# Self-Testing of Universal and Fault-Tolerant Sets of Quantum Gates

*Wim van Dam** *Frédéric Magniez*† *Michele Mosca*‡ *Miklos Santha*§

**Abstract**

We consider the design of self-testers for quantum gates. A self-tester for the gates $\boldsymbol{F}_1, \ldots, \boldsymbol{F}_m$ is a classical procedure that, given any gates $\boldsymbol{G}_1, \ldots, \boldsymbol{G}_m$, decides with high probability if each $\boldsymbol{G}_i$ is close to $\boldsymbol{F}_i$. 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 c-NOT gate, and a phase rotation gate of angle $\pi/4$ is self-testable.

## 1 Introduction

In the last decade quantum computing has become an extremely active research area. The initial idea that the simulation of quantum physical systems might be out of reach for classical devices goes back to Feynman[18]. He raised the possibility that computational devices based on the principles of quantum mechanics might be more powerful than classical ones. This challenge to the quantitative version of the Church-Turing thesis, which asserts that all physically realisable computational devices can be simulated with only a polynomial overhead by a probabilistic Turing machine, is the driving force behind the study of quantum computers and algorithms.

The first formal models of quantum computing, the quantum Turing machine and quantum circuits were defined by Deutsch[13, 14]. Yao has shown[35] that these two models have polynomially equivalent computational power when the circuits are uniform. In a sequence of papers oracles have been exhibited [16, 7, 9, 34], relative to which quantum Turing machines are more powerful than classical (probabilistic or non-deterministic) ones. These results culminated in the seminal paper of Shor[33] where he gave polynomial time quantum algorithms for the factoring and the discrete logarithm problems.

A quantum circuit operates on $n$ quantum bits (qubits), where $n$ is some integer. The actual computation takes place in the Hilbert space $\mathbb{C}^{\{0,1\}^n}$ whose computational basis consists of the $2^n$ orthonormal vectors $|i\rangle$ for $i \in \{0,1\}^n$. According to the standard model, during the computation the state of the system is a unit length linear superposition of the basis states. The computational steps of the system are done by quantum gates which perform unitary operations and are local in the sense that they involve only a constant number of qubits. At the end of the computation a measurement takes place on one of the qubits. This is a probabilistic experiment whose outcome can be 0 or 1, and the probability of measuring the bit $b$ is the squared length of the projection of the superposition to the subspace spanned by the basis states that are compatible with the outcome. As a result of a measurement, the state of the system becomes this projected state.

The most convenient way to describe all possible operations on a quantum register is in the formalism of 'density matrices'. In this approach, which differs from the Dirac notation, the quantum operations are described by completely positive superoperators (CPSOs) that act on matrices. These density matrices describe mixed states (that is, classical probability distributions over pure quantum states), and the CPSOs

*C.W.I. Amsterdam; Centre for Quantum Computation, University of Oxford. wimvdam@qubit.org
†Université Paris Sud, LRI. magniez@lri.fr
‡University of Waterloo; Centre for Quantum Computation, University of Oxford. mosca@qubit.org
§CNRS, Université Paris Sud, LRI. santha@lri.fr

correspond exactly to all the physically allowed transformations on them. Such a model of quantum circuits with mixed states was described by Aharonov, Kitaev and Nisan[3], and we will adopt it here. The unitary quantum gates of the standard model and measurements are special CPSOs. CPSOs can be simulated by unitary quantum gates on a larger number of qubits, and in [3] it was shown that the computational powers of the two models are polynomially equivalent.

Unitary quantum gates for small number of qubits have been extensively studied. One reason is that although quantum gates for up to three qubits have already been built, constructing gates for large numbers seems to be elusive. Another reason is that universal sets of gates can be built from them, which means that they can simulate (approximately) any unitary transformation on an arbitrary number of qubits. The first universal quantum gate which operates on three qubits was identified by Deutsch[14]. After a long sequence of work on universal quantum gates [17, 4, 15, 24, 6, 32, 21, 20], Boykin et al.[8] have recently shown that the set consisting of a Hadamard gate, a c-NOT gate, and a phase rotation gate of angle $\pi/4$ is universal. In order to form a practical basis for quantum computation, a universal set must also be able to operate in a noisy environment, and therefore has to be fault-tolerant[32, 2, 20, 22]. The above set of three gates has the additional advantage of also being fault-tolerant.

Experimental procedures for determining the properties of quantum "black boxes" were given by Chuang and Nielsen[12] and Poyatos, Cirac and Zoller[26], however these procedures implicitly require apparatus that has already been tested and characterized.

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[25] have designed tests for deciding if a photon source is perfect. These tests guarantee that if source passes them then it is adequate for the security of the Bennett-Brassard[5] quantum key distribution protocol.

In this paper we develop the theory of self-testing of quantum gates by classical procedures. Given a CPSO $\boldsymbol{G}$ for $n$ qubits, and a family $\mathcal{F}$ of unitary CPSOs, we would like to decide if $\boldsymbol{G}$ belongs to $\mathcal{F}$. Intuitively, a self-tester is a procedure that answers the question "$\boldsymbol{G} \in \mathcal{F}$ ?" by interacting with the CPSO $\boldsymbol{G}$ in a purely classical way. More precisely, it will be a probabilistic algorithm that is able to access $\boldsymbol{G}$ as a black box in the following sense: it can prepare the classical states $w \in \{0,1\}^n$, iterate $\boldsymbol{G}$ 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 $\boldsymbol{G}$: 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 $\boldsymbol{G}$ 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 $\boldsymbol{G}$, whenever the distance of $\boldsymbol{G}$ 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[10], Rubinfeld[28], Lipton[23] and Gemmel et al.[19]. 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 function from the given family. This clearly inspired the definition of our self-testers which have the particularity that they should test quantum objects that they can access only in some particular way. 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[29] and by Rubinfeld[30]. It will play a crucial role in our case.

We note in the Preliminaries that for any real $\varphi$ the states $|1\rangle$ and $e^{i\varphi}|1\rangle$ are experimentally indistinguishable. This implies that if we start by only distinguishing the classical states 0 and 1 then there are families of CPSOs which are indistinguishable as well. For example, let $\boldsymbol{H}$ be the well-known Hadamard gate, and let $\boldsymbol{H}_\varphi$ be the same gate expressed in the basis $(|0\rangle, e^{i\varphi}|1\rangle)$, for $\varphi \in [0, 2\pi)$. Any experiment that starts in state 0 or 1 and uses only $\boldsymbol{H}$ will produce outcomes 0 and 1 with the same probabilities as the same experiment with $\boldsymbol{H_\varphi}$. Thus no experiment that uses this quantum gate alone can distinguish it from all the other Hadamard gates. Indeed, as stated later in Fact 5, a family $\mathcal{F}$ containing $\boldsymbol{H}$ can only be tested if the entire Hadamard family $\mathcal{H} = \{\boldsymbol{H}_\varphi : \varphi \in [0, 2\pi)\}$ is included in $\mathcal{F}$.

The main result of this paper is **Theorem 7** which states that for several sets of unitary CPSOs, in particular, the Hadamard gates family, Hadamard gates together with c-NOT gates, and Hadamard gates with c-NOT and phase rotation gates of angle $\pm\pi/4$, 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[8].

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 1**, **2**, and **3** we will exhibit experimental equations for the families of unitary CPSOs we want to characterize. In **Theorem 4** 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 6** 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 **Theorem 5** for the equations characterizing the Hadamard family $\mathcal{H}$.

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.

