On quantum computation theory
van Dam, W.K.

Citation for published version (APA):

General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: http://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.
Chapter 6
Self-Testing of Quantum Gates

This chapter concerns the problem how to test the behavior of a quantum gate. If we think that we have a Hadamard gate $H$, how can we be sure that $H$ behaves indeed correctly on all possible input qubits $\alpha|0\rangle + \beta|1\rangle$? How can we test this without having to rely on other quantum mechanical components that can be equally unreliable? These questions concern the *self-testability* of quantum gates.

We show how some gates or families of gates are self-testable whereas others are not. These self-testing procedures are also "robust". By this we mean that the error during the test-procedure and the error of the gate are proportional: If we detect a small error during the testing-procedure, then this will always correspond to a small error in the gate. The method is also extended to two-qubit gates.

6.1 Introduction

We consider the design of self-testers for quantum gates. A self-tester for the gates $F_1, \ldots, F_m$ is a classical procedure that, given any gates $G_1, \ldots, G_m$, decides with high probability if each $G_i$ is close to $F_i$. This decision has to rely only on measuring in the computational basis the effect of iterating the gates on the classical states. It turns out that instead of individual gates, we can only design procedures for families of gates. To achieve our goal we borrow some elegant ideas of the theory of program testing: we characterize the gate families by specific properties, we develop a theory of robustness for them, and show that they lead to self-testers. In particular we prove that the universal and fault-tolerant set of gates consisting of a Hadamard gate, a CNot gate, and a phase rotation gate of angle $\pi/4$ is self-testable.

The idea of self-testing in quantum devices is implicit in the work of Adleman, Demarrais and Huang[1]. They have developed a procedure by which a quantum Turing machine is able to estimate its internal angle by its own means under the hypothesis that the machine is unitary. In the context of quantum cryptography Mayers and Yao[71] have designed tests for deciding if a photon source is perfect. These tests guarantee that
Chapter 6. Self-Testing of Quantum Gates

If source passes them then it is adequate for the security of the Bennett-Brassard[20] quantum key distribution protocol.

Here we develop the theory of self-testing of quantum gates by classical procedures. Given a completely positive super operator (CPSO) $G$ for $n$ qubits, and a family $\mathcal{F}$ of unitary CPSOs, we would like to decide if $G$ belongs to $\mathcal{F}$. Intuitively, a self-tester is a procedure that answers the question \("G \in \mathcal{F} ?\" by interacting with the CPSO $G$ in a purely classical way. More precisely, it will be a probabilistic algorithm that is able to access $G$ as a black box in the following sense: it can prepare the classical states $w \in \{0,1\}^n$, iterate $G$ on these states, and afterwards, measure in the computational basis. The access must be seen as a whole, performed by a specific, experimental oracle for $G$: once the basis state $w$ and the number of iterations $k$ have been specified, the program in one step gets back one of the possible probabilistic outcomes of measuring the state of the system after $G$ is iterated $k$-times on $w$. The intermediate quantum states of this process cannot be used by the program, which cannot perform any other quantum operations either. For $0 \leq \delta_1 \leq \delta_2$, such an algorithm will be a $(\delta_1, \delta_2)$-tester for $\mathcal{F}$ if for every CPSO $G$, whenever the distance of $G$ and $\mathcal{F}$ is at most $\delta_1$ (in some norm), it accepts with high probability, and whenever the same distance is greater than $\delta_2$, it rejects with high probability, where the probability is taken over the measurements performed by the oracle and by the internal coin tosses of the algorithm. Finally we will say that $\mathcal{F}$ is testable if for every $\delta_2 > 0$, there exists $0 < \delta_1 \leq \delta_2$ such that there exists a $(\delta_1, \delta_2)$-tester for $\mathcal{F}$. These definitions can be extended to several classes of CPSOs.

The study of self-testing programs is a well-established research area which was initiated by the work of Blum, Luby and Rubinfeld[24], Rubinfeld[79], Lipton[69] and Gemmel et al. [47]. The purpose of a self-tester for a function family is to detect by simple means if a program which is accessible as an oracle computes a specific function from the given family. This clearly inspired the definition of our self-testers which have the peculiarity that they should test quantum objects that they can access only in some restricted manner. The analogy with self-testing does not stop with the definition. One of the main tools in self-testing of function families is the characterization of these families by robust properties. Informally, a property is robust if whenever a function satisfies the property approximately, then it is close to a function which satisfies it exactly. The concept of robustness was introduced and its implication for self-testing was first studied by Rubinfeld and Sudan[81] and by Rubinfeld[80]. It will play a crucial role in our case as well.

We note in the Preliminaries that for any real $\phi$ the states $|1\rangle$ and $e^{i\phi}|1\rangle$ are experimentally indistinguishable. This implies that if both the input states and the measurement basis vectors are the classical states $|0\rangle$ and $|1\rangle$, then there are ‘families’ of CPSOs which are mutually indistinguishable. For example, let the CPSO $H$ be the well-known Hadamard gate with

$$|0\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad \text{and} \quad |1\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$
and let $H_{\phi}$ be the same gate expressed in the basis $|0\rangle, e^{i\phi}|1\rangle$, hence

$$
|0\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi}|1\rangle) \quad \text{and} \quad |1\rangle \mapsto \frac{1}{\sqrt{2}}(e^{-i\phi}|0\rangle - |1\rangle),
$$

for $\phi \in [0, 2\pi)$. Any experiment that uses $H$ and starts with the state $|0\rangle$ or $|1\rangle$ will produce the outcomes “0” and “1” with the same probabilities as the same experiment with the $H_{\phi}$ gate. Thus, no experiment that uses this quantum gate alone can distinguish $H$ from $H_{\phi}$. Indeed, as stated later in Fact 15, we will have to consider a testable ‘family’ $F = \{H_{\phi} | \phi \in [0, 2\pi)\}$ containing all $H_{\phi}$ gates.

The main result is Theorem 15 which states that for several sets of unitary CPSOs, in particular, the Hadamard gates family, Hadamard gates together with CNot gates, and Hadamard gates with CNot and phase rotation gates of angle $\pm \frac{\pi}{4}$, are testable. This last family is of particular importance since every triplet in the family forms a universal and fault-tolerant set of gates for quantum computation[26].

For the proof we will define the notion of experimental equations which are functional equations for CPSOs corresponding to the properties of the quantum gate that a self-tester can approximately test. These tests are done via the interaction with the experimental oracle. The proof itself contains three parts. In Theorems 10, 11, and 12 we will exhibit experimental equations for the families of unitary CPSOs we want to characterize. In Theorem 13 we will show that actually all experimental equations are robust; in fact, the distance of a CPSO from the target family is polynomially related to the error tolerated in the experimental equations. Finally Theorem 14 gives self-testers for CPSO families which are characterized by a finite set of robust experimental equations.

In some cases, we are able to calculate explicitly the polynomial bound in the robustness of experimental equations. Such a result will be illustrated in Lemma 14 for the equations characterizing the Hadamard family $\{H_{\phi}\}$.

Technically, these results will be based on the representation of one-qubit states and CPSOs in $\mathbb{R}^3$, where they are respectively vectors in the unit ball of $\mathbb{R}^3$, and particular affine transformations. This correspondence is known as the Bloch Ball representation.

### 6.2 The Bloch Ball representation

Specific for the one-qubit case there is a very appealing way of describing both the states and its unitary transformations in 3 dimensional Euclidean space, known as the Bloch ball picture. This representation relies on the isomorphism between the group $U(2)/U(1)$ and the special rotation group $SO(3)$, the set of $3 \times 3$ orthogonal matrices with determinant 1. This allows us to view one-qubit states as vectors in the unit ball of $\mathbb{R}^3$, and unitary superoperators as rotations on $\mathbb{R}^3$. We will now describe exactly this correspondence.

The Bloch Ball $B$ (respectively Bloch Sphere $S$) is the ball (sphere) with radius 1 of the Euclidean affine space $\mathbb{R}^3$. Any point $\vec{u} \in \mathbb{R}^3$ determines a vector with the same
coordinates which we will also denote by $\vec{u}$. The inner product of $\vec{u}$ and $\vec{v}$ will be denoted by $(\vec{u}, \vec{v})$, and the Euclidean norm of $\vec{u}$ by $||\vec{u}||$.

