Self-Testing of Quantum Circuits*

Frédéric Magniez[1], Dominic Mayers[2], Michele Mosca[3,4], and Harold Ollivier[4]

[1] CNRS–LRI, University Paris-Sud, France
[2] Institute for Quantum Information, Caltech, USA
[3] Institute for Quantum Computing, University of Waterloo, Canada
[4] Perimeter Institute for Theoretical Physics, Waterloo, Canada

Abstract. We prove that a quantum circuit together with measurement apparatuses and EPR sources can be *self-tested*, i.e. fully verified without any reference to some trusted set of quantum devices.
To achieve our goal we define the notions of simulation and equivalence. Using these two concepts, we construct sets of simulation conditions which imply that the physical device of interest is equivalent to the one it is supposed to implement. Another benefit of our formalism is that our statements can be proved to be robust.
Finally, we design a test for quantum circuits whose complexity is polynomial in the number of gates and qubits, and the required precision.

1 Introduction

The purpose of this paper is to address the issue of deciding whether an implementation of a quantum circuit follows its specification. The precise setting in which we ask this question is that of *self-testing*. In such setting, the sources, the gates as well as the measurement apparatuses that are used, are considered as black-boxes. Moreover, none of them will be trusted to implement the quantum operator it is supposed to implement. As a consequence, the tests cannot make reference to another set of trusted and already characterized quantum devices. Such notion of self-testing follows quite closely the one defined initially for classical programs [1, 2], and is indeed based on its extension to quantum devices [3, 4] and to quantum testers of logical properties [5, 6].

The task of self-testing a set of quantum devices has been the focus of attention of two papers [3, 4], each of which considers a very particular set of assumptions. The work by Mayers and Yao [3] focuses on testing entangled EPR states shared between two distinguishable locations, A and B. The main assumptions they exploit are (1) locality, in the sense that the measurements at A commute with the measurements at B; and that (2) one can perform independent repetitions of the same experiments, in order to gather statistics (i.e., apparatuses have no memory of previous runs of the experiments). However, they do not assess the robustness of their results, i.e. if a state satisfies only approximately the required statistics then it is still close to an EPR state. Robustness is nonetheless

* Supported by QAIP, AlgoQP, NSERC, ARDA, ORDCF, CFI, CIAR, ResQuant.

an important property very much worth studying for practical reasons: first, one can never learn any statistics with infinite precision by sampling only; second, by their very nature, physical implementations are only approximate.

The work of Van Dam, Magniez, Mosca and Santha [4] focuses instead on testing gates. They make a number of assumptions, in addition to the above, (3) the ability to use the same gate in different places of the same experiment; (4) the ability to prepare and measure '0' and '1'; and (5) the dimension of the physical qubits (i.e., 2-level systems). Of these assumptions, the last one is certainly the most unrealistic one, but also the most crucial one. Relaxing it allows for "conspiracies" that can spoof the test.

Our work improves upon the results of [3] by making them robust. We also improve upon the paper [4] by removing the need for assumptions (3), (4) and (5). Let us detail the assumptions that we make. We assume that, (H1) the physical system we are working with consists of several identifiable sub-systems; that (H2) two subsystems interact only if we are applying a gate that has both those subsystems as input; (H3) each gate will behave identically in each experiment it is used in; and (H4) classical computation and control can be trusted.

First (Section 2), we define a precise mathematical framework for testing quantum devices. This is done by introducing the concept of *simulation* which amounts to producing the expected probability distribution for the outcomes of the measurements that are performed at the end of the computation. This alone will not be sufficient to propose efficient tests of quantum circuits. For this purpose, we introduce the concept of *equivalence* which relates the action of the devices on physical quantum systems used in the implementation, to the action of the unitary operators specifying the circuit on logical qubits.

Second (Section 3), we characterize unitary gates and circuits in terms of simulation. We explain how simulation implies equivalence, and how by composing equivalences one can derive the correctness of a physical implementation of a circuit. The main tool used in this section is the Mayers-Yao test of an EPR pair, which provides the most simple example in which simulation implies equivalence. We will then show that this test can be generalized and yields trusted input states to be used in conjunction with self-testable quantum circuits.