# 2 Preliminaries

## 2.1 The quantum state

A *pure state* in a quantum physical system is described by a unit vector in a Hilbert space. In the *Dirac* notation it is denoted by $|\psi\rangle$. In particular a *qubit* (a quantum two-state system) is an element of the Hilbert space $\mathbb{C}^{\{0,1\}}$. The orthonormal basis containing $|0\rangle$ and $|1\rangle$ is called the *computational basis* of $\mathbb{C}^{\{0,1\}}$. Therefore a pure state $|\psi\rangle \in \mathbb{C}^{\{0,1\}}$ is a *superposition* of the computational basis states, that is, $|\psi\rangle = c_0|0\rangle + c_1|1\rangle$, with $|c_0|^2 + |c_1|^2 = 1$. A physical system which deals with $n$ qubits is described mathematically by the $2^n$-dimensional Hilbert space which is by definition $\mathbb{C}^{\{0,1\}} \otimes \cdots \otimes \mathbb{C}^{\{0,1\}}$, that is, the $n^{\text{th}}$ tensor power of $\mathbb{C}^{\{0,1\}}$. Let $N = 2^n$. The computational basis of this space consists of the $N$ orthonormal states $|i\rangle$ for $0 \leq i < N$. If $i$ is in binary notation $i_1 i_2 \ldots i_n$, then $|i_1 \ldots i_n\rangle = |i_1\rangle \ldots |i_n\rangle$, where this is a short notation for $|i_1\rangle \otimes \cdots \otimes |i_n\rangle$. All vectors and matrices will be expressed in the computational basis. The transposed complex conjugate $|\psi\rangle^\dagger$ of $|\psi\rangle$ is denoted by $\langle\psi|$. The inner product between $|\psi\rangle$ and $|\psi'\rangle$ is denoted by $\langle\psi|\psi'\rangle$, and their outer product by $|\psi\rangle\langle\psi'|$.

Quantum systems can also be in more general states than what can be described by pure states. The most general states are *mixed states*, described by a probability distribution over pure states. Such a mixture can be denoted by $\{(p_k, |\psi_k\rangle) : k \in \mathbb{N}\}$, where the system is in the pure state $|\psi_k\rangle$ with probability $p_k$.

Different mixtures (even different pure states $|\psi\rangle$) can represent the same physical system. This notational redundancy can be avoided if we use the formalism of the density matrices. A *density matrix* that represents an $n$-qubit state is an $N \times N$ Hermitian semi-positive matrix with trace 1. The pure state $|\psi\rangle$ in this representation is described by the density matrix $\psi = |\psi\rangle\langle\psi|$, and a mixture $\{(p_k, |\psi_k\rangle) : k \in \mathbb{N}\}$ by the density matrix $\psi = \sum_{k\in\mathbb{N}} p_k |\psi_k\rangle\langle\psi_k|$. For example, the pure states $e^{i\gamma}|\psi\rangle$, for $\gamma \in [0, 2\pi)$, or the mixtures $\{(\frac{1}{2}, |0\rangle), (\frac{1}{2}, |1\rangle)\}$ and $\{(\frac{1}{2}, \frac{|0\rangle+|1\rangle}{\sqrt{2}}), (\frac{1}{2}, \frac{|0\rangle-|1\rangle}{\sqrt{2}})\}$ have respectively the same density matrix.

Since a density matrix is Hermitian semi-positive, its eigenvectors are orthogonal and its eigenvalues are non-negative. Because the density matrix has trace 1, its eigenvalues sum to 1. Therefore a density matrix represents the mixture of its orthonormal eigenvectors, where the probabilities are the respective eigenvalues. Note that diagonal density matrices correspond to a mixture over pure states $|i\rangle$, for $0 \leq i < N$. Density matrices that represent pure states have a simple algebraic characterization: $\rho$ is a pure state if and only if it has two eigenvalues, 0 with multiplicity $N-1$ and 1 with multiplicity 1, equivalently $\rho$ is a pure state exactly when $\rho^2 = \rho$.

A $2 \times 2$ Hermitian matrix of unit trace is semi-positive if and only if its determinant is between 0 and 1/4. Therefore in the case of one qubit, any density matrix $\rho$ can be written as $\rho = p|0\rangle\langle 0| + (1-p)|1\rangle\langle 1| + \alpha|1\rangle\langle 0| + \alpha^*|0\rangle\langle 1|$, where $p \in [0,1]$, and $\alpha$ is a complex number such that $|\alpha|^2 \leq p(1-p)$. This density matrix will be denoted by $\rho(p,\alpha)$. Remark that $\rho(p,\alpha)$ is a pure state exactly when $|\alpha|^2 = p(1-p)$, that is, its determinant is 0.

## 2.2 Superoperators

The evolution of physical systems is described by specific transformations on density matrices, that is, on operators. A *superoperator* for $n$ qubits is a linear transformation on $\mathbb{C}^{N\times N}$. A *positive* superoperator (PSO) is a superoperator that sends density matrices to density matrices. A *completely positive* superoperator (CPSO) $\boldsymbol{G}$ is a PSO such that for all positive integers $M$, $\boldsymbol{G} \otimes \boldsymbol{I}_M$ is also a PSO, where $\boldsymbol{I}_M$ is the identity on $\mathbb{C}^{M\times M}$. CPSOs are exactly the physically allowed transformations on density matrices. An example of a PSO for one qubit that is not a CPSO is the transpose superoperator $\boldsymbol{T}$ defined by $\boldsymbol{T}(|i\rangle\langle j|) = |j\rangle\langle i|$, for $0 \leq i,j \leq 1$.

Quantum computation is based on the possibility of constructing some particular CPSOs, *unitary* superoperators, which preserve the set of pure states. These operators are characterized by transformations from $\mathrm{U}(N)$, the set of $N \times N$ unitary matrices. For any $A \in \mathrm{U}(N)$, we define a CPSO which maps a density matrix $\rho$ into $A\rho A^\dagger$. When the underlying unitary transformation $A$ is clear from the context, by somewhat abusing the notation, we will denote this CPSO simply by $\boldsymbol{A}$. If $|\psi'\rangle$ denotes $A|\psi\rangle$, then the unitary superoperator $\boldsymbol{A}$ maps the pure state $\psi$ to the pure state $\psi'$. As was the case in the Dirac representation of states, there is the same phase redundancy in the set of unitary transformations $\mathrm{U}(N)$. If $A \in \mathrm{U}(N)$, then for all $\gamma \in [0, 2\pi)$, the transformations $e^{i\gamma}A$ are different, however the corresponding superoperators are identical. We will therefore focus on $\mathrm{U}(N)/\mathrm{U}(1)$.

## 2.3 Measurements

Measurements form another important class of (non-unitary) CPSOs. They describe physical transformations corresponding to the observation of the system. We will define now formally one of the simplest classes of measurements which correspond to the projections to elements of the computational basis.

A *Von Neumann measurement in the computational basis* of $n$ qubits is the $n$-qubit CPSO $\boldsymbol{M}$ that, for every density matrix $\rho$, satisfies $\boldsymbol{M}(\rho)_{i,i} = \rho_{i,i}$ and $\boldsymbol{M}(\rho)_{i,j} = 0$, for $i \neq j$.

In the case of one qubit, the Von Neumann measurement in the computational basis maps the density matrix $\rho(p,\alpha)$ into $\rho(p,0)$. We will say that $p = \langle 0|\rho|0\rangle$ is the *probability of measuring* $|0\rangle\langle 0|$, and we will denote it by $\Pr^0[\rho]$.

In general, a *Von Neumann measurement* of $n$ qubits in any basis can be viewed as the Von Neumann measurement in the computational basis preceded by some unitary superoperator.

## 2.4 The Bloch Ball representation

Specific for the one-qubit case, there is an isomorphism between the group $\mathrm{U}(2)/\mathrm{U}(1)$ and the special rotation group $\mathrm{SO}(3)$, the set of $3\times 3$ orthogonal matrices with determinant 1. This allows us to represent 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* $\mathcal{B}$ (respectively *Bloch Sphere* $\mathcal{S}$) is the unit ball (respectively unit sphere) of the Euclidean affine space $\mathbb{R}^3$. Any point $\overline{u} \in \mathbb{R}^3$ determines a vector with the same coordinates which we will also denote by $\overline{u}$. The inner product of $\overline{u}$ and $\overline{v}$ will be denoted by $(\overline{u}, \overline{v})$, and their Euclidean norm by $\|\overline{u}\|$.