Using spherical coordinates, we can characterize each point $\vec{u} \in \mathbb{R}^3$ by its norm $r \geq 0$, its latitude $\theta \in [0, \pi]$, and its longitude $\phi \in [0, 2\pi)$. The latitude is the angle between the z-axis and the vector $\vec{u}$, and the longitude is the angle between the x-axis and the orthogonal projection of $\vec{u}$ in the plane defined by $z = 0$. If $\vec{u} = (x, y, z)^T$, then these parameters satisfy $x = r \sin \theta \cos \phi$, $y = r \sin \theta \sin \phi$, and $z = r \cos \theta$. For every $(x, y, z)^T \in B \subset \mathbb{R}^3$ there exists a unique density matrix such that

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 + z & x - iy & x + iy \\ x - iy & 1 - z & y + ix \\ y - ix & 1 + z & x + iy \end{pmatrix} = \tilde{\rho}.$$  

This mapping is a bijection that also obeys

$$\tilde{\rho}(p, \alpha) = \begin{pmatrix} p & \alpha^* \\ \alpha & 1 - p \end{pmatrix} = \begin{pmatrix} \alpha + \alpha^* \\ i\alpha^* - i\alpha \\ 2p - 1 \end{pmatrix}.$$  

In this formalism, the pure states are nicely characterized in $B$ by their norm.

**Fact 9** A density matrix $\rho$ represents a pure state if and only if $\tilde{\rho} \in S$, that is, $||\tilde{\rho}|| = 1$.

Also, if $\theta \in [0, \pi]$ and $\phi \in [0, 2\pi)$ are respectively the latitude and the longitude of $\vec{v} \in S$, then the corresponding density matrix represents a pure state and satisfies $|\psi\rangle = \cos(\frac{\theta}{2})|0\rangle + \sin(\frac{\theta}{2})e^{i\phi}|1\rangle$. Observe that the pure states $|\psi\rangle$ and $|\phi\rangle$ are orthogonal if and only if $\vec{v} = -\vec{\phi}$. We will use the following notation for the six pure states along the $x$, $y$ and $z$ axes: $|\xi_+\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$, $|\xi_-\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)$, $|\xi_0\rangle = |0\rangle$, and $|\xi_1\rangle = |1\rangle$, with the respective coordinates $(\pm 1, 0, 0)$, $(0, \pm 1, 0)$ and $(0, 0, \pm 1)$ in $\mathbb{R}^3$.

For each CPSO $G$, there exists a unique affine transformation $\overline{G}$ over $\mathbb{R}^3$, which maps the ball $B$ into $B$ and is such that, for all density matrices $\rho$, $\overline{G}(\tilde{\rho}) = \overline{G}(\rho)$. Unitary superoperators have a nice characterization in $B$.

**Fact 10** The map between $U(2)/U(1)$ and $SO(3)$ that sends $\mathcal{A}$ to $\overline{\mathcal{A}}$, is an isomorphism.

For $\alpha \in (-\pi, \pi]$, $\theta \in [0, \frac{\pi}{2}]$, and $\phi \in [0, 2\pi)$, we will define the unitary transformation $R_{\alpha, \theta, \phi}$ over $\mathcal{H}_2$. If $|\psi\rangle = \cos(\frac{\theta}{2})|0\rangle + e^{i\phi}\sin(\frac{\theta}{2})|1\rangle$ and $|\psi^\perp\rangle = \sin(\frac{\theta}{2})|0\rangle - e^{i\phi}\cos(\frac{\theta}{2})|1\rangle$ then by definition $R_{\alpha, \theta, \phi}|\psi\rangle = |\psi\rangle$ and $R_{\alpha, \theta, \phi}|\psi^\perp\rangle = e^{i\alpha}|\psi^\perp\rangle$. If $A$ is a unitary superoperator then we have $A = R_{\alpha, \theta, \phi}$ for some $\alpha$, $\theta$, and $\phi$. In $\mathbb{R}^3$ the transformation $\overline{R}_{\alpha, \theta, \phi}$ is the rotation of angle $\alpha$ whose axis cuts the sphere $S$ in the opposite points $\vec{v}$.
and \( -\overrightarrow{\psi} = \overrightarrow{\psi^2} \). Note that for \( \theta = 0 \) the CPSO \( R_{\alpha,0,\phi} \) does not depend on \( \phi \). We will denote this phase rotation by \( R_{\alpha} \).

The affine transformation in \( B \) which corresponds to the Von Neumann measurement in the computational basis is the orthogonal projection to the \( z \)-axis. Therefore it maps \( \overrightarrow{\rho} = (x, y, z) \) into \((0, 0, z)\), the point which corresponds to the density matrix \( \frac{1}{2} |0\rangle \langle 0| + \frac{1}{2} |1\rangle \langle 1| \). Thus \( \text{Prob}^0[\rho] = \frac{1}{2} \).

### 6.3 Norm and Distance

Consider the space of \( n \times n \) dimensional, complex valued matrices. We define the \textit{trace norm} for this space as follows.

**Definition 13 (Trace norm)** Let \( A \in M_n(\mathbb{C}) \) be a complex valued matrix, the trace norm is defined by

\[
\|A\|_{\text{tr}} := \text{tr} \left( \sqrt{A \cdot A^*} \right)
\]

\[
= \sum_{i=1}^{n} \sigma_i,
\]

where \( A^* \) is the conjugate transpose of \( A \) and \( \sigma_1, \sigma_2, \ldots \) are the singular values of \( A \).

(See the appendix of thesis or [54] for more information on these terms.)

**Definition 14 (Euclidean norm)** For \( A \in M_n(\mathbb{C}) \) a complex valued matrix, its Euclidean norm is defined by

\[
\|A\|_2 := \sqrt{\sum_{i,j=1}^{n} |A_{ij}|^2}
\]

\[
= \sum_{i=1}^{n} \sigma_i^2,
\]

with \( \sigma_i \) the singular values of the matrix \( A \).

Both norms are \textit{matrix norms} because they obey the following properties (see Chapter 5 in [54] for much more on this topic):

1. nonnegative: \( \|A\| \geq 0 \)
2. positive: \( \|A\| = 0 \) if and only if \( A = 0 \)
3. homogeneous: \( \|\alpha A\| = |\alpha| \cdot \|A\| \) for all \( \alpha \in \mathbb{C} \)
4. triangle inequality: \( \|A + B\| \leq \|A\| + \|B\| \)
5. submultiplicative: \( \|AB\| \leq \|A\| \cdot \|B\| \).

In addition, for the tensor product between two matrices, we also have the equality

- \( \|A \otimes B\| = \|A\| \cdot \|B\| \).

A very useful relation between the trace and the Euclidean norm is easily established by the inequalities \( \sqrt{\sum_i \sigma_i^2} \leq \sum_i \sigma_i \leq \sqrt{n} \sqrt{\sum_i \sigma_i^2} \) with the summation over the \( n \) singular values. We thus have

\[
\|A\|_2 \leq \|A\|_{\text{tr}} \leq \sqrt{n} \|A\|_2
\]

for all \( A \in M_n(\mathbb{C}) \).

The trace norm has several advantages when we consider the difference between two quantum states \( \rho_1 \) and \( \rho_2 \). Given a measurement setting \( \mathcal{P} = \{P_i\} \) (with the normalization restriction \( \sum_i P_i^* P_i = I \)), a density matrix \( \rho \) induces a probability distribution \( \text{Prob}(P_i | \rho) \) over the different projectors \( P_i \). It can be shown that in this setting, the trace norm of the difference \( \rho_1 - \rho_2 \) is the maximal total variation distance between the two states:

\[
\|\rho_1 - \rho_2\|_{\text{tr}} = \max_{\mathcal{P}} \left( \sum_{P_i \in \mathcal{P}} |\text{Prob}(\rho_1 = P_i) - \text{Prob}(\rho_2 = P_i)| \right),
\]

where the maximization is taken over all measurement settings \( \mathcal{P} \). This result suggests that the expression \( \|\rho_1 - \rho_2\|_{\text{tr}} \) is a natural way of measuring the difference between the two states \( \rho_1 \) and \( \rho_2 \). The following Fact strengthens this belief.