Last (Section 4), we prove the robustness of our characterization. In particular, we show that the EPR test of [3] can tolerate ε inaccuracy in the statistics and still yields states and measurements that are within $O(\varepsilon^{1/4})$ of their specification. Using the concepts of simulation and equivalence, such proofs are not so difficult although the robustness of the EPR test had been left open. The crucial point is to realize that the robustness of our characterization needs only to be stated on a rather small subspace in order for it to be of practical interest.

The important consequence of our study is the design of an efficient self-tester (Section 5) for quantum circuits with some specific input. Contrary to tomography which requires trusted measurement devices and an exponential number of statistics to be checked, our test has a complexity linear in the number of qubits and gates involved in the circuit, and polynomial in the required precision. We describe our tester in a general context and illustrate it with an example.

2 Testing Concepts

Notation. Set $\mathcal{H}_N = \mathbb{C}^N$, whose computational basis is $(|i\rangle)_{0\leq i<N}$. For $\alpha \in \mathbb{R}$, let $|\alpha\rangle = \cos\alpha|0\rangle + \sin\alpha|1\rangle$. In particular $|\frac{\pi}{2}\rangle = |1\rangle$. Denote by $|\phi^+\rangle$ the EPR state $\frac{1}{\sqrt{2}}(|0\rangle\otimes|0\rangle + |1\rangle\otimes|1\rangle)$, and by $|\Phi_n^+\rangle$ the tensor product of n EPR states: $|\Phi_n^+\rangle = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle\otimes|x\rangle$. Let $\mathcal{U}(H)$ be the set of unitary transformations on H, and $\mathcal{I}(H,H')$ the set of isomorphisms between H and H' which preserve the inner product. When $H = \mathcal{H}_N$ we let $\mathcal{U}(N) = \mathcal{U}(\mathcal{H}_N)$. In case of transformations over real spaces, we use the notations $\mathcal{O}(N)$ and $\mathcal{O}(H)$ instead of $\mathcal{U}(N)$ and $\mathcal{U}(H)$. For transformations M and M' on H, and $S \subseteq H$, the notation $M =_S M'$ means that the equality holds when restricted to S. When M is a linear transformation on A, we extend M on any tensor product $A\otimes B$ by $M\otimes \mathrm{Id}_B$.

Simulation. Two states *simulate* one another when they produce the same probability distributions of outcomes for two families of projectors. Here, the projectors are used in the same way measurement devices are used in a laboratory: they act as reference systems against which systems are tested.

More precisely, we are given a family of projectors $(P^w)_{w\in\mathcal{W}}$ acting on a physical space H and a state $|\psi\rangle \in H$, whose purpose is to implement some given and fixed projectors $|w\rangle\langle w|$ on the logical space $\mathcal{H}_N$ and a state $|\phi\rangle \in \mathcal{H}_N$.

Definition 1. *A quantum state* $|\psi\rangle \in H$ simulates *the quantum state* $|\phi\rangle \in \mathcal{H}_N$ *(with respect to* $(P^w)_{w\in\mathcal{W}}$*), if* $\|P^w|\psi\rangle\|^2 = |\langle w|\phi\rangle|^2$*, for every* $w \in \mathcal{W}$*.*

The notion of simulation can be rephrased for the whole space H. Assume we are given a family of states $(|\psi_i\rangle)_i$ of H that respectively simulate the basis states $(|i\rangle)_i$) (with respect to fixed set of projectors $(P^w)_{w\in\mathcal{W}}$). Then we say that H *simulates* $\mathcal{H}_N$.

We now extend the simulation notion to gates.

Definition 2. *Assume that* H *simulates* $\mathcal{H}_N$*:* $(|\psi_i\rangle)_i$ *simulates* $(|i\rangle)_i$ *(with respect to* $(P^w)_{w\in\mathcal{W}}$*). A unitary transformation* $G \in \mathcal{U}(H)$ simulates *the unitary transformation* $T \in \mathcal{U}(\mathcal{H}_N)$ *(with respect to* $(|\psi_i\rangle)_i$ *and* $(P^w)_{w\in\mathcal{W}}$*), if* $G|\psi_i\rangle$ *simulates* $T|i\rangle$ *(with respect to* $(P^w)_{w\in\mathcal{W}}$*), for every* i*.*

Equivalence. Testing a circuit as a single unitary operation is not an option. Indeed, this would require checking a simulation condition by sampling a probability distribution with a number of realizations exponential in the number of qubits involved in the circuit. Rather, we would like to test each of the physical devices that constitute the circuit individually in order to conclude that their composition simulates the whole circuit. Unfortunately, statements about simulation cannot be composed. This is the reason for the introduction of another concept, the concept of equivalence.