Each point $\overline{u} \in \mathbb{R}^3$ can be also characterized by its norm $r \geq 0$, its latitude $\theta \in [0,\pi]$, and its longitude $\varphi \in [0, 2\pi)$. The *latitude* is the angle between the $z$-axis and the vector $\overline{u}$, and the *longitude* is the angle between the $x$-axis and the orthogonal projection of $\overline{u}$ in the plane defined by $z = 0$. If $\overline{u} = (x,y,z)$, then these parameters satisfy $x = r\sin\theta\cos\varphi$, $y = r\sin\theta\sin\varphi$ and $z = r\cos\theta$.

For every density matrix $\rho$ for one qubit there exists a unique point $\overline{\rho} = (x,y,z) \in \mathcal{B}$ such that

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

This mapping is a bijection that also obeys

$$\overline{\rho(p,\alpha)} \quad = \quad (2\mathrm{Re}(\alpha), 2\mathrm{Im}(\alpha), 2p-1).$$

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

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

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

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

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

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

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

### 2.5 Norm and distance

Let $N = 2^n$. We will consider the *trace norm* on $\mathbb{C}^{N\times N}$ which is defined as follows: for all $V \in \mathbb{C}^{N\times N}$, $\|V\|_1 = \mathrm{Tr}\sqrt{V^\dagger V}$. This norm has several advantages when we consider the difference of density matrices. Given a Von Neumann measurement, a density matrix induces a probability distribution over the basis of the measurement. The trace norm of the difference of two density matrices is the maximal variation distance between the two induced probability distributions, over all Von Neumann measurements. It also satisfies the following properties.

**Fact 3** *For all density matrices $\rho(p,\alpha)$ and $\rho(q,\beta)$ for one qubit we have:*

$$\|\rho(p,\alpha) - \rho(q,\beta)\|_1 \quad = \quad \|\overline{\rho(p,\alpha)} - \overline{\rho(q,\beta)}\| \quad = \quad 2\sqrt{(p-q)^2 + |\alpha-\beta|^2}.$$

**Fact 4** *For all $V \in \mathbb{C}^{N\times N}$ and $W \in \mathbb{C}^{M\times M}$ we have $\|V \otimes W\|_1 = \|V\|_1\|W\|_1$ and $|\mathrm{Tr}(V)| \leq \|V\|_1$. For density matrices $\rho$ it holds that $\|\rho\|_1 = 1$.*

For $n$-qubit superoperators, the superoperator norm associated to the trace norm is defined as

$$\|\boldsymbol{G}\|_\infty \quad = \quad \sup\{\|\boldsymbol{G}(V)\|_1 : \|V\|_1 = 1\}.$$

This norm is always 1 when $\boldsymbol{G}$ is a CPSO. The norm $\|\ \|_\infty$ can be easily generalized for $k$-tuples of superoperators by $\|(\boldsymbol{G}_1,\ldots,\boldsymbol{G}_k)\|_\infty = \max(\|\boldsymbol{G}_1\|_\infty,\ldots,\|\boldsymbol{G}_k\|_\infty)$. We will denote by $\mathrm{dist}_\infty$ the natural induced distance by the norm $\|\ \|_\infty$.

## 3 Properties of CPSOs

Here we will establish the properties of CPSOs that we will need for the characterization of our CPSO families. In this extended abstract we will omit the proof of Lemma 1, and the proof of Lemma 2 will be in Appendix A.

**Lemma 1** *Let $\boldsymbol{G}$ be a CPSO for one qubit, and let $\rho$ and $\tau$ be density matrices for one qubit.*

*(a)* $\|\boldsymbol{G}(\rho) - \boldsymbol{G}(\tau)\|_1 \leq \|\rho - \tau\|_1$.

*(b) If $\boldsymbol{G}$ is not constant and $\boldsymbol{G}(\rho)$ is a pure state then $\rho$ is a pure state.*

An affine transformation of $\mathbb{R}^3$ is uniquely defined by the images of four non-coplanar points. Surprisingly, if the transformation is a CPSO for one qubit, the images of three points are sometimes sufficient. The following will make this precise more generally for $n$ qubits.

**Lemma 2** *Let $n \geq 1$ be an integer, and let $\rho_1$, $\rho_2$, and $\rho_3$ be three distinct one-qubit density matrices representing pure states, such that the plane in $\mathbb{R}^3$ containing the points $\overline{\rho_1}, \overline{\rho_2}, \overline{\rho_3}$ goes through the center of $\mathcal{B}$. If $\boldsymbol{G}$ is a CPSO for $n$ qubits which acts as the identity on the set $\{\rho_1, \rho_2, \rho_3\}^{\otimes n}$, then $\boldsymbol{G}$ is the identity mapping.*

We also use the property that for CPSOs unitarity and invertibility are equivalent (see e.g. [27, Ch. 3, Sec. 8]).

**Lemma 3** *Let $\boldsymbol{G}$ be a CPSO for $n$ qubits. If there exists a CPSO $\boldsymbol{H}$ for $n$ qubits such that $\boldsymbol{H} \circ \boldsymbol{G}$ is the identity mapping, then $\boldsymbol{G}$ is a unitary superoperator.*

# 4 Characterization

## 4.1 One-Qubit 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.

An *experimental equation* in one variable is a CPSO equation of the form

$$\Pr^0[\boldsymbol{G}^k(|b\rangle\langle b|)] \quad = \quad r, \tag{1}$$

where $k$ is a non-negative 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 $\boldsymbol{G}$ 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 $\boldsymbol{G}$ $\varepsilon$*-satisfies* (1) if $|\Pr^0[\boldsymbol{G}^k(|b\rangle\langle b|)] - r| \leq \varepsilon$, and when $\varepsilon = 0$ we will just say that $\boldsymbol{G}$ *satisfies* (1). Let $(E)$ be a finite set of experimental equations. If $\boldsymbol{G}$ $\varepsilon$-satisfies all equations in $(E)$ we say that $\boldsymbol{G}$ $\varepsilon$-satisfies $(E)$. If some $\boldsymbol{G}$ satisfies $(E)$ then $(E)$ is *satisfiable*. The set $\{\boldsymbol{G} : \boldsymbol{G} \text{ satisfies } (E)\}$ will be denoted by $\mathcal{F}_{(E)}$. A family $\mathcal{F}$ of CPSOs is *characterizable* if it is $\mathcal{F}_{(E)}$ for some finite set $(E)$ of experimental equations. In this case we say that $(E)$ *characterizes* $\mathcal{F}$.

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

$$\Pr^0[\boldsymbol{F}^{k_1} \circ \boldsymbol{G}^{l_1} \circ \cdots \circ \boldsymbol{F}^{k_t} \circ \boldsymbol{G}^{l_t}(|b\rangle\langle b|)] \quad = \quad r,$$

where $k_1, \ldots, k_t, l_1, \ldots, l_t$ are non-negative 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 $\boldsymbol{R}_{\alpha,\theta,\varphi}$, for $\alpha \in (-\pi, \pi]$, $\theta \in [0, \pi/2]$, and $\varphi \in [0, 2\pi)$. First observe that due to the restrictions of experimental equations, there are unitary superoperators that they cannot distinguish.

