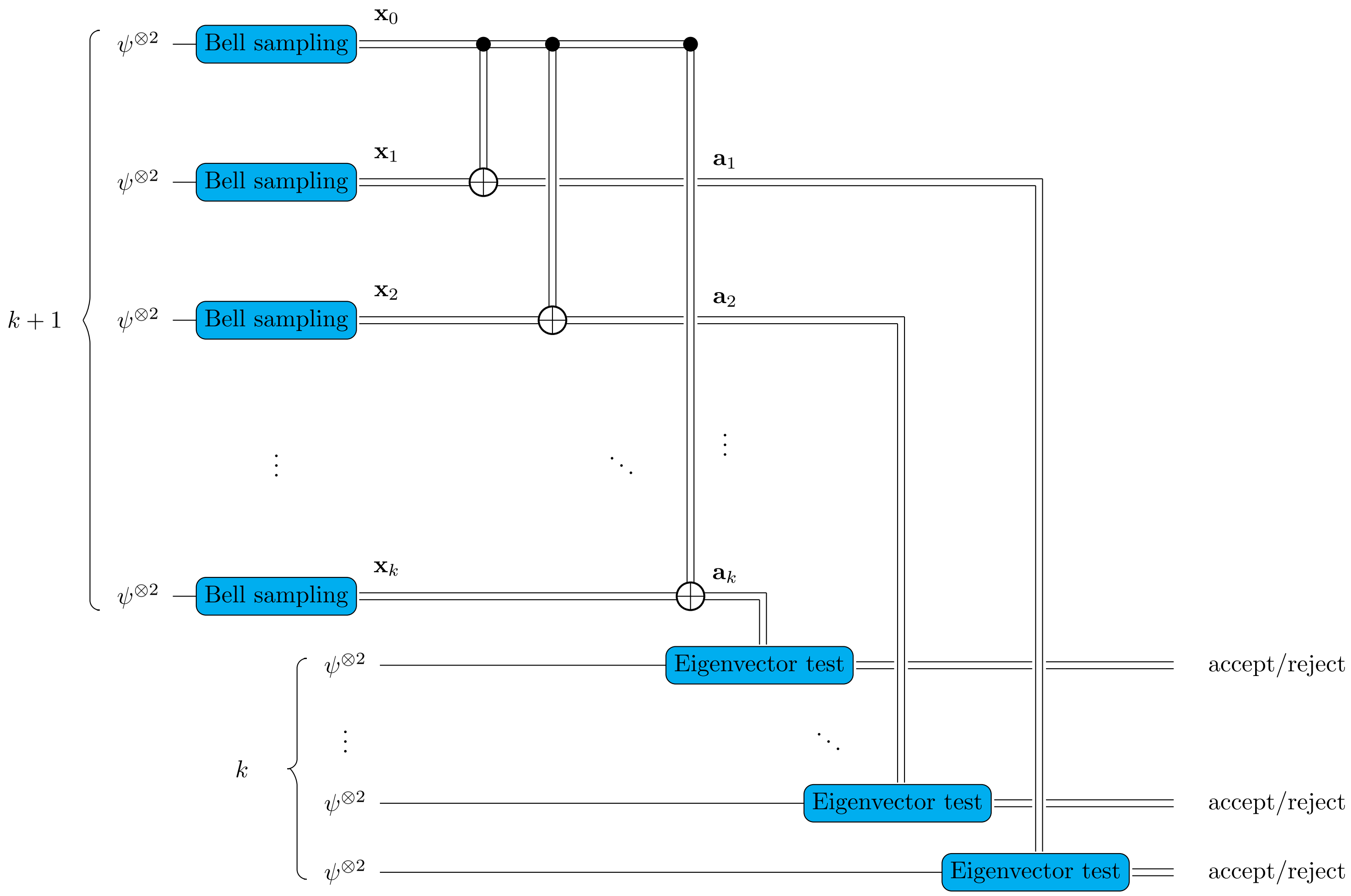

Figure 5.9: A high-level circuit for $(k, 2)$-star protocol.