**Fact 11** The trace-norm distance between two qubit states \( \rho_1 \) and \( \rho_2 \) is identical to the Euclidean distance between \( \tilde{\rho}_1 \) and \( \tilde{\rho}_2 \) in the Bloch ball representation:

\[
\|\rho_1 - \rho_2\|_{\text{tr}} = \|\tilde{\rho}_1 - \tilde{\rho}_2\|_2.
\]

For the density matrices \( \rho(p, \alpha) \) and \( \rho(q, \beta) \) this value is explicitly expressed by

\[
\|\rho(p, \alpha) - \rho(q, \beta)\|_{\text{tr}} = 2\sqrt{(p - q)^2 + |\alpha - \beta|^2}.
\]

### 6.4 Norms on Superoperators

**Definition 15 (Trace Induced Superoperator Norm)** For superoperators, the norm induced by the trace norm is defined as

\[
\|G\|_{\text{tr}} := \max_{X \neq 0} \left\{ \frac{\|G(X)\|_{\text{tr}}}{\|X\|_{\text{tr}}} \right\}.
\]
We will denote by $\text{dist}_{\text{tr}}$ the natural induced distance by the norm $\| \cdot \|_{\text{tr}}$:

$$\text{dist}_{\text{tr}}(F, G) := \| F - G \|_{\text{tr}} = \max_{X \neq 0} \left\{ \frac{\| F(X) - G(X) \|_{\text{tr}}}{\| X \|_{\text{tr}}} \right\}.$$ 

As $\| \cdot \|_{\text{tr}}$ is a norm, the usual properties like $\| F + G \|_{\text{tr}} \leq \| F \|_{\text{tr}} + \| G \|_{\text{tr}}$ and $\| \alpha F \|_{\text{tr}} = |\alpha| \| F \|_{\text{tr}}$ hold. Furthermore, we also have for every power $k \in \mathbb{N}$:

$$\text{dist}_{\text{tr}}(F^k, G^k) \leq k \cdot \text{dist}_{\text{tr}}(F, G),$$

which we will use later in this chapter.

### 6.5 Properties of CPSOs

Here we will establish the properties of CPSOs that we will need for the characterization of our CPSO families.

**Fact 12 (Monotonicity of the trace-norm distance [82])** Let $G$ be a completely positive, trace preserving transformation (a CPSO). The trace-norm distance between two states is non-increasing under the action of $G$:

$$\| G(\rho_1) - G(\rho_2) \|_{\text{tr}} \leq \| \rho_1 - \rho_2 \|_{\text{tr}},$$

for all quantum states $\rho_1$ and $\rho_2$.

**Proof:** First we rewrite the Hermitian difference matrix $\rho_1 - \rho_2$ according to its spectral decomposition $\rho_1 - \rho_2 = \lambda_1 \sigma_1 - \lambda_2 \sigma_2$ with $\lambda_1, \lambda_2 \geq 0$, and $\sigma_1$ and $\sigma_2$ two unit trace, Hermitian matrices that obey $\sigma_1 \sigma_2 = 0$. Because the trace of the matrix $(\rho_1 - \rho_2)$ is zero and $\| \sigma_1 - \sigma_2 \|_{\text{tr}} = 2$, we have $\lambda_1 = \lambda_2 = \frac{1}{2} \| \rho_1 - \rho_2 \|_{\text{tr}}$. We conclude the proof by using the triangle inequality and the homogeneity of the norm $\| \cdot \|_{\text{tr}}$, in combination with the requirement that the $G$ is a completely positive, trace preserving linear superoperator:

$$\| G(\rho_1 - \rho_2) \|_{\text{tr}} = \| G(\lambda_1 \sigma_1 + (-\lambda_1) \sigma_2) \|_{\text{tr}} \leq \lambda_1 \cdot \| G(\sigma_1) \|_{\text{tr}} + \lambda_1 \cdot \| G(\sigma_2) \|_{\text{tr}} = \| \rho_1 - \rho_2 \|_{\text{tr}}.$$

\[\square\]

**Definition 16 (Constant transformation)** A transformation is constant if it maps all states to the same output state.

**Fact 13** If the mixture $p \rho_1 + (1-p) \rho_2$ (with the non-degenerate probability $0 < p < 1$) is a pure state $\varphi$, then both $\rho_1$ and $\rho_2$ are identical to $\varphi$ as well.
Chapter 6. Self-Testing of Quantum Gates

Lemma 11 If a CPSO \( G : M_n(C) \to M_m(C) \) maps the totally mixed state \( \frac{1}{n}I_n \) to a pure state \( \varphi \), then \( G \) is constant.

Proof: Take an \( n \)-dimensional state \( \rho \). The density matrix \( \rho' = \frac{n+1}{n^2}I_n - \frac{1}{n}\rho \) will represent a proper state, and by linearity we know that \( \frac{1}{n+1}G(\rho) + \frac{n}{n+1}G(\rho') = G\left(\frac{1}{n}I_n\right) = |\varphi\rangle \langle \varphi| \). This is only possible if \( G(\rho) = |\varphi\rangle \langle \varphi| \) (in combination with \( G(\rho') = |\varphi\rangle \langle \varphi| \)). \( \Box \)

Lemma 12 Let \( G \) be a quantum mechanical transformation of a single qubit, and let \( \rho \) be a qubit state. If \( G \) is not constant and \( G(\rho) \) is a pure state, then \( \rho \) has to be a pure state.

Proof: Let \( \rho \) be a mixed qubit and \( G(\rho) \) a pure state \( \varphi \). We can decompose \( \rho \) always as \( \lambda|\psi\rangle\langle\psi| + (1 - \lambda)|\psi'\rangle\langle\psi'| \), with \( \frac{1}{2} \leq \lambda < 1 \) and \( |\psi\rangle \) orthogonal to \( |\psi'| \). By linearity, it follows that \( G(\rho) = (2\lambda - 1)G(|\psi\rangle\langle\psi|) + (2 - 2\lambda)G\left(\frac{1}{2}I_2\right) \) equals the pure state \( \varphi \). Because \( 0 \leq 2\lambda - 1 < 1 \) and \( 0 < 2 - 2\lambda \leq 1 \), we can conclude that \( G \) maps the total mixture \( \frac{1}{2}I_2 \) to the pure state. By the previous lemma this implies that \( G \) is constant. \( \Box \)

The space of \( 2^n \times 2^n \) matrices has dimension \( 4^n \), hence every \( n \)-qubit CPSO is uniquely defined by the images of \( 4^n \) independent states. However, the following lemma shows that for unitary transformations it is sometimes sufficient to know only \( 3^n \) images.

Lemma 13 Let \( \rho_1, \rho_2, \) and \( \rho_3 \) be three distinct qubit density matrices representing pure states, such that there is a convex combination \( \lambda_1\rho_1 + \lambda_2\rho_2 + \lambda_3\rho_3 \) that represents the totally mixed qubit \( \frac{1}{2}I_2 \). If \( G \) is a CPSO for \( n \) qubits that acts as the identity on the set \( \{\rho_1, \rho_2, \rho_3\} \otimes^n \), then \( G \) is the identity mapping \( I_{2^n} \).

Proof: Let \( P \) be the set of convex combinations of the three density matrices: \( P = \{\lambda_1\rho_1 + \lambda_2\rho_2 + \lambda_3\rho_3 | \lambda_1 + \lambda_2 + \lambda_3 = 1; \lambda_i \in [0, 1]\} \). To simplify the discussion, we suppose without loss of generality that \( P \) contains the states \( \zeta_0 \) and \( \zeta_x \). By linearity of \( G \), we know that it acts as the identity on all the states \( \rho_i \otimes \cdots \otimes \rho_n \) as long as \( \rho_i \in P \) for all \( 1 \leq i \leq n \). It will be sufficient to show that \( G \) is the identity on density matrices representing non-entangled pure states, since they form a basis for all density matrices.