**Fact 5** *Let $\alpha \in [0, \pi]$, $\theta \in [0, \pi/2]$, and $\varphi_1, \varphi_2 \in [0, 2\pi)$ such that $\varphi_1 \neq \varphi_2$. Let $(E)$ be a finite set of experimental equations in $m$ variables. If $(\boldsymbol{R}_{\alpha,\theta,\varphi_1}, \boldsymbol{G}_2, \ldots, \boldsymbol{G}_m)$ satisfies $(E)$ then there exist $\boldsymbol{G}'_2, \ldots, \boldsymbol{G}'_m$ and $\boldsymbol{G}''_2, \ldots, \boldsymbol{G}''_m$ such that $(\boldsymbol{R}_{-\alpha,\theta,\varphi_1}, \boldsymbol{G}'_2, \ldots, \boldsymbol{G}'_m)$ and $(\boldsymbol{R}_{\alpha,\theta,\varphi_2}, \boldsymbol{G}''_2, \ldots, \boldsymbol{G}''_m)$ 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 $|0\rangle\langle 0|$ 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 $\varphi$ 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 $\mathcal{R}_{\alpha,\theta}$ denote the superoperator family $\{\boldsymbol{R}_{\pm\alpha,\theta,\varphi} : \varphi \in [0, 2\pi)\}$. For $\varphi \in [0, 2\pi)$, let the $\mathrm{NOT}_\varphi$ transformation be defined by $\mathrm{NOT}_\varphi|0\rangle = e^{i\varphi}|1\rangle$ and $\mathrm{NOT}_\varphi(e^{i\varphi}|1\rangle) = |0\rangle$, and recall that the Hadamard transformation $H_\varphi$ obeys $H_\varphi|0\rangle = (|0\rangle + e^{i\varphi}|1\rangle)/\sqrt{2}$ and $H_\varphi(e^{i\varphi}|1\rangle) = (|0\rangle - e^{i\varphi}|1\rangle)/\sqrt{2}$. Observe that $\boldsymbol{H}_\varphi = \boldsymbol{R}_{\pi,\pi/4,\varphi}$ and $\mathbf{NOT}_\varphi = \boldsymbol{R}_{\pi,\pi/2,\varphi}$, for $\varphi \in [0, 2\pi)$. Finally let $\mathcal{H} = \{\boldsymbol{H}_\varphi : \varphi \in [0, 2\pi)\}$, and $\mathcal{N} = \{\mathbf{NOT}_\varphi : \varphi \in [0, 2\pi)\}$.

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 $\alpha/\pi$ is rational. This is a reasonable choice 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 $\alpha = (t/n_\alpha)2\pi$. Observe that the case $n_\alpha = 1$ corresponds to the identity superoperator.

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

**Theorem 1** *Let $(\alpha, \theta) \in (0, \pi] \times (0, \pi/2] \backslash \{(\pi, \pi/2)\}$ be such that $\alpha/\pi$ is rational. Let $z_k(\alpha, \theta) = \cos^2\theta + \sin^2\theta \cos(k\alpha)$. Then the following experimental equations characterize $\mathcal{R}_{\alpha,\theta}$:*

$$\Pr{}^0[\boldsymbol{G}^{n_\alpha}(|1\rangle\langle 1|)] = 0 \quad \textit{and} \quad \Pr{}^0[\boldsymbol{G}^k(|0\rangle\langle 0|)] = \tfrac{1}{2} + \tfrac{1}{2}z_k(\alpha, \theta), \quad k \in \{1, 2, \ldots, n_\alpha\}.$$

**Proof:** First observe that every CPSO in $\mathcal{R}_{\alpha,\theta}$ satisfies the equations of the theorem since the $z$-coordinate of $\overline{\boldsymbol{R}^k_{\alpha,\theta,\varphi}(|0\rangle\langle 0|)}$ is $z_k(\alpha, \theta)$ for every $\varphi \in [0, 2\pi)$. Let $\boldsymbol{G}$ be a CPSO which satisfies these equations. We will prove that $\boldsymbol{G}$ is a unitary superoperator. Then, Fact 6 implies that $\boldsymbol{G} \in \mathcal{R}_{\alpha,\theta}$.

Since $z_1(\alpha, \theta) \neq \pm 1$, we know $\boldsymbol{G}(|0\rangle\langle 0|) \notin \{|0\rangle\langle 0|, |1\rangle\langle 1|\}$. Observing that $\boldsymbol{G}^{n_\alpha}(|0\rangle\langle 0|) = |0\rangle\langle 0|$, Lemma 1(b) implies that $\boldsymbol{G}(|0\rangle\langle 0|)$ is a pure state. Thus $|0\rangle\langle 0|$, $|1\rangle\langle 1|$, and $\boldsymbol{G}(|0\rangle\langle 0|)$ are distinct pure states, and since $\boldsymbol{G}^{n_\alpha}$ acts as the identity on them, by Lemma 2 it is the identity mapping. Hence by Lemma 3 $\boldsymbol{G}$ is a unitary superoperator. ■

**Fact 6** *Let $\alpha \in (0, \pi]$, $\theta \in (0, \pi/2]$, $\alpha' \in (-\pi, \pi]$, $\theta' \in (0, \pi/2]$ be such that $\alpha/\pi$ is rational. If $z_k(\alpha, \theta) = z_k(\alpha', \theta')$, for $k \in \{1, 2, \ldots, n_\alpha\}$, then $|\alpha'| = \alpha$ and $\theta' = \theta$.*

The remaining families $\mathcal{R}_{\alpha,\theta}$ for which $\alpha/\pi$ is rational are $\{\boldsymbol{R}_{-\alpha}, \boldsymbol{R}_\alpha\}$, for $\alpha \in [0, \pi]$, and $\mathcal{N}$. Let us recall that $\boldsymbol{M}$ is the CPSO which represents the Von Neumann measurement in the computational basis. Since $\boldsymbol{M}$ satisfies exactly the same equations as $\boldsymbol{R}_{\pm\alpha}$, and $\mathbf{NOT}_0 \circ \boldsymbol{M}$ satisfies exactly the same equations as $\mathbf{NOT}_\varphi$, for any $\varphi \in [0, 2\pi)$, these families are not characterizable by experimental equations in one variable. Nevertheless it turns out that together with the family $\mathcal{H}$ they become characterizable. This is stated in the following theorem whose proof is omitted.

**Theorem 2** *The family $\{(\boldsymbol{H}_\varphi, \mathbf{NOT}_\varphi) : \varphi \in [0, 2\pi)\} \subset \mathcal{H} \times \mathcal{N}$ is characterized by the experimental equations in two variables $(\boldsymbol{F}, \boldsymbol{G})$:*

$$\begin{cases} \Pr^0[\boldsymbol{F}(|0\rangle\langle 0|)] = \frac{1}{2}, & \Pr^0[\boldsymbol{F}^2(|0\rangle\langle 0|)] = 1, \quad \Pr^0[\boldsymbol{F}^2(|1\rangle\langle 1|)] = 0, \\ \Pr^0[\boldsymbol{G}(|0\rangle\langle 0|)] = 0, & \Pr^0[\boldsymbol{G}(|1\rangle\langle 1|)] = 1, \\ \Pr^0[\boldsymbol{F} \circ \boldsymbol{G}^2 \circ \boldsymbol{F}(|0\rangle\langle 0|)] = 1, & \Pr^0[\boldsymbol{F} \circ \boldsymbol{G} \circ \boldsymbol{F}(|0\rangle\langle 0|)] = 1. \end{cases}$$

*If $\alpha/\pi$ is rational, then the family $\mathcal{H} \times \{\boldsymbol{R}_{\pm\alpha}\}$ is characterized by the experimental equations in two variables $(\boldsymbol{F}, \boldsymbol{G})$:*

$$\begin{cases} \Pr^0[\boldsymbol{F}(|0\rangle\langle 0|)] = \frac{1}{2}, & \Pr^0[\boldsymbol{F}^2(|0\rangle\langle 0|)] = 1, \quad \Pr^0[\boldsymbol{F}^2(|1\rangle\langle 1|)] = 0, \\ \Pr^0[\boldsymbol{G}(|0\rangle\langle 0|)] = 1, & \Pr^0[\boldsymbol{G}(|1\rangle\langle 1|)] = 0, \\ \Pr^0[\boldsymbol{F} \circ \boldsymbol{G}^{n_\alpha} \circ \boldsymbol{F}(|0\rangle\langle 0|)] = 1, & \Pr^0[\boldsymbol{F} \circ \boldsymbol{G} \circ \boldsymbol{F}(|0\rangle\langle 0|)] = \frac{1}{2} + \frac{1}{2}\cos\alpha. \end{cases}$$

### 4.2 Characterization of c-NOT 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 **c-NOT** gates together with the family $\mathcal{H}$ is characterizable. First we need some definitions.