Chapter 6

Conclusion and further research

6.1 Conclusion

In this thesis, we make several contributions. First, we study the proof of the 6-copy stabilizer testing algorithm and give another perspective on its analysis. This inspires us to propose a stabilizer testing protocol that has better efficiency than the protocol that just repeats the 6-copy algorithm. We also study some other natural stabilizer testing protocols and learn how their parameters affect the performance of the protocol. We formalize a no-go theorem for dimensional independent stabilizer testing algorithm and make a connection to quantum design and prove a no-go theorem for 4 copies. We do not prove a no-go theorem for 5 copies but explain a strategy that is similar to the strategy of proving the no-go theorem for 4 copies.

6.2 Further research

We list some possible directions for further research.

1. Dimension-independent stabilizer testing with 5 copies.
   It will be interesting to investigate dimensional independent stabilizer testing whether no-go theorem for 5 copies holds. In Section 4.4, we explains possible strategy towards this direction.

2. Testing stabilizer states with real amplitudes.
   We also know that if we only consider states with real amplitudes, we have a dimension

independent stabilizer testing algorithm that only uses 4 copies instead of 6 copies. Indeed, we just need to perform Bell sampling once on two copies of $|\psi\rangle$ and perform Weyl measurement twice on two independent copies of $|\psi\rangle$.

It is now natural to also ask whether it is possible to have a stabilizer testing algorithm for stabilizer states with real amplitudes if we have less than 4 copies. Moreover, we can also investigate if there exists a better strategy than just repeating the 4-copy algorithm when we know that

3. Testing whether a state has stabilizer rank less than or equal to k.
   We say that a state has stabilizer rank k if k is the least positive integer such that the state can be written as a superposition of k stabilizer states. Stabilizer rank is an interesting notion that is related to understand how efficient we can do classical simulation of quantum computation [BSS16, BG16, GMC17]. Stabilizer states are of course the states that have stabilizer rank 1. An interesting research direction would be to investigate how to test efficiently, given a positive integer $k \geq 2$, whether a state has stabilizer rank that is less than or equal to k.

Acknowledgement

I would like to thank my supervisor Michael Walter who has been a great supervisor to me. Michael is always enthusiastic. I still remember when he said *'Good! Let's do science!'* after we fix some administrative issues. His enthusiasm is contagious. He is a great company for discussion and has many interesting ideas but he never makes me afraid to ask stupid and trivial questions. He always encourages me and I remember it when I was stressed out and thought that things were going all the way wrong. Without him, I would not be able to finish this thesis. I would also like to thank Sepehr Nezami for the discussion together with Michael of the proof strategy for no-go theorem for 4 copies in this thesis.

I would like to thank my thesis committee members, Ronald de Wolf, Christian Schaffner, and Maris Ozols, for reading this thesis. Also thank you for the feedbacks given to improve this thesis.

To my *mamak* Jenny Sipayung and my *bapak* Kander Damanik who have provided me unconditional love, I will be back very soon. My two sisters Ivo Gustiara Damanik and Novita Hillary Christy Damanik who are in my team since day one.

To Bu Sumartianingsih, my high school math teacher, who believed in me.

My life in Amsterdam would not have been as good without other logic students. Especially, thanks for Marlou and Marvin for being around during my difficult times. Thanks to David Santamaria who can make even the most unexpected situation funny. Thanks are due to my course buddies Krsto Prorokovic and David Veenstra who want to share their knowledge through discussions. Also, I would like to thank everybody who makes studying in MOL room enjoyable.

I also would like to thank Ulle Endriss, for helping me adapting with the new academic environment. Also, Professor Benedikt Löwe, for discussions about the world of sets and mathematics (and mathematics culture) and Lorenzo Galeotti who are very helpful in the course that I took. Ronald de Haan, for the fun complexity project. Yurii Khomski, for the fun alternative set theory project. Malvin, who has been a kind TA in my first semester here and provides room for errors so I can improve in the direction that I want. Tanja Kassenaar, who has been helping me even before I came to Amsterdam for Master of Logic programme.

I am also grateful to QuSoft members who have been a great source of learning for me about theory of quantum computing. I would like to thank Ronald for introducing me to the world of quantum computing. Chris, Jan, and Yfke who have been providing room to learn quantum cyrpto in an enjoyable way. Tom and Freek, who are very patient in explaining me things from complexity theory and symmetry and quantum information theory class. Also to Casper who have helped me understanding some mathematics that I was afraid of.