The equivalence notion we introduce is motivated by results of Mayers and Yao [3], but was not explicitly stated in their work. It is a mathematical notion

based on the possibility of transferring states which lie within a physical space into a logical system.

For a Hilbert space H, that will describe our physical system, we set a *logical* space $H_c = \mathcal{H}_N$ for some given integer N, and define $\bar{H} = H_c \otimes H$. We now identify H with $|0\rangle \otimes H$, and consider H as a subspace of $\bar{H}$.

First, we define the equivalence between a subspace of H and the logical system H_c with respect to a set of projectors. As for the notion of simulation, these projectors act as reference systems.

Definition 3. *Let $U \in \mathcal{U}(\bar{H})$. A subspace S of H is* U-equivalent *to H_c (with respect to $(P^w)_{w\in\mathcal{W}}$), if for every $w \in \mathcal{W}$, $P^w =_S U^\dagger(|w\rangle\langle w| \otimes \mathrm{Id}_H)U$.*

The above definition is equivalent to the commutative diagram: $\begin{array}{ccc} S & \xrightarrow{P^w} & S \\ U\downarrow & & \uparrow U^\dagger \\ \bar{H} & \xrightarrow{|w\rangle\langle w|\otimes \mathrm{Id}_H} & \bar{H} \end{array}$. Intuitively, the unitary transformation U ensures that the correspondence between the physical system H and the logical system H_c is well defined on S. As a consequence, the projectors P^w satisfy $P^w(S) \subseteq S$.

Define now the U-equivalence for states and gates that implies the simulation.

Definition 4. *Let S be a subspace of H. A state $|\psi\rangle \in S$ is* U-equivalent *to $|\phi\rangle \in H_c$ on S (with respect to $(P^w)_{w\in\mathcal{W}}$), if*
1. *S is U-equivalent to H_c,*
2. *$|\psi\rangle = U^\dagger(|\phi\rangle \otimes |\chi\rangle)$, for some $|\chi\rangle \in H$.*

Definition 5. *Let S be a subspace of H. A unitary transformation $G \in \mathcal{U}(H)$ is* (U, V)-equivalent *to $T \in \mathcal{U}(H_c)$ on S (with respect to $(P^w)_{w\in\mathcal{W}}$), if*
1. *S is U-equivalent to H_c,*
2. *$S' = G(S)$ is V-equivalent to H_c,*
3. *$G =_S V^\dagger(T \otimes W)U$, for some $W \in \mathcal{U}(H)$.*

This equivalence can be summarized by the following commutative diagram: $\begin{array}{ccccccc} S & \xleftarrow{P^w} & S & \xrightarrow{G} & S' & \xrightarrow{P^w} & S' \\ U^\dagger\uparrow & & \downarrow U & & V^\dagger\uparrow\downarrow V & & \uparrow V^\dagger \\ \bar{H} & \xleftarrow{|w\rangle\langle w|\otimes \mathrm{Id}_H} & \bar{H} & \xrightarrow{T\otimes W} & \bar{H} & \xrightarrow{|w\rangle\langle w|\otimes \mathrm{Id}_H} & \bar{H} \end{array}$.

Proposition 1. *Assume that $\{0, 1, \ldots, N-1\} \subseteq \mathcal{W}$. Let $(|\psi_i\rangle)_{0\le i<N}$ be a unit vector of $P^i(S)$. If $G \in \mathcal{U}(H)$ is equivalent to $T \in \mathcal{U}(H_c)$ on S, then G simulates T with respect to $(|\psi_i\rangle)_i$.*