For every $\varphi \in [0, 2\pi)$, we define c-NOT$_\varphi$ as the only unitary transformation over $\mathbb{C}^4$ satisfying c-NOT$_\varphi(|0\rangle|\psi\rangle) = |0\rangle|\psi\rangle$ and c-NOT$_\varphi|1\rangle|\psi\rangle = |1\rangle$NOT$_\varphi|\psi\rangle$, for all $|\psi\rangle \in \mathbb{C}^2$.

We extend the definition of the experimental equation for CPSOs given in (2) for $n$ qubits. It is an equation of the form

$$\Pr^v[\boldsymbol{F}^{k_1} \circ \boldsymbol{G}^{l_1} \circ \cdots \circ \boldsymbol{F}^{k_t} \circ \boldsymbol{G}^{l_t}(|w\rangle\langle w|)] \quad = \quad r, \tag{2}$$

where in addition to the notation of (2) $v, w \in \{0,1\}^n$, and $\Pr^v$ is the probability of measuring $|v\rangle\langle v|$. For the variables $\boldsymbol{F}$ and $\boldsymbol{G}$ of (2), 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 3** *The family* $\{(\boldsymbol{H}_\varphi, \textbf{c-NOT}_\varphi) : \varphi \in [0, 2\pi)\}$ *is characterized by the experimental equations in two variables* $(\boldsymbol{F}, \boldsymbol{G})$*:*

$$\begin{cases}
\Pr^0[\boldsymbol{F}(|0\rangle\langle 0|)] = \frac{1}{2}, \quad \Pr^0[\boldsymbol{F}^2(|0\rangle\langle 0|)] = 1, \quad \Pr^0[\boldsymbol{F}^2(|1\rangle\langle 1|)] = 0, \\
\Pr^{00}[\boldsymbol{G}(|00\rangle\langle 00|)] = 1, \; \Pr^{01}[\boldsymbol{G}(|01\rangle\langle 01|)] = 1, \; \Pr^{11}[\boldsymbol{G}(|10\rangle\langle 10|)] = 1, \; \Pr^{10}[\boldsymbol{G}(|11\rangle\langle 11|)] = 1, \\
\Pr^{00}[(\boldsymbol{I}_2 \otimes \boldsymbol{F}) \circ \boldsymbol{G} \circ (\boldsymbol{I}_2 \otimes \boldsymbol{F})(|00\rangle\langle 00|)] = 1, \quad \Pr^{10}[(\boldsymbol{I}_2 \otimes \boldsymbol{F}) \circ \boldsymbol{G} \circ (\boldsymbol{I}_2 \otimes \boldsymbol{F})(|10\rangle\langle 10|)] = 1, \\
\Pr^{00}[(\boldsymbol{F} \otimes \boldsymbol{I}_2) \circ \boldsymbol{G}^2 \circ (\boldsymbol{F} \otimes \boldsymbol{I}_2)(|00\rangle\langle 00|)] = 1, \quad \Pr^{01}[(\boldsymbol{F} \otimes \boldsymbol{I}_2) \circ \boldsymbol{G}^2 \circ (\boldsymbol{F} \otimes \boldsymbol{I}_2)(|01\rangle\langle 01|)] = 1, \\
\Pr^{00}[(\boldsymbol{F} \otimes \boldsymbol{F}) \circ \boldsymbol{G} \circ (\boldsymbol{F} \otimes \boldsymbol{F})(|00\rangle\langle 00|)] = 1.
\end{cases}$$

**Proof:** Let $\boldsymbol{F}$ and $\boldsymbol{G}$ satisfy these equations. By Theorem 1, with $\alpha = \pi$ and $\theta = \pi/4$, the first three equations imply that $\boldsymbol{F} = \boldsymbol{H}_\varphi$, for some $\varphi \in [0, 2\pi)$. Using Lemma 2, the remaining equations imply that $\boldsymbol{G}^2 = \boldsymbol{I}_4$, and it follows from Lemma 3 that $\boldsymbol{G}$ is a unitary CPSO. A straightforward verification then shows that indeed $\boldsymbol{G} = \textbf{c-NOT}_{\boldsymbol{\varphi}}$. ∎

## 5 Robustness

In this section we introduce the notion of robustness for experimental equations which will be the crucial ingredient for proving self-testability. In this extended abstract we will deal only with the case of experimental equations for one qubit and in one variable. From now on $(E)$ will always denote a set of such equations. Similar results can be obtained for several qubits and several variables.

**Definition 1** *Let* $\varepsilon, \delta \geq 0$*, and let* $(E)$ *be a finite satisfiable set of experimental equations. We say that* $(E)$ *is* $(\varepsilon, \delta)$-robust *if whenever a CPSO* $\boldsymbol{G}$ $\varepsilon$*-satisfies* $(E)$*, we have* $\mathrm{dist}_\infty(\boldsymbol{G}, \mathcal{F}_{(E)}) \leq \delta$*.*

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 always the case.

**Theorem 4** *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 [11]. In the proof, $\mathbb{C}$ is identified with $\mathbb{R}^2$. Then the set $K$ of CPSOs for one qubit is a real compact semi-algebraic set. Suppose that in $(E)$ there are $d$ equations. Let $f : K \to \mathbb{R}$ be the function that maps the CPSO $\boldsymbol{G}$ to the maximum of the magnitudes of the difference between the probability term and the constant term of the $i^{\text{th}}$ 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 $\boldsymbol{G}$.

Let $g : K \to \mathbb{R}$ defined in $\boldsymbol{G}$ by $g(\boldsymbol{G}) = \mathrm{dist}_\infty(\boldsymbol{G}, \mathcal{F}_{(E)})$. Since $K$ is a compact semi-algebraic set, $g$ is a continuous semi-algebraic function. Moreover, for all $\boldsymbol{G} \in K$, we have $f(\boldsymbol{G}) = 0$ if and only if $g(\boldsymbol{G}) = 0$. Then Fact 7 concludes the proof. ∎

For a proof of the following fact, see for example [11, Prop. 2.3.11].

**Fact 7 (Lojasiewicz's inequality)** *Let $X \subseteq \mathbb{R}^m$ be a compact semi-algebraic set. Let $f, g : X \to \mathbb{R}$ be 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 4. We will illustrate these techniques with the equations in Theorem 1 for the case $\alpha = \pi$ and $\theta = \pi/4$. Let us recall that these equations characterize the set $\mathcal{H}$.

**Theorem 5** *For every $0 \leq \varepsilon \leq 1$, the following equations are $(\varepsilon, 4579\sqrt{\varepsilon})$-robust:*

$$\Pr^0[\boldsymbol{G}(|0\rangle\langle 0|)] = \tfrac{1}{2}, \quad \Pr^0[\boldsymbol{G}^2(|0\rangle\langle 0|)] = 1, \ \textit{and} \quad \Pr^0[\boldsymbol{G}^2(|1\rangle\langle 1|)] = 0.$$

The proof of this theorem will be given in Appendix B.

# 6 Quantum Self-Testers

In this final section we define formally our testers and establish the relationship between robust equations and testability. Again, we will do it here only for the case of one qubit and one variable. Let $\boldsymbol{G}$ be a CPSO. The *experimental oracle* $\mathcal{O}[\boldsymbol{G}]$ for $\boldsymbol{G}$ is a probabilistic procedure. It takes inputs from $\{0,1\} \times \mathbb{N}$ and generates outcomes from the set $\{0,1\}$ such that for every $k \in \mathbb{N}$,

$$\Pr[\mathcal{O}[\boldsymbol{G}](b,k) = 0] \quad = \quad \Pr^0[\boldsymbol{G}^k(|b\rangle\langle b|)].$$

An oracle program $T$ with an experimental oracle $\mathcal{O}[\boldsymbol{G}]$ is a program denoted by $T^{\mathcal{O}[\boldsymbol{G}]}$ which can ask queries from the experimental oracle in the following sense: when it presents a query $(b,k)$ to the oracle, in one computational step it receives the probabilistic outcome of $\mathcal{O}[\boldsymbol{G}]$ on it.