For every \( k \), let \( A_k \) be the set of density matrices representing \( k \)-qubit non-entangled pure states, and let \( B_{n-k} = \{\zeta_0, \zeta_x\} \otimes^{n-k} \). We will show by induction on \( k \) that, for every \( 0 \leq k \leq n \), the CPSO \( G \) acts as the identity on \( A_k \otimes B_{n-k} \). The case \( k = 0 \) follows by the hypothesis of the lemma.

Suppose the statement is true for some \( k \). Fix \( \sigma \in A_k \) and \( \tau \in B_{n-k-1} \). For every one-qubit density matrix \( \rho \) let \( \tilde{\rho} \) denote the \( n \)-qubit density matrix \( \sigma \otimes \rho \otimes \tau \).

We now prove that \( G(\tilde{\rho}) = \tilde{\rho} \), for every \( \rho \in A_1 \). For this, we use the fact that the density matrix \( \Psi^+ \) representing the entangled EPR state \( \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \), can be written in terms of tensor products of the \( \zeta \) states:

\[
\Psi^+ = \frac{1}{2}(\zeta_x^+ \otimes \zeta_x^+ + \zeta_x^- \otimes \zeta_x^- + \zeta_y^+ \otimes \zeta_y^- + \zeta_y^- \otimes \zeta_y^+ - \zeta_y^+ \otimes \zeta_y^- - \zeta_y^- \otimes \zeta_y^+ ).
\]
6.6. Characterization of CPSO Families

This can be generalized for the pure state \(|\psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)\):

\[
\psi^+ = \frac{1}{2} (\zeta_x^+ \otimes \zeta_x^- + \zeta_x^- \otimes \zeta_x^+ + \zeta_y^+ \otimes \zeta_y^- + \zeta_y^- \otimes \zeta_y^+).
\]

If we apply the superoperator \(I_{2^n} \otimes G\) to the state \(|\psi^+\rangle\) we get:

\[
(I_{2^n} \otimes G)(|\psi^+\rangle) = +\frac{1}{2} (\zeta_x^+ \otimes \zeta_x^- + \zeta_x^- \otimes \zeta_x^+) + \frac{1}{2} (\zeta_y^+ \otimes \zeta_y^- + \zeta_y^- \otimes \zeta_y^+) - \frac{1}{2} (\zeta_y^+ \otimes G(\zeta_y^+) + \zeta_y^- \otimes G(\zeta_y^-)).
\]

If \(|\varphi\rangle\) and \(|\varphi^\perp\rangle\) are orthogonal \(n\)-qubit pure states, then let \(\Phi^-_{\varphi\varphi^\perp} = \frac{1}{\sqrt{2}}(|\varphi\rangle|\varphi^\perp\rangle - |\varphi^\perp\rangle|\varphi\rangle)\). Since \(\Phi^-_{\varphi\varphi^\perp}\) is orthogonal to all symmetric \(2n\)-qubit pure states of the form \(\psi \otimes \psi\), by projecting \((I_{2^n} \otimes G)(|\psi^+\rangle)\) to \(\Phi^-_{\varphi\varphi^\perp}\) we obtain:

\[
\langle \Phi^-_{\varphi\varphi^\perp} | (I_{2^n} \otimes G)(|\psi^+\rangle) | \Phi^-_{\varphi\varphi^\perp} \rangle = -\frac{1}{2} \langle \Phi^-_{\varphi\varphi^\perp} | \zeta_y^+ \otimes G(\zeta_y^+) | \Phi^-_{\varphi\varphi^\perp} \rangle - \frac{1}{2} \langle \Phi^-_{\varphi\varphi^\perp} | \zeta_y^- \otimes G(\zeta_y^-) | \Phi^-_{\varphi\varphi^\perp} \rangle.
\]

Since \(G\) is a completely positive, the left-hand side of this equality has to be non-negative and in the right-hand side both terms are non-positive. Therefore, for every orthogonal \(n\)-qubit pure states \(|\varphi\rangle\) and \(|\varphi^\perp\rangle\), we get

\[
\langle \Phi^-_{\varphi\varphi^\perp} | \zeta_y^+ \otimes G(\zeta_y^+) | \Phi^-_{\varphi\varphi^\perp} \rangle = \langle \Phi^-_{\varphi\varphi^\perp} | \zeta_y^- \otimes G(\zeta_y^-) | \Phi^-_{\varphi\varphi^\perp} \rangle = 0.
\]

A straightforward calculation then shows that \(G(\zeta_y^+) = \zeta_y^+\). Therefore \(G\) acts as the identity on density matrices \(\zeta_x^+\), \(\zeta_x^-\) and \(\zeta_y^+\), which generate all density matrices, and thus \(G(\hat{\rho}) = \hat{\rho}\). □

We also use the property that for CPSOs unitarity and invertibility are equivalent.

**Fact 14** Let \(G\) be a CPSO for \(n\) qubits. If there exists a CPSO \(F\) for \(n\) qubits such that \(F \circ G\) is the identity mapping, then \(G\) is a unitary superoperator.

**Proof:** See, for example, Chapter 3.8 in [78]. □

### 6.6 Characterization of CPSO Families

In this section, every CPSO will be for one qubit. First we define the notion of experimental equations, and then we show that several important CPSO families are characterizable by them.

**Definition 17 (Experimental equation)** An experimental equation in one CPSO variable, is an equation of the form

\[
\text{Prob}^0[G^k(b \langle b\rangle)] = r, \tag{6.4}
\]

where \(k\) is a nonnegative integer, \(b \in \{0, 1\}\), and \(0 \leq r \leq 1\).
We will call the left-hand side of the equation the probability term, and the right-hand side the constant term. The size of this equation is \( k \). A CPSO \( G \) will “almost” satisfy the equations if, for example, it is the result of adding small systematic and random errors (independent of time) to a CPSO that does. For \( \varepsilon \geq 0 \), the CPSO \( G \) \( \varepsilon \)-satisfies Equation 6.4 if \(|\text{Prob}^0[G^k(\langle b\rangle|) - r| \leq \varepsilon|, and when \( \varepsilon = 0 \) we will just say that \( G \) satisfies Equation 6.4. Let \( \{E\} \) be a finite set of experimental equations. If \( G \) \( \varepsilon \)-satisfies all equations in \( \{E\} \) we say that \( G \) \( \varepsilon \)-satisfies \( \{E\} \). If some \( G \) satisfies \( \{E\} \) then \( \{E\} \) is satisfiable. The set \( \{G : G \text{ satisfies } \{E\}\} \) will be denoted by \( F_{\{E\}} \). A family \( F \) of CPSOs is characterizable if it is \( F_{\{E\}} \) for some finite set \( \{E\} \) of experimental equations. In this case we say that \( \{E\} \) characterizes \( F \).

All these definitions generalize naturally for \( m \)-tuples of CPSOs for \( m \geq 2 \). In what follows we will need only the case \( m = 2 \). An experimental equation in two CPSO variables is an equation of the form

\[
\text{Prob}^0[F^{k_1} o G^{l_1} o \cdots o F^{k_t} o G^{l_t}(\langle b\rangle|)] = r,
\]

where \( k_1, \ldots, k_t, l_1, \ldots, l_t \) are nonnegative integers, \( b \in \{0, 1\} \), and \( 0 \leq r \leq 1 \).

We discuss now the existence of finite sets of experimental equations in one variable that characterize unitary superoperators, that is, the operators \( R_{\alpha, \theta, \phi} \), for \( \alpha \in (-\pi, \pi] \), \( \theta \in [0, \frac{\pi}{2}] \), and \( \phi \in [0, 2\pi) \). First observe that due to the restrictions of experimental equations, there are unitary superoperators that they cannot distinguish.