When $H = \bigotimes_{i=1}^n H^i$, and $P^w = \bigotimes_{i=1}^n P_{H^i}^{w^i}$, where $w = (w^1, w^2, \ldots, w^n) \in \mathcal{W}^1 \times \mathcal{W}^2 \ldots \mathcal{W}^n$, we will often use the equivalence for matrices U that can be tensor product decomposed as $U = \bigotimes_i U^i$, for some $U^i \in \mathcal{U}(\bar{H}^i)$. In that case, we will say that G is *tensor equivalent* to T. Notice that $|\chi\rangle$ and W are not required to be also tensor product decomposable. This is because we want to encompass situations where the physical implementation G of the gate creates or destroys entanglement in the hidden degrees of freedom of the quantum register. Finally, note that the tensor equivalence on H implies the equivalence for each factor H^i, if the projectors $P_{H^i}^{w^i}$ are *complete*, namely if they linearly generate the identity in H^i. This will be the case in the rest of the paper.

Norm and approximation We consider the ℓ_2 norm $\|\cdot\|$ for states, and the corresponding operator $\|\cdot\|$ norm for linear transformations. These norms are stable by tensor product composition in the following sense: $\|u \otimes v\| = \|u\| \times \|v\|$, if u and v denote either vectors or linear transformations. We note $|\psi\rangle =^{\varepsilon} |\psi'\rangle$ when two vectors $|\psi\rangle, |\psi'\rangle$ are such that $\||\psi\rangle - |\psi'\rangle\| \leq \varepsilon$. We extend the ℓ_2-operator norm for restrictions of linear transformations on H. Namely if M is a linear transformation on H, and S is a subspace of H we define by $\|M\|_S = \sup(\|M|\psi\rangle\| : |\psi\rangle \in S \text{ and } \||\psi\rangle\| = 1)$. Similarly to states, we will write $M =^{\varepsilon}_S N$ when $\|M - N\|_S \leq \varepsilon$. We introduce the notion of *ε-simulation* by extending the notion of simulation where statistics equalities are only approximately valid up to some additive term $\leq \varepsilon$. The notions of equivalence can be similarly extended to *ε-equivalence*, by replacing each equality $=_S$ by $=^{\varepsilon}_S$.

3 Building a Test from Simulation

We consider a *test* as a set of simulation conditions, each of which can be checked through sampling. We show how to design efficient tests for quantum circuits by studying elementary tests that characterize sources and gates, and proving that the elementary tests are enough to characterize the whole circuit.

3.1 EPR State Testing

We rephrase Mayers and Yao [3] in our framework of quantum testing we just introduced. This is the simplest situation in which simulation implies equivalence. Their main result will be stated in an extended form that is most convenient for testing several registers successively. We will then use this result as a building block for finding other situations in which simulation implies equivalence.

From now and until the end of the paper, let $\mathcal{A}_0 = \{0, \frac{\pi}{8}, \frac{\pi}{4}\}$, $\mathcal{A}_1 = \{a + \frac{\pi}{2} : a \in \mathcal{A}_0\}$, and $\mathcal{A} = \mathcal{A}_0 \cup \mathcal{A}_1$. We fix orthogonal measurements $(P^a_A, P^{a+\pi/2}_A)_{a\in\mathcal{A}_0}$ and $(P^b_B, P^{b+\pi/2}_B)_{b\in\mathcal{A}_0}$ respectively on two Hilbert spaces A and B. Namely, we assume that $P^a_A + P^{a+\pi/2}_A = \mathrm{Id}_A$ and $P^a_B + P^{a+\pi/2}_B = \mathrm{Id}_B$, for every $a \in \mathcal{A}_0$.

Theorem 1. *Let $H = A \otimes B \otimes C$, and $|\psi\rangle \in H$ that simulates $|\phi^+\rangle$ with respect to $(P^a_A \otimes P^b_B \otimes \mathrm{Id}_C)_{a,b\in\mathcal{A}}$. Then there exist two unitary transformations $U_{\bar{A}} \in \mathcal{U}(\bar{A})$ and $U_{\bar{B}} \in \mathcal{U}(\bar{B})$ such that $|\psi\rangle$ is $(U_{\bar{A}} \otimes U_{\bar{B}})$-equivalent to $|\phi^+\rangle$ on $S = \mathrm{span}\{P^a_A \otimes P^b_B \otimes \mathrm{Id}_C|\psi\rangle : a, b \in \mathcal{A}\}$. Moreover the dimension of S is 4.*

In [3], the theorem was initially extended from S to the supports of $|\psi\rangle$ on each side. Nonetheless our results will be stated on S since this is sufficient for our purpose, and because their respective robustness can only be stated on S.