**Definition 2** *Let $\mathcal{F}$ be a family of CPSOs, and let $0 \leq \delta_1 \leq \delta_2 < 1$. A $(\delta_1, \delta_2)$-*tester for $\mathcal{F}$ *is a probabilistic oracle program $T$ such that for every CPSO $\boldsymbol{G}$,*

- *if* $\mathrm{dist}_\infty(\boldsymbol{G}, \mathcal{F}) \leq \delta_1$ *then* $\Pr[T^{\mathcal{O}[\boldsymbol{G}]}$ *says* `PASS`$] \geq 2/3$,
- *if* $\mathrm{dist}_\infty(\boldsymbol{G}, \mathcal{F}) > \delta_2$ *then* $\Pr[T^{\mathcal{O}[\boldsymbol{G}]}$ *says* `FAIL`$] \geq 2/3$,

*where the probability is taken over the probability distribution of the outcomes of the experimental oracle and the internal coin tosses of the program.*

**Theorem 6** *Let $\varepsilon, \delta > 0$, 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 $(\varepsilon, \delta)$-robust then there exists an $(\varepsilon/(3k), \delta)$-tester for $\mathcal{F}_{(E)}$ which makes $O(d\ln(d)/\varepsilon^2)$ queries.*

Sketch of proof. We will describe a probabilistic oracle program $T$. Let $\boldsymbol{G}$ be a CPSO. We can suppose that for every equation in $(E)$, $T$ has a rational number $\tilde{r}$ such that $|\tilde{r} - r| \leq \varepsilon/6$, where $r$ is the constant term of the equation. By sampling the oracle $\mathcal{O}[\boldsymbol{G}]$, for every equation in $(E)$, $T$ obtains a value $\tilde{p}$ such that $|\tilde{p} - p| \leq \varepsilon/6$ with probability at least $1 - 1/(3d)$, where $p$ is the probability term of the equation. A standard Chernoff bound argument shows that this is feasible with $O(\ln(d)/\varepsilon^2)$ queries for each equation. If for every equation $|\tilde{p} - \tilde{r}| \leq 2\varepsilon/3$, then $T$ says `PASS`, otherwise $T$ says `FAIL`. Using the robustness of $(E)$ and Lemma 4, one can verify that $T$ is a $(\varepsilon/(3k), \delta)$-tester for $\mathcal{F}_{(E)}$. ■

**Lemma 4** *Let $(E)$ be a finite satisfiable set of experimental equations such that the size of every equation is at most $k$, and let $\boldsymbol{G}$ be a CPSO. For every $\varepsilon \geq 0$, if $\mathrm{dist}_\infty(\boldsymbol{G}, \mathcal{F}_{(E)}) \leq \varepsilon$ then $\boldsymbol{G}$ $(k\varepsilon)$-satisfies $(E)$.*

Our main result is the consequence of Theorems 1, 2, 3, 4, 5, 6, and the many-qubit generalizations of them.

**Theorem 7** *Let $\mathcal{F}$ be one of the following families :*

- $\mathcal{R}_{\alpha,\theta}$ *for $(\alpha, \theta) \in (0, \pi] \times (0, \pi/2] \backslash \{(\pi, \pi/2)\}$ where $\alpha/\pi$ is rational,*

- $\{(\boldsymbol{H}_\varphi, \mathbf{NOT}_\varphi) : \varphi \in [0, 2\pi)\}$,
- $\mathcal{H} \times \{\boldsymbol{R}_{\pm\alpha}\}$ *for* $\alpha/\pi$ *rational,*
- $\{(\boldsymbol{H}_\varphi, \mathbf{c\text{-}NOT}_\varphi) : \varphi \in [0, 2\pi)\}$,
- $\{(\boldsymbol{H}_\varphi, \boldsymbol{R}_{s\pi/4}, \mathbf{c\text{-}NOT}_\varphi) : \varphi \in [0, 2\pi), s = \pm 1\}$.

*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 which makes* $O(1/\varepsilon^2)$ *queries. Moreover, for every* $0 < \varepsilon \leq 1$, $\mathcal{H}$ *has an* $(\varepsilon/6, 4579\sqrt{\varepsilon})$*-tester which makes* $O(1/\varepsilon^2)$ *queries.*

Note that each triplet of the last family forms a universal and fault-tolerant set of quantum gates[8].

## 7 Acknowledgements

We would like to thank Jean-Benoit Bost, Stéphane Boucheron, Charles Delorme, Stéphane Gonnord, Lucien Hardy, Richard Jozsa, and Vlatko Vedral for several useful discussions and advice.

This work has been supported by C.E.S.G., Wolfson College Oxford, Hewlett-Packard, European TMR Research Network ERP-4061PL95-1412, the Institute for Logic, Language and Computation in Amsterdam, ESPRIT Working Group RAND2 no. 21726, NSERC, British-French Bilateral Project ALLIANCE no. 98101, and the Quantum Information Theory programme of the European Science Foundation.

## References

[1] L. Adleman, J. Demarrais, and M. Huang. Quantum computability. *SIAM J. on Comput.*, 26:5, pp. 1524–1540, 1997.

[2] D. Aharonov and M. Ben-Or. Fault-tolerant quantum computation with constant error. In *Proc. 29th STOC*, pp. 46–55, 1997.

[3] D. Aharonov, A. Kitaev, and N. Nisan. Quantum circuits with mixed states. In *Proc. 30th STOC*, pp. 20–30, 1998.

[4] A. Barenco. A universal two-bit gate for quantum computation. In *Proc. Roy. Soc. London*, Ser. A, 449, pp. 679–683, 1995.

[5] C.H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proc. IEEE International Conference on Computers, Systems, and Signal Processing*, pp. 175–179, 1984.

[6] A. Barenco, C.H. Bennett, R. Cleve, D. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter. Elementary gates for quantum computation. *Phys. Rev.*, Ser. A, 52, pp. 3457–3467, 1995.

[7] A. Berthiaume and G. Brassard. The quantum challenge to structural complexity theory. In *Proc. 7th Structure in Complexity Theory*, pp. 132–137, 1992.

[8] P. Boykin, T. Mor, M. Pulver, V. Roychowdhury, and F. Vatan. On universal and fault-tolerant quantum computing: A novel basis and a new constructive proof of universality for Shor's basis. In *Proc. 40th FOCS*, pp. 486–494, 1999.

[9] E. Bernstein and U. Vazirani. Quantum complexity theory. *SIAM J. on Comput.*, 26:5, pp. 1411–1473, 1997.

[10] M. Blum, M. Luby, and R. Rubinfeld. Self-testing/correcting with applications to numerical problems. *J. of Comp. and Syst. Sci.*, pp. 549–595, 1990.

[11] R. Benedetti and J.-J. Risler. *Real algebraic and semi-algebraic sets*, Hermann, 1990.

[12] I.L. Chuang and M.A. Nielsen. Prescription for experimental determination of the dynamics of a quantum black box. *J. Modern Optics*, 44, pp. 732–744, 1997.

[13] D. Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. In *Proc. Roy. Soc. London*, Ser. A, 400, pp. 97–117, 1985.

[14] D. Deutsch. Quantum computational networks. In *Proc. Roy. Soc. London*, Ser. A, 425, pp. 73–90, 1989.

[15] D. Deutsch, A. Barenco, and A. Ekert. Universality in quantum computation. In *Proc. Roy. Soc. London*, Ser. A, 449, pp. 669–677, 1995.

[16] D. Deutsch and R. Jozsa. Rapid solution of problems by quantum computation. In *Proc. Roy. Soc. London*, Ser. A, 439, pp. 553–558, 1992.

[17] D. DiVincenzo. Two-bit gates are universal for quantum computation. *Phys. Rev.*, Ser. A, 51, pp. 1015–1022, 1995.