**Fact 15** Let \( \alpha \in [0, \pi] \), \( \theta \in [0, \frac{\pi}{2}] \), and \( \phi_1, \phi_2 \in [0, 2\pi) \) such that \( \phi_1 \neq \phi_2 \). Let \( \{E\} \) be a finite set of experimental equations in \( m \) variables. If

\[
(R_{\alpha, \theta, \phi_1}, G_2, \ldots, G_m) \text{ satisfies } \{E\}
\]

then there exist \( G'_2, \ldots, G'_m \) and \( G''_2, \ldots, G''_m \) such that

\[
(R_{-\alpha, \theta, \phi_1}, G'_2, \ldots, G'_m) \text{ and } (R_{\alpha, \theta, \phi_2}, G''_2, \ldots, G''_m) \text{ both satisfy } \{E\}.
\]

In the Bloch Ball formalism this corresponds to the following degrees of freedom in the choice of the orthonormal basis of \( \mathbb{R}^3 \). Since experimental equations contain exactly the states \( \langle 0\rangle |0\rangle \) and \( |1\rangle \langle 1| \) there is no freedom in the choice of the \( z \)-axis, but there is complete freedom in the choice of the \( x \) and \( y \) axes. The indistinguishability of the latitude \( \phi \) corresponds to the freedom of choosing the oriented \( x \)-axis, and the indistinguishability of the sign of \( \alpha \) corresponds to the freedom of choosing the orientation of the \( y \)-axis.

We introduce the following notations. Let \( R_{\alpha, \theta} \) denote the superoperator family \( \{R_{\pm \alpha, \theta, \phi} | \phi \in [0, 2\pi]\} \). For \( \phi \in [0, 2\pi) \), let the Not transformation be defined by \( \text{Not}_\phi(0) = e^{i\phi} |1\rangle \) and \( \text{Not}_\phi(e^{i\phi}|1\rangle) = |0\rangle \), and recall that the Hadamard transformation \( H_\phi \) obeys \( H_\phi(0) = \frac{1}{\sqrt{2}} (|0\rangle + e^{i\phi}|1\rangle) \) and \( H_\phi(e^{i\phi}|1\rangle) = \frac{1}{\sqrt{2}} (|0\rangle - e^{i\phi}|1\rangle) \). Observe that \( H_\phi = R_{\pi, \frac{\pi}{2}, \phi} \) and \( \text{Not}_\phi = R_{\pi, \frac{\pi}{2}, \phi} \) for \( \phi \in [0, 2\pi) \). Finally, let \( \{H_\phi\} = \{H_\phi | \phi \in [0, 2\pi]\} \), and \( \{\text{Not}_\phi\} = \{\text{Not}_\phi | \phi \in [0, 2\pi]\} \).
Since the sign of $\alpha$ cannot be determined, we will assume that $\alpha$ is in the interval $[0, \pi]$. We will also consider only unitary superoperators such that $\frac{\alpha}{\pi}$ is rational. This choice is good enough since these superoperators form a dense subset of all unitary superoperators. For such a unitary superoperator, let $n_\alpha$ be the smallest positive integer $n$ for which $n\alpha = 0 \mod 2\pi$. Then either $n_\alpha = 1$, or $n_\alpha \geq 2$ and there exists $t \geq 1$ which is coprime with $n_\alpha$ such that $\alpha = (\frac{1}{n_\alpha})2\pi$. Observe that the case $n_\alpha = 1$ corresponds to the identity superoperator.

Our first theorem shows that almost all families $R_{\alpha,\theta}$ are characterizable by some finite set of experimental equations. In particular $\{H_\phi\}$ is characterizable.

**Theorem 10** Let $(\alpha, \theta) \in (0, \pi] \times (0, \frac{\pi}{2}) \setminus \{(\pi, \frac{\pi}{2})\}$ be such that $\frac{\alpha}{\pi}$ is rational. Let $z_k(\alpha, \theta) = \cos^2 \theta + \sin^2 \theta \cos(k\alpha)$. Then the following experimental equations characterize $R_{\alpha,\theta}$:

\[
\text{Prob}^0|G^n_\alpha(11)\rangle = 0 \quad \text{and} \quad \text{Prob}^0|G^k_\alpha(00)\rangle = \frac{1}{2} + \frac{1}{2}z_k(\alpha, \theta),
\]

for $k \in \{1, \ldots, n_\alpha\}$.

**Proof:** First observe that every CPSO in $R_{\alpha,\theta}$ satisfies the equations of the theorem since the z-coordinate of $R^k_{\alpha,\theta,\phi}(|0\rangle\langle 0|)$ is $z_k(\alpha, \theta)$ for every $\phi \in [0, 2\pi)$. Let $G$ be a CPSO that satisfies these equations. We will prove that $G$ is a unitary superoperator. Then, Fact 16 implies that $G \in R_{\alpha,\theta}$.

Since $z_1(\alpha, \theta) \neq \pm 1$, we know $G(|0\rangle\langle 0|) \notin \{|0\rangle\langle 0|, |1\rangle\langle 1|\}$. Observing that $G^n_\alpha(|0\rangle\langle 0|) = |0\rangle\langle 0|$, Lemma 12 implies that $G(|0\rangle\langle 0|)$ is a pure state. Thus $|0\rangle\langle 0|$, $|1\rangle\langle 1|$, and $G(|0\rangle\langle 0|)$ are distinct pure states, and since $G^n_\alpha$ acts as the identity on them, by Lemma 13 it is the identity mapping. Hence by Fact 14 $G$ is a unitary superoperator. \hfill \Box

**Fact 16** Let $\alpha \in (0, \pi]$, $\theta \in (0, \frac{\pi}{2})$, $\alpha' \in (-\pi, \pi]$, $\theta' \in (0, \frac{\pi}{2})$, with $\frac{\alpha}{\pi}$ a rational and $n_\alpha$ the smallest positive integer such that $n_\alpha \alpha = 0 \mod 2\pi$, and let $z_k$ be the function $z_k(\alpha, \theta) = \cos^2 \theta + \sin^2 \theta \cos(k\alpha)$. If $z_k(\alpha, \theta) = z_k(\alpha', \theta')$, for $k \in \{1, \ldots, n_\alpha\}$, then $\alpha' = \alpha$ and $\theta' = \theta$.

The remaining families $R_{\alpha,\theta}$ for which $\frac{\alpha}{\pi}$ is rational are $\{R_{\pm,\alpha}, R_{\alpha}\}$, for $\alpha \in [0, \pi]$, and $\{\text{Not}_\phi\}$. Let us recall that $M$ is the CPSO that represents the Von Neumann measurement in the computational basis. Since $M$ satisfies exactly the same equations as $R_{\pm,\alpha}$, and $\text{Not}_\phi \circ M$ satisfies exactly the same equations as $\text{Not}_\phi$, for every $\phi \in [0, 2\pi)$, these families are not characterizable by experimental equations in one variable. Nevertheless it turns out that together with the family $\{H_\phi\}$ they become characterizable. This is stated in the following theorem.

**Theorem 11** The family $\{(H_\phi, \text{Not}_\phi)|\phi \in [0, 2\pi)\} \subset \{H_\phi\} \times \{\text{Not}_\phi\}$ is character-
ized by the experimental equations in two variables \((F, G)\):

\[
\begin{aligned}
\text{Prob}^0[F(\langle 0 | 0 \rangle)] &= \frac{1}{2} \\
\text{Prob}^0[F^2(\langle 0 | 0 \rangle)] &= 1 \\
\text{Prob}^0[F^2(\langle 1 | 1 \rangle)] &= 0 \\
\text{Prob}^0[G(\langle 0 | 0 \rangle)] &= 0 \\
\text{Prob}^0[G(\langle 1 | 1 \rangle)] &= 1 \\
\text{Prob}^0[F \circ G \circ F(\langle 0 | 0 \rangle)] &= 1.
\end{aligned}
\]

If \(\alpha \) is rational, then the family \(\{H_\alpha\} \times \{R_{\pm \alpha}\}\) is characterized by the experimental equations in two variables \((F, G)\):

\[
\begin{aligned}
\text{Prob}^0[F(\langle 0 | 0 \rangle)] &= \frac{1}{2} \\
\text{Prob}^0[F^2(\langle 0 | 0 \rangle)] &= 1 \\
\text{Prob}^0[F^2(\langle 1 | 1 \rangle)] &= 0 \\
\text{Prob}^0[G(\langle 0 | 0 \rangle)] &= 1 \\
\text{Prob}^0[G(\langle 1 | 1 \rangle)] &= 0 \\
\text{Prob}^0[F \circ G^\alpha \circ F(\langle 0 | 0 \rangle)] &= 1 \\
\text{Prob}^0[F \circ G \circ F(\langle 0 | 0 \rangle)] &= \frac{1}{2} + \frac{1}{2} \cos \alpha.
\end{aligned}
\]

**Proof:** By the previous theorem, \(H_\phi\) is characterized by the first three experimental equations involving \(F\). Because of this we know that \(F|0\rangle \langle 0|\) corresponds to the pure state \(\zeta^\phi = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi}|1\rangle)\).