To my Badminton Vereniging Amsterdam (BVA) friends for the memorable moments on court and off court: Bonar, Mas Jaka, Pak Ivan, Hennie, Jurian, Julien, Viktor, Pierre, Mono, Faishol, Junaed, Uthe, Wiepk, Edward, Debora, Raimond, Arihant, Esmee, Nina, Ming, Stefan, and many other players from this lovely club.

My study and living in Amsterdam is generously funded by LPDP Scholarship, Ministry of Finance, Indonesia.

Bibliography

[AB09] Sanjeev Arora and Boaz Barak. *Computational Complexity: A Modern Approach*. Cambridge University Press, New York, NY, USA, 1st edition, 2009.

[AG04] Scott Aaronson and Daniel Gottesman. Improved Simulation of Stabilizer Circuits. *Physical Review A*, 70(5):052328, 2004.

[AG08] Scott Aaronson and Daniel Gottesman. Identifying Stabilizer States. `http://pirsa.org/08080052`, 2008.

[BBC$^+$93] Charles H Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K Wootters. Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels. *Physical Review Letters*, 70(13):1895, 1993.

[BG16] Sergey Bravyi and David Gosset. Improved Classical Simulation of Quantum Circuits Dominated by Clifford Gates. *Physical Review Letters*, 116:250501, Jun 2016.

[BSS16] Sergey Bravyi, Graeme Smith, and John A. Smolin. Trading Classical and Quantum Computational Resources. *Physical Review X*, 6:021043, Jun 2016.

[Die82] DGBJ Dieks. Communication by EPR Devices. *Physics Letters A*, 92(6):271–272, 1982.

[dW18] Ronald de Wolf. Quantum Computing: Lecture Notes. `https://homepages.cwi.nl/~rdewolf/qcnotes.pdf`, 2018.

[GMC17] Héctor J. García, Igor L. Markov, and Andrew W. Cross. On the Geometry of Stabilizer States. 2017. arXiv:1711.07848v1.

[GNW17] David Gross, Sepehr Nezami, and Michael Walter. Schur-Weyl Duality for the Clifford Group with Applications: Property Testing, a Robust Hudson Theorem, and de Finetti Representations. 2017. arXiv:1712.08628v1.

[Got97] David Gottesman. Stabilizer codes and quantum error correction. *PhD thesis, California Institute of Technology*, 1997.

[Har13] Aram W Harrow. The Church of the Symmetric Subspace. *arXiv:1308.6595*, 2013.

[Hol73] Alexander Semenovich Holevo. Bounds for the Quantity of Information Transmitted by a Quantum Communication Channel. *Problemy Peredachi Informatsii*, 9(3):3–11, 1973.

[KG15] Richard Kueng and David Gross. Qubit Stabilizer States are Complex Projective 3-Designs. 2015. arXiv:1510.02767.

[MdW16] Ashley Montanaro and Ronald de Wolf. A Survey of Quantum Property Testing. *Theory of Computing, Graduate Surveys*, 7:1–81, 2016.

[Mon17] Ashley Montanaro. Learning Stabilizer States. 2017. arXiv:1707.04012.

[PB00] Arun Kumar Pati and Samuel L Braunstein. Impossibility of Deleting an Unknown Quantum State. *Nature*, 404(6774):164, 2000.

[RBB03] Robert Raussendorf, Daniel E. Browne, and Hans J. Briegel. Measurement-based Quantum Computation on Cluster States. *Physical Review A*, 68:022312, Aug 2003.

[Ser12] Jean-Pierre Serre. *Linear Representations of Finite Groups*, volume 42. Springer Science & Business Media, 2012.

[Wal18] Michael Walter. Symmetry and Quantum Information. https://staff.fnwi.uva.nl/m.walter/qit18/qit18.pdf, 2018.

[Woo87] William K Wootters. A Wigner-function Formulation of Finite-state Quantum Mechanics. *Annals of Physics*, 176(1):1–21, 1987.

[WZ82] William K Wootters and Wojciech H Zurek. A Single Quantum Cannot be Cloned. *Nature*, 299(5886):802–803, 1982.

[ZKGG16] Huangjun Zhu, Richard Kueng, Markus Grassl, and David Gross. The Clifford group fails gracefully to be a unitary 4-design. 2016. arXiv:1609.08172v1.

[ZPDF16] Liming Zhao, Carlos A Pérez-Delgado, and Joseph F Fitzsimons. Fast Graph Operations in Quantum Computation. *Physical Review A*, 93(3):032314, 2016.