[18] R. Feynman. Simulating physics with computers. *Internat. J. Theoret. Phys.*, 21, pp. 467–488, 1982.

[19] P. Gemmell, R. Lipton, R. Rubinfeld, M. Sudan, and A. Wigderson. Self-testing/correcting for polynomials and for approximate functions. In *Proc. 23rd STOC*, pp. 32–42, 1991.

[20] A. Kitaev. Quantum computations: Algorithms and error correction. *Russian Math. Surveys*, 52, pp. 1191–1249, 1997.

[21] E. Knill, R. Laflamme, and W.H. Zurek. Threshold accuracy for quantum computation. `http://xxx.lanl.gov/abs/quant-ph/9610011`.

[22] E. Knill, R. Laflamme, and W.H. Zurek. Resilient quantum computation: error models and thresholds. In *Proc. Roy. Soc. London*, Ser. A, 454, pp. 365–384, 1998.

[23] R. Lipton. *New directions in testing*, Vol. 2 of *Series in Discrete Mathematics and Theoretical Computer Science*, pp. 191–202. ACM/AMS, 1991.

[24] S. Lloyd. Almost any quantum logic gate is universal. *Phys. Rev. Let.*, 75, pp. 346–349, 1995.

[25] D. Mayers and A. Yao. Quantum cryptography with imperfect apparatus. In *Proc. 39th FOCS*, pp. 503–509, 1998.

[26] J.F. Poyatos, J.I. Cirac, and P. Zoller. Complete characterization of a quantum process: the two-bit quantum gate. *Phys. Rev. Let.*, 78, pp. 390-393, 1997.

[27] J. Preskill. *Quantum Computing*. Lecture notes, `http://www.theory.caltech.edu/people/preskill/ph229/`.

[28] R. Rubinfeld. *A mathematical theory of self-checking, self-testing and self-correcting programs.* PhD thesis, University of California, Berkeley, 1990.

[29] R. Rubinfeld and M. Sudan. Robust characterizations of polynomials with applications to program testing. *SIAM J. on Computing*, 25:2, pp. 252–271, 1996.

[30] R. Rubinfeld. On the robustness of functional equations. In *Proc. 35th FOCS*, pp. 288–299, 1994.

[31] P. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52, pp. 2493–2496, 1995.

[32] P. Shor. Fault-tolerant quantum computation. In *Proc. 37th FOCS,* pp. 56–65, 1996.

[33] P. Shor. Algorithms for quantum computation: Discrete logarithm and factoring. *SIAM J. on Comput.*, 26:5, pp. 1484–1509, 1997.

[34] D. Simon. On the power of quantum computation. *SIAM J. on Comput.*, 26:5, pp. 1474–1483, 1997.

[35] A. Yao. Quantum circuit complexity. In *Proc. 34th FOCS*, pp. 352–361, 1993.

# A Appendix: Proof of Lemma 2

Proof of Lemma 2. Let $P$ be the plane defined in $\mathbb{R}^3$ by $\overline{\rho_1}$, $\overline{\rho_2}$ and $\overline{\rho_3}$. To simplify the discussion, we suppose w.l.o.g. that $\overline{\zeta_z^\pm}$ and $\overline{\zeta_x^\pm}$ are in $P$. Every one-qubit $\rho$ satisfying $\overline{\rho} \in P$ is a linear combination of $\rho_1$, $\rho_2$ and $\rho_3$. Therefore by linearity of $\boldsymbol{G}$ we get that it acts as the identity on $\{\rho : \overline{\rho} \in P\}^{\otimes n}$. Moreover it is sufficient to show that $\boldsymbol{G}$ is the identity on density matrices representing non-entangled pure states, since they form a basis for all density matrices.

For this, for every $k$, let $A_k$ be the set of density matrices representing $k$-qubit non-entangled pure states, and let $B_k = \{\zeta_x^\pm, \zeta_z^\pm\}^{\otimes n}$. We will show by induction on $k$ that, for every $0 \le k \le n$, the CPSO $\boldsymbol{G}$ 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 $(|00\rangle + |11\rangle)/\sqrt{2}$, can be written in terms of tensor products of the $\zeta$ states:

$$\Psi^+ \quad = \quad \tfrac{1}{2}(\zeta_x^+ \otimes \zeta_x^+ + \zeta_x^- \otimes \zeta_x^- + \zeta_z^+ \otimes \zeta_z^+ + \zeta_z^- \otimes \zeta_z^-) - \tfrac{1}{2}(\zeta_y^+ \otimes \zeta_y^+ + \zeta_y^- \otimes \zeta_y^-).$$

This can be generalized for the pure state $|\mu\rangle = (|\tilde{0}\rangle|\tilde{0}\rangle + |\tilde{1}\rangle|\tilde{1}\rangle)/\sqrt{2}$:

$$\mu \quad = \quad \tfrac{1}{2}(\tilde{\zeta}_x^+ \otimes \tilde{\zeta}_x^+ + \tilde{\zeta}_x^- \otimes \tilde{\zeta}_x^- + \tilde{\zeta}_z^+ \otimes \tilde{\zeta}_z^+ + \tilde{\zeta}_z^- \otimes \tilde{\zeta}_z^-) - \tfrac{1}{2}(\tilde{\zeta}_y^+ \otimes \tilde{\zeta}_y^+ + \tilde{\zeta}_y^- \otimes \tilde{\zeta}_y^-).$$

If we apply the CPSO $\boldsymbol{I}_{2^n} \otimes \boldsymbol{G}$ to the state $\mu$ we get:

$$(\boldsymbol{I}_{2^n} \otimes \boldsymbol{G})(\mu) \quad = \quad \tfrac{1}{2}(\tilde{\zeta}_x^+ \otimes \tilde{\zeta}_x^+ + \tilde{\zeta}_x^- \otimes \tilde{\zeta}_x^- + \tilde{\zeta}_z^+ \otimes \tilde{\zeta}_z^+ + \tilde{\zeta}_z^- \otimes \tilde{\zeta}_z^- - \tilde{\zeta}_y^+ \otimes \boldsymbol{G}(\tilde{\zeta}_y^+) - \tilde{\zeta}_y^- \otimes \boldsymbol{G}(\tilde{\zeta}_y^-)).$$

If $|\varphi\rangle$ and $|\varphi'\rangle$ are orthogonal $n$-qubit pure states, then let $\Phi^-_{\varphi\varphi'} = (|\varphi\rangle|\varphi'\rangle - |\varphi'\rangle|\varphi\rangle)/\sqrt{2}$. Since $\Phi^-_{\varphi\varphi'}$ is orthogonal to all symmetric $2n$-qubit pure states of the form $\psi \otimes \psi$, by projecting $(\boldsymbol{I}_{2^n} \otimes \boldsymbol{G})(\mu)$ to $\Phi^-_{\varphi\varphi'}$ we obtain:

$$\langle \Phi^-_{\varphi\varphi'}|(\boldsymbol{I}_{2^n} \otimes \boldsymbol{G})(\mu)|\Phi^-_{\varphi\varphi'}\rangle \quad = \quad -\tfrac{1}{2}\langle \Phi^-_{\varphi\varphi'}|\tilde{\zeta}_y^+ \otimes \boldsymbol{G}(\tilde{\zeta}_y^+)|\Phi^-_{\varphi\varphi'}\rangle - \tfrac{1}{2}\langle \Phi^-_{\varphi\varphi'}|\tilde{\zeta}_y^- \otimes \boldsymbol{G}(\tilde{\zeta}_y^-)|\Phi^-_{\varphi\varphi'}\rangle.$$

Since $\boldsymbol{G}$ is a CPSO, the left-hand side of this equality is non-negative and in the right-hand side both terms are non-positive. Therefore for every orthogonal $n$-qubit pure states $|\varphi\rangle$ and $|\varphi'\rangle$, we get

$$\langle \Phi^-_{\varphi\varphi'}|\tilde{\zeta}_y^+ \otimes \boldsymbol{G}(\tilde{\zeta_y}^+)|\Phi^-_{\varphi\varphi'}\rangle \quad = \quad \langle \Phi^-_{\varphi\varphi'}|\tilde{\zeta}_y^- \otimes \boldsymbol{G}(\tilde{\zeta_y}^-)|\Phi^-_{\varphi\varphi'}\rangle \quad = \quad 0.$$