In combination with the knowledge that \(G \circ F|0\rangle \langle 0|\) also yields the state \(\zeta^\phi\), this tells us that \(G\) acts as the identity on \(\zeta^\phi\). Consider now the combined CPSO \(\text{Not}_\phi \circ G\).

This operator acts as the identity on the three density matrices \(|0\rangle \langle 0|, |1\rangle \langle 1|, \zeta^\phi\), which, following Lemma 13, implies that \(\text{Not}_\phi \circ G\) is indeed \(I_2\). This is only possible if \(G\) equals \(\text{Not}_\phi\).

For the second part of the theorem, we employ a proof method of similar vein. Because \(F|0\rangle \langle 0| = \zeta^\phi\) and \(F \circ G^\alpha \circ F(\langle 0 | 0 \rangle) = |0 \rangle \langle 0|\), We know that \(G^\alpha\) acts as the identity on the pure state \(\zeta^\phi\), and hence (using \(G|0\rangle \langle 0| = |0 \rangle \langle 0|\) and \(G|1\rangle \langle 1| = |1 \rangle \langle 1|\)) that \(G^\alpha\) is \(I_2\), which is only possible if \(G\) is unitary. The eigenvectors of the \(U(2)/U(1)\) rotation associated with \(G\) are \(|0\rangle\) and \(|1\rangle\), and because the \(n_\alpha\)-th power of \(G\) is the identity, its two eigenvalues have to obey \(\lambda_0^{n_\alpha} = \lambda_1^{n_\alpha}\). By the probability \(\text{Prob}^0[F \circ G \circ F(\langle 0 | 0 \rangle)] = \frac{1}{2} + \frac{1}{2} \cos \alpha\) it follows that \(\lambda_1 = \lambda_0 e^{\pm i \alpha}\). Hence \(G\) equals \(R_\alpha\) or \(R_{-\alpha}\). \(\Box\)
6.7 Characterization of CNot gates

In this section we will extend our theory of characterization of CPSO families for several qubits. In particular, we will show that the family of CNot gates together with the family \( \{ H_\phi \} \) is characterizable. First we need some definitions.

For every \( \phi \in [0, 2\pi) \), we define CNot\(_\phi\) as the only unitary transformation over \( \mathbb{C}^4 \) satisfying CNot\(_\phi\)(\(|0\rangle\langle \psi|\)) = \(|0\rangle\langle \psi|\) and CNot\(_\phi\)(\(|1\rangle\langle \psi|\)) = \(|1\rangle\langle \psi|\), for all \(|\psi\rangle \in \mathcal{H}_2\).

We extend the definition of the experimental equation for CPSOs given in Equation 6.5 for \( n \) qubits. It is an equation of the form

\[
\text{Prob}^v[F^{k_1} \circ G^{l_1} \circ \cdots \circ F^{k_2} \circ G^{l_2}(|w\rangle\langle w|)] = r,
\]

(6.5)

where in addition to the notation of Equation 6.5 \( v, w \in \{0, 1\}^n \), and \( \text{Pr}^v \) is the probability of measuring \(|\psi\rangle\langle \psi|\). For the variables \( F \) and \( G \) of Equation 6.5, we also allow both the tensor product of two CPSO variables and the tensor product of a CPSO variable with the identity. We now state the characterization.

**Theorem 12** The family \( \{(H_\phi, \text{CNot}_\phi) | \phi \in [0, 2\pi) \} \) is characterized by the experimental equations in two variables \((F, G)\):

\[
\begin{align*}
\text{Prob}^0[F(|0\rangle\langle 0|)] &= \frac{1}{2} \\
\text{Prob}^0[F^2(|0\rangle\langle 0|)] &= 1 \\
\text{Prob}^0[F^2(|1\rangle\langle 1|)] &= 0 \\
\text{Prob}^{00}[G(|00\rangle\langle 00|)] &= 1 \\
\text{Prob}^{01}[G(|01\rangle\langle 01|)] &= 1 \\
\text{Prob}^{10}[G(|10\rangle\langle 10|)] &= 1 \\
\text{Prob}^{11}[G(|11\rangle\langle 11|)] &= 1 \\
\text{Prob}^{00}[G \circ (I_2 \otimes F) \circ (I_2 \otimes F)(|00\rangle\langle 00|)] &= 1 \\
\text{Prob}^{10}[G \circ (I_2 \otimes F) \circ (I_2 \otimes F)(|10\rangle\langle 10|)] &= 1 \\
\text{Prob}^{00}[G \circ (F \otimes I_2) \circ (F \otimes I_2)(|00\rangle\langle 00|)] &= 1 \\
\text{Prob}^{01}[G \circ (F \otimes I_2) \circ (F \otimes I_2)(|01\rangle\langle 01|)] &= 1 \\
\text{Prob}^{00}[G \circ (F \otimes F) \circ (F \otimes F)(|00\rangle\langle 00|)] &= 1.
\end{align*}
\]

**Proof:** Let \( F \) and \( G \) satisfy these equations. By Theorem 10, with \( \alpha = \pi \) and \( \theta = \frac{\pi}{4} \), the first three equations imply that \( F = H_\phi \), for some \( \phi \in [0, 2\pi) \). Using Lemma 13, the remaining equations imply that \( G^2 = I_4 \), and it follows from Fact 14 that \( G \) is a unitary CPSO. A straightforward verification then shows that indeed \( G = \text{CNot}_\phi \). 

\[\square\]
6.8 Robustness

In this section we introduce the notion of robustness for experimental equations which will be the crucial ingredient for proving self-testability. From now on, \( \{ E \} \) will always denote a such a set of equations.

First we define the notion of the distance between a CPSO and a family of gates.

**Definition 18** The distance between a CPSO \( G \) and a set \( \mathcal{F} \) of gates is defined by the minimization

\[
\text{dist}_{\text{tr}}(G, \mathcal{F}) := \min_{F \in \mathcal{F}} \text{dist}_{\text{tr}}(G, F).
\]

For a Euclidean metric, this distance would express the length of the shortest line between a point and a set. We use this generalized distance to define a notion of 'robustness' for a set of experimental equations.

**Definition 19 (Robustness)** Let \( \varepsilon, \delta \geq 0 \), and let \( \{ E \} \) be a set of experimental equations. We say that \( \{ E \} \) is \((\varepsilon, \delta)\)-robust if whenever a CPSO \( G \) \( \varepsilon \)-satisfies \( \{ E \} \), we have

\[
\text{dist}_{\text{tr}}(G, \mathcal{F}_{\{ E \}}) \leq \delta.
\]

When a CPSO family is characterized by a finite set of experimental equations \( \{ E \} \), one would like to prove that \( \{ E \} \) is robust. The next theorem shows that this is the case for \( \delta \in O(\varepsilon^{1/k}) \) with \( k \) depending on \( \{ E \} \).

**Theorem 13** Let \( \{ E \} \) be a finite satisfiable set of experimental equations. Then there exists an integer \( k \geq 1 \) and a real \( C > 0 \) such that for all \( \varepsilon \geq 0 \), \( \{ E \} \) is \((\varepsilon, C\varepsilon^{1/k})\)-robust.

**Proof:** We will use basic notions from algebraic geometry for which we refer the reader for example to [18]. In the proof, \( \mathbb{C} \) is identified with \( \mathbb{R}^2 \). Then the set \( \mathcal{K} \) of CPSOs for a fixed number of qubits is a real compact semi-algebraic set. Suppose that in \( \{ E \} \) there are \( d \) equations. Let \( f : \mathcal{K} \to \mathbb{R} \) be the function that maps the CPSO \( G \) to the maximum of the magnitudes of the difference between the probability term and the constant term of the \( i \)th equation in \( \{ E \} \), for \( i = 1, \ldots, d \). By definition of \( f \), we get

\[
f^{-1}(0) = \mathcal{F}_{\{ E \}}.
\]

Moreover, \( f \) is a continuous semi-algebraic function, since it is the maximum of the magnitudes of polynomial functions in the (real) coefficients of \( G \).

Let \( g : \mathcal{K} \to \mathbb{R} \) defined in \( G \) by \( g(G) = \text{dist}_{\text{tr}}(G, \mathcal{F}_{\{ E \}}) \). Since \( \mathcal{K} \) is a compact semi-algebraic set, \( g \) is a continuous semi-algebraic function. Moreover, for all \( G \in \mathcal{K} \), we have \( f(G) = 0 \) if and only if \( g(G) = 0 \). Then Fact 17 concludes the proof.

For a proof of the following fact, see for example [18, Prop. 2.3.11].

**Fact 17 (Lojasiewicz's inequality)** Let \( X \subseteq \mathbb{R}^m \) be a compact semi-algebraic set. Let \( f, g : X \to \mathbb{R} \) be two continuous semi-algebraic functions. Assume that for all \( x \in X \), if \( f(x) = 0 \) then \( g(x) = 0 \). Then there exists an integer \( k \geq 1 \) and a real \( C > 0 \) such that, for all \( x \in X \), \( |g(x)|^k \leq C|f(x)| \).
In some cases we can explicitly compute the constants C and k of Theorem 13. We will illustrate these techniques with the equations in Theorem 10 for the case α = π and θ = π/4. Let us recall that these equations characterize the set \{H_φ\}.

**Lemma 14** For every 0 ≤ ε ≤ 1, the following equations are (ε, 1824\sqrt{ε})-robust:

\[
\text{Prob}^0[G(|0\rangle\langle 0|)] = \frac{1}{2}, \quad \text{Prob}^0[G^2(|0\rangle\langle 0|)] = 1, \quad \text{and} \quad \text{Prob}^0[G^2(|1\rangle\langle 1|)] = 0.
\]

**Proof:** Let G be a CPSO that ε-satisfies the equations. First we will show there is a point \(\overline{p} \in S\) with z-coordinate 0 whose distance from \(G(|0\rangle\langle 0|)\) is at most 10\sqrt{ε}. The last two equations imply that ||G^2(|b\rangle\langle b|) - |b\rangle\langle b||_tr ≤ 3\sqrt{ε}, for b = 0, 1. Therefore \(\|G^2(|0\rangle\langle 0|) - G^2(|1\rangle\langle 1|)\|_tr ≥ 2 - 6\sqrt{ε}\), and by Fact 12 we have \(\|G(|0\rangle\langle 0|) - G(|1\rangle\langle 1|)\|_tr ≥ 2 - 6\sqrt{ε}\). Thus \(\|G(|b\rangle\langle b|)\|_2 ≥ 1 - 6\sqrt{ε}\), for b = 0, 1. Let \(\tau = \rho(p, \alpha)\), where G(|0\rangle\langle 0|) = \rho(p, \alpha). The first equation implies that \(\|G - \rho\|_2 ≤ 2\epsilon\). Therefore, for \(\overline{p} = \overline{\tau}/\|\overline{\tau}\|_2\) we get \(\|G(|0\rangle\langle 0|) - \rho\|_tr ≤ 10\sqrt{ε}\).

The point \(\overline{p}\) on S uniquely defines \(\phi \in [0, 2\pi]\) such that \(H_φ(|0\rangle\langle 0|) = \overline{p}\). One can verify that \(H_φ^{-1} \circ G\) acts as the identity with error at most 19\sqrt{ε} on the four density matrices \(|0\rangle\langle 0|, |1\rangle\langle 1|, H_φ(|0\rangle\langle 0|),\) and \(H_φ(|1\rangle\langle 1|)\). From Lemma 16 we conclude that \(\|G - H_φ\|_tr ≤ 1824\sqrt{ε}\).

**Lemma 15** Let G be a superoperator on \(M_2(\mathbb{C})\). Let 0 ≤ ε ≤ 1 be such that \(\|G(\xi^\pm) - \xi^\pm\|_tr, \|G(\zeta^\pm_x) - \zeta^\pm_x\|_tr, \|G(\zeta^\pm_y) - \zeta^\pm_y\|_tr \leq \varepsilon\); then \(\|G - I_2\|_tr ≤ \sqrt{10}\varepsilon\).

**Proof:** Define a four dimensional basis \(\{b_i\}\) for the linear space \(\mathbb{C}^{2\times 2}\) by \(b_1 = \xi^+, b_2 = \zeta^+_x, b_3 = \zeta^+_y - \zeta^-_x\) and \(b_4 = \zeta^-_y - \zeta^-_x\). Any \(2 \times 2\) complex valued matrix can now be expressed as \(M_\alpha = \sum \alpha_i b_i\), with \(\alpha_i \in \mathbb{C}\). This implies for the trace norm of the matrix \(\|M_\alpha\|_tr ≥ \|M_\alpha\|_2 = \sqrt{|\alpha_1|^2 + |\alpha_2|^2 + |\alpha_3|^2 + |\alpha_4|^2}\). By the assumption of the lemma we have \(\|(G - I_2)(b_1)\|_tr, \|(G - I_2)(b_2)\|_tr ≤ \varepsilon\), and also \(\|(G - I_2)(b_3)\|_tr, \|(G - I_2)(b_4)\|_tr ≤ 2\varepsilon\). Combining these bounds yields

\[
\|(G - I_2)(M_\alpha)\|_tr ≤ \|(\alpha_1 + \alpha_2 + 2|\alpha_3| + 2|\alpha_4|)\varepsilon\).
\]

We are thus left to maximize the fraction

\[
\frac{\|(G - I_2)(M_\alpha)\|_tr}{\|M_\alpha\|_tr} ≤ \frac{(|\alpha_1| + |\alpha_2| + 2|\alpha_3| + 2|\alpha_4|)\varepsilon}{\sqrt{|\alpha_1|^2 + |\alpha_2|^2 + |\alpha_3|^2 + |\alpha_4|^2}}
\]

over all \(\alpha_i \in \mathbb{C}\). Clearly, we can assume all \(\alpha\)-coefficients to be nonnegative reals and impose the restriction \(\sum \alpha_i^2 = 1\). With the use of Lagrange multipliers one can now prove without much effort that the above fraction cannot be bigger than \(\sqrt{10}\varepsilon\) (which is established by the values \(\alpha_1 = \alpha_2 = \sqrt{\frac{1}{10}}\) and \(\alpha_3 = \alpha_4 = \sqrt{\frac{1}{10}}\)).

**Lemma 16** Let u and v represent two pure qubit states (and \(u^\perp\) and \(v^\perp\) the respective orthogonal dual states), with \(|\langle u|v\rangle|^2 = \frac{1}{2}\). If G is a one-qubit CPSO such that \(\|G(x) - x\|_tr ≤ \varepsilon\) for 0 ≤ \(\varepsilon ≤ 1\) and all \(x \in \{u, v, u^\perp, v^\perp\}\), then \(\|G - I_2\|_tr ≤ 96\varepsilon\).
Chapter 6. Self-Testing of Quantum Gates

**Proof:** We can suppose without loss of generality that $u = \zeta^+_x$ and $v = \zeta^+_z$. Consider the state $\rho = G(\zeta^+_y)$, with its three parameters $x, y, z$ in

$$
\rho = \frac{1}{2} \left[ \begin{array}{cc} 1 + z & x - iy \\ x + iy & 1 - z \end{array} \right].
$$

From Fact 12 it follows that $\|G(\zeta^+_+) - \rho\|_{\text{tr}} \leq \|\zeta^+_z - \zeta^+_y\|_{\text{tr}} = \sqrt{2}$. By the assumption of this lemma we have that $\|G(\zeta^+_+) - \zeta^+_z\|_{\text{tr}} \leq \varepsilon$, and hence $\|\zeta^+_z - \rho\|_{\text{tr}} \leq \sqrt{2} + \varepsilon$. The same relation holds also for the other three fixed points $\zeta^+_x$, $\zeta^+_z$, and $\zeta^+_x$. As a result, the three coordinates of $\rho$ have to obey the four inequalities

$$
x^2 + y^2 + (z \pm 1)^2 \quad \text{and} \quad (x \pm 1)^2 + y^2 + z^2 \leq (\sqrt{2} + \varepsilon)^2 \leq 2 + 4\varepsilon \quad (6.6)
$$