A straightforward calculation then shows that $\boldsymbol{G}(\tilde{\zeta_y}^\pm) = \tilde{\zeta}_y^\pm$. Therefore $\boldsymbol{G}$ acts as the identity on density matrices $\tilde{\zeta}_z^\pm$, $\tilde{\zeta}_x^+$ and $\tilde{\zeta}_y^+$, which generate all density matrices, and thus $\boldsymbol{G}(\tilde{\rho}) = \tilde{\rho}$. ∎

# B Appendix: Proof of Theorem 5

**Fact 8** *Let $\boldsymbol{G}$ be a superoperator on $\mathbb{C}^{2\times 2}$. Let $0 \le \varepsilon \le 1$ be such that $\|\boldsymbol{G}(\zeta_x^\pm) - \zeta_x^\pm\|_1$, $\|\boldsymbol{G}(\zeta_y^\pm) - \zeta_y^\pm\|_1$, $\|\boldsymbol{G}(\zeta_z^\pm) - \zeta_z^\pm\|_1 \le \varepsilon$; then $\|\boldsymbol{G} - \boldsymbol{I}_2\|_\infty \le 8\varepsilon$.*

**Lemma 5** *Let $\overline{u}$ and $\overline{v}$ be two orthonormal vectors in $\mathbb{R}^3$, and $0 \le \varepsilon \le 1$ a constant. If $\boldsymbol{G}$ is a CPSO for one qubit such that $\|\overline{\boldsymbol{G}}(\pm\overline{u}) - \pm\overline{u}\| \le \varepsilon$ and $\|\overline{\boldsymbol{G}}(\pm\overline{v}) - \pm\overline{v}\| \le \varepsilon$, then $\|\boldsymbol{G} - \boldsymbol{I}_2\|_\infty \le 241\varepsilon$.*

**Proof:** We can suppose w.l.o.g. that $u = \zeta_x^+$ and $v = \zeta_z^+$. Let $\rho = \boldsymbol{G}(\zeta_y^+)$, where $\overline{\rho} = (x, y, z)$. From Lemma 1 it follows that $\|\boldsymbol{G}(\zeta_z^+) - \rho\|_1 \le \|\zeta_z^+ - \zeta_y^+\|_1 = \sqrt{2}$. By the assumption of this lemma we have that $\|\boldsymbol{G}(\zeta_z^+) - \zeta_z^+\|_1 \le \varepsilon$, and hence $\|\zeta_z^+ - \rho\|_1 \le \sqrt{2} + \varepsilon$. The same relation holds also for the other three fixed points $\zeta_z^-$, $\zeta_x^+$, and $\zeta_x^-$. As a result, the three coordinates of $\overline{\rho}$ have to obey the four inequalities

$$x^2 + y^2 + (z \pm 1)^2 \text{ and } (x \pm 1)^2 + y^2 + z^2 \quad \le \quad (\sqrt{2} + \varepsilon)^2 \quad \le \quad 2 + 4\varepsilon \qquad (3)$$

A second set of restrictions on $(x,y,z)$ comes from the complete positivity of $\boldsymbol{G}$. Again we use the decomposition of the EPR state $\Psi^+$, to analyze the two-qubit state:

$$\begin{aligned}(\boldsymbol{I}_2\otimes\boldsymbol{G})(\Psi^+) &= \tfrac{1}{2}(\zeta_x^+\otimes\boldsymbol{G}(\zeta_x^+)+\zeta_x^-\otimes\boldsymbol{G}(\zeta_x^-))+\tfrac{1}{2}(\zeta_z^+\otimes\boldsymbol{G}(\zeta_z^+)+\zeta_z^-\otimes\boldsymbol{G}(\zeta_z^-))\\ &\quad -\tfrac{1}{2}(\zeta_y^+\otimes\boldsymbol{G}(\zeta_y^+)+\zeta_y^-\otimes\boldsymbol{G}(\zeta_y^-)).\end{aligned}$$

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

$$\langle\Phi^-|(\boldsymbol{I}_2\otimes\boldsymbol{G})(\Psi^+)|\Phi^-\rangle \leq 2\varepsilon-\tfrac{1}{2}\langle\Phi^-|\zeta_y^+\otimes\boldsymbol{G}(\zeta_y^+)|\Phi^-\rangle-\tfrac{1}{2}\langle\Phi^-|\zeta_y^-\otimes\boldsymbol{G}(\zeta_y^-)|\Phi^-\rangle.$$

Since $\boldsymbol{G}$ is a CPSO, as in Lemma 2 we get $\langle\Phi^-|\zeta_y^+\otimes\rho|\Phi^-\rangle\leq 4\varepsilon$. 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 (3), 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 $\overline{\rho}$ satisfy $|x|,|z|\leq 18\varepsilon$.

These bounds imply

$$\|\boldsymbol{G}(\zeta_y^+)-\zeta_y^+\|_1 = \sqrt{x^2+(y-1)^2+z^2} \leq \sqrt{904\varepsilon}.$$

The same result can be proved for $\zeta_y^-$. Therefore by Fact 8 we can conclude the proof. ∎

Proof of Theorem 5. Let $\boldsymbol{G}$ be a CPSO which $\varepsilon$-satisfies the equations. First we will show there is a point $\overline{\rho}\in\mathcal{S}$ with $z$-coordinate 0 whose distance from $\overline{\boldsymbol{G}(|0\rangle\langle 0|)}$ is at most $10\sqrt{\varepsilon}$. The last two equations imply that $\|\boldsymbol{G}^2(|b\rangle\langle b|)-|b\rangle\langle b|\|_1\leq 3\sqrt{\varepsilon}$, for $b=0,1$. Therefore $\|\boldsymbol{G}^2(|0\rangle\langle 0|)-\boldsymbol{G}^2(|1\rangle\langle 1|)\|_1\geq 2-6\sqrt{\varepsilon}$, and by Lemma 1(a) we have $\|\boldsymbol{G}(|0\rangle\langle 0|)-\boldsymbol{G}(|1\rangle\langle 1|)\|_1\geq 2-6\sqrt{\varepsilon}$. Thus $\|\boldsymbol{G}(|b\rangle\langle b|)\|\geq 1-6\sqrt{\varepsilon}$, for $b=0,1$. Let $\tau=\rho(\frac{1}{2},\alpha)$, where $\boldsymbol{G}(|0\rangle\langle 0|)=\rho(p,\alpha)$. The first equation implies that $\|\overline{\tau}-\overline{\boldsymbol{G}(|0\rangle\langle 0|)}\|\leq 2\varepsilon$. Therefore for $\overline{\rho}=\overline{\tau}/\|\overline{\tau}\|$ we get $\|\boldsymbol{G}(|0\rangle\langle 0|)-\rho\|_1\leq 10\sqrt{\varepsilon}$.

The point $\overline{\rho}$ on $\mathcal{S}$ uniquely defines $\varphi\in[0,2\pi)$ such that $\overline{\boldsymbol{H}_\varphi(|0\rangle\langle 0|)}=\overline{\rho}$. One can verify that $\boldsymbol{H}_\varphi^{-1}\circ\boldsymbol{G}$ acts as the identity with error at most $19\sqrt{\varepsilon}$ on the four density matrices $|0\rangle\langle 0|$, $|1\rangle\langle 1|$, $\boldsymbol{H}_\varphi(|0\rangle\langle 0|)$, and $\boldsymbol{H}_\varphi(|1\rangle\langle 1|)$. From Lemma 5 we conclude that $\|\boldsymbol{G}-\boldsymbol{H}_\varphi\|_\infty\leq 4579\sqrt{\varepsilon}$. ∎