A second set of restrictions on $(x, y, z)$ comes from the complete positivity of $G$. Like in the proof of Lemma 13 we use the decomposition of the EPR state $\Psi^+$, to analyze the two-qubit state:

$$(I_2 \otimes G)(\Psi^+) = -\frac{1}{2}(\zeta^+_y \otimes G(\zeta^+_z) + \zeta^+_z \otimes G(\zeta^+_y)) + \frac{1}{2}(\zeta^+_y \otimes G(\zeta^+_z) + \zeta^+_z \otimes G(\zeta^+_y)) + \frac{1}{2}(\zeta^+_y \otimes G(\zeta^+_z) + \zeta^+_z \otimes G(\zeta^+_y)).$$

Using the hypothesis, the projection of this state onto the anti-symmetrical entangled qubit pair $|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ yields

$$
\langle \Phi^- | (I_2 \otimes G)(\Psi^+) | \Phi^\pm \rangle \leq 2\varepsilon - \frac{1}{2} \langle \Phi^- | \zeta^+_y \otimes G(\zeta^+_z) | \Phi^- \rangle - \frac{1}{2} \langle \Phi^- | \zeta^+_y \otimes G(\zeta^+_y) | \Phi^- \rangle.
$$

Since $G$ is a CPSO, as in Lemma 13 we get $\langle \Phi^- | \zeta^+_y \otimes \rho | \Phi^\pm \rangle \leq 4\varepsilon$. A straightforward calculation shows that this last relation is equivalent with a restriction on the $y$ coordinate: $y \geq 1 - 16\varepsilon$.

This last inequality implies $y^2 \geq 1 - 32\varepsilon$, which combined with the restrictions of Equation 6.6, leads to the conclusion that $(x \pm 1)^2 \leq 2 + 4\varepsilon - y^2 - z^2 \leq 1 + 36\varepsilon$, and similarly $(z \pm 1)^2 \leq 1 + 36\varepsilon$. The $x$ and $z$ coordinates of $\rho$ satisfy $|x|, |z| \leq 18\varepsilon$. Together these bounds imply

$$
\|G(\zeta^+_y) - \zeta^+_y\|_{\text{tr}} = \sqrt{x^2 + (y - 1)^2 + z^2} \leq \sqrt{904\varepsilon}.
$$

The same result can be proved for $\zeta^+_y$. Therefore by Lemma 15 we can conclude the proof.

\[ \square \]

6.9 Quantum Self-Testers

In this final section we formally define our testers and establish the relationship between robust equations and testability. The experimental oracle $O[G]$ for $G$ is a probabilistic procedure that takes inputs $(b, k) \in \{0, 1\} \times \mathbb{N}$ and generates outcomes from
the set \{0, 1\} such that for every input bit \(b\) and size \(k\)
\[
\Pr[\mathcal{O}[G](b, k) = 0] = \text{Prob}^0[G^k(|b\rangle\langle b|)].
\]

An oracle program \(T\) with an experimental oracle \(\mathcal{O}[G]\) is a program denoted by \(T^{\mathcal{O}[G]}\) that can ask queries to the experimental oracle in the following sense. When \(T\) presents a query \((b, k)\) to the oracle, it receives the probabilistic outcome of \(\mathcal{O}[G]\) in one computational step. A query to the experimental oracle thus captures the notion of a single experimental run of the black-box \(G\).

**Definition 20 (Tester)** Let \(\mathcal{F}\) be a family of CPSOs, and let \(0 < \delta_1 \leq \delta_2 < 1\). A \((\delta_1, \delta_2)\)-tester for \(\mathcal{F}\) is a probabilistic oracle program \(T\) such that for every CPSO \(G\),

- if \(\text{dist}_{tr}(G, \mathcal{F}) \leq \delta_1\) then \(\Pr[T^{\mathcal{O}[G]} \text{ says PASS}] \geq \frac{2}{3}\),
- if \(\text{dist}_{tr}(G, \mathcal{F}) > \delta_2\) then \(\Pr[T^{\mathcal{O}[G]} \text{ says FAIL}] \geq \frac{2}{3}\),

where the probability is the expectation over the outcomes of the experimental oracle and the internal coin tosses of the program.

**Theorem 14** Let \(\epsilon, \delta > 0\), and let \(\{E\}\) be a satisfiable set of \(d\) experimental equations such that the size of every equation is at most \(k\). If \(\{E\}\) is \((\epsilon, \delta)\)-robust then there exists an \((\frac{\epsilon}{3k}, \delta)\)-tester for \(\mathcal{F}_{\{E\}}\) that makes \(O(d \log(d)/\epsilon^2)\) queries.

**Proof:** We will describe a probabilistic oracle program \(T\). Let \(G\) be a CPSO. We can suppose that for every equation in \(\{E\}\), \(T\) has a rational number \(r\) such that \(|\bar{r} - r| \leq \frac{\delta}{8}\), where \(r\) is the constant term of the equation. By sampling the oracle \(\mathcal{O}[G]\), for every equation in \(\{E\}\), \(T\) obtains a value \(\bar{p}\) such that \(|\bar{p} - p| \leq \frac{\delta}{8}\) with probability at least \(1 - \frac{1}{3d^2}\), where \(p\) is the probability term of the equation. A standard Chernoff bound argument shows that this is feasible with \(O(\log(d)/\epsilon^2)\) queries for each equation. If for every equation \(|\bar{p} - \bar{r}| \leq \frac{\delta}{3}\), then \(T\) says PASS, otherwise \(T\) says FAIL. Using the robustness of \(\{E\}\) and Lemma 17, one can verify that \(T\) is a \((\frac{\epsilon}{3k}, \delta)\)-tester for \(\mathcal{F}_{\{E\}}\).

**Lemma 17** Let \(\{E\}\) be a finite satisfiable set of experimental equations such that the size of every equation is at most \(k\), and let \(G\) be a CPSO. For every \(\epsilon > 0\), if \(\text{dist}_{tr}(G, \mathcal{F}_{\{E\}}) \leq \epsilon\) then \(G\) \((k\epsilon)\)-satisfies \(\{E\}\).

**Proof:** Let \(F\) be the CPSO in \(\mathcal{F}\) such that \(\text{dist}_{tr}(G, F) \leq \epsilon\). Then \(\text{dist}_{tr}(G^j, F^j) \leq j\epsilon\) for every \(j \in \mathbb{N}\). Hence, by the maximum size \(k\) of the experimental equations \(\{E\}\), the lemma follows.

Our main result is the consequence of Theorems 10, 11, 12, 13, 14, and Lemma 14.

**Theorem 15** Let \(\mathcal{F}\) be one of the following families:

- \(\mathcal{R}_{\alpha, \theta}\) for \((\alpha, \theta) \in (0, \pi) \times (0, \frac{\pi}{2}) \setminus \{(\pi, \frac{\pi}{2})\}\) where \(\frac{\alpha}{\pi}\) is rational,
Chapter 6. Self-Testing of Quantum Gates

- \{(H_\phi, \text{Not}_\phi) | \phi \in [0, 2\pi)\},
- \{H_\phi \times \{R_{\pm \alpha} \} \text{ for } \alpha \pi \text{ rational},
- \{(H_\phi, \text{CNot}_\phi) | \phi \in [0, 2\pi)\},
- \{(H_\phi, R_{s\pi/4}, \text{CNot}_\phi) | \phi \in [0, 2\pi), s = \pm 1\}.

Then there exists an integer \(k \geq 1\) and a real \(C > 0\) such that, for all \(\varepsilon > 0\), \(\mathcal{F}\) has an \((\varepsilon, C\varepsilon^{1/k})\)-tester that makes \(O(1/\varepsilon^2)\) queries. Moreover, for every \(0 < \varepsilon \leq 1\), \(\{H_\phi\}\) has an \((\varepsilon, 1824\sqrt{\varepsilon})\)-tester that makes \(O(1/\varepsilon^2)\) queries.

Note that each triplet of the last family forms a universal and fault-tolerant set of quantum gates[26].