From Theorem 1 we derive by induction over n our main tool for testing n-qubit registers. Let $A = \bigotimes_{i=1}^n A^i$ and $B = \bigotimes_{i=1}^n B^i$. We now fix $(P^{a^i}_{A^i}, P^{a^i+\pi/2}_{A^i})_{a^i\in\mathcal{A}_0}$ and $(P^{b^i}_{B^i}, P^{b^i+\pi/2}_{B^i})_{b^i\in\mathcal{A}_0}$ to be orthogonal measurements on A^i and B^i respectively for every i. We denote $P^a_A = \bigotimes_{i=1}^n P^{a^i}_{A^i}$, with $a = (a^i)_{i=1}^n$ and $P^b_B = \bigotimes_{i=1}^n P^{b^i}_{B^i}$ with $b = (b^i)_{i=1}^n$.

Corollary 1. *Let $H = A \otimes B \otimes C$, and $|\Psi\rangle \in H$ that simulates $|\phi^+\rangle$ with respect to $(P_{A^i}^{a^i} \otimes P_{B^i}^{b^i} \otimes \mathrm{Id}_C)_{a^i,b^i \in \mathcal{A}}$ for every $i = 1, 2, \ldots, n$. Then there exist two unitary transformations $U_{\bar{A}} \in \bigotimes_i \mathcal{U}(\bar{A}^i)$ and $U_{\bar{B}} \in \bigotimes_i \mathcal{U}(\bar{B}^i)$ such that $|\Psi\rangle$ is $(U_{\bar{A}} \otimes U_{\bar{B}})$-equivalent to $|\Phi_n^+\rangle$ on $S = \mathrm{span}\{P_A^a \otimes P_B^b |\psi\rangle : a, b \in \mathcal{A}^n\}$. Moreover the dimension of S is 4^n.*

Therefore, testing a $2n$-qubit EPR state can be done by checking the probabilities of $O(n)$ outcomes, whereas there are $2^{O(n)}$ possible joint measurement outcomes.

3.2 Gate Testing

One-qubit Gate Testing. As a first attempt, we state how to check that a gate is equivalent to the identity.

Proposition 2. *Let $H = A \otimes B$ and $G \in \mathcal{U}(A)$. Let $|\psi\rangle \in H$ be such that $|\psi\rangle$ and $G|\psi\rangle$ simulate $|\phi^+\rangle$ with respect to some projectors $(P_A^a)_{a \in \mathcal{A}}$ and $(P_B^b)_{b \in \mathcal{A}}$. Then, $G \otimes \mathrm{Id}_B$ is tensor equivalent to $\mathrm{Id}_{A_c} \otimes \mathrm{Id}_{B_c}$ on $S = \mathrm{span}\{P_A^a \otimes P_B^b |\psi\rangle : a, b \in \mathcal{A}\}$.*

Stating the above result allows us to exhibit simple characteristics of the general method used for proving that gates can be self-tested. First, any gate testing requires two EPR tests. These are used to ensure that the input and output states together with the measurements act properly before and after the gate. These are *conspiracy tests*. Second, the fundamental properties of EPR states is used in order to show that the gate G and the measurements commute on the input state. This allows to perform tomography of the gate G. These tests will be referred to as *tomography tests*.

We can now state the general result concerning any 1-qubit real gate. We use the fact that any real gate on one qubit of the EPR state $|\phi^+\rangle$ can be undone by doing the same real gate on the other qubit.

Theorem 2. *Let $T \in \mathcal{O}(2)$. Let $H = A \otimes B$, $G_A \in \mathcal{U}(A)$, and $G_B \in \mathcal{U}(B)$. Let $|\psi\rangle \in H$ be such that $|\psi\rangle$ and $G_A G_B |\psi\rangle$ simulate $|\phi^+\rangle$, and such that $G_A|\psi\rangle$ simulates $(T \otimes \mathrm{Id}_2)|\phi^+\rangle$. Then, G_A is tensor equivalent to T on $S = \mathrm{span}\{P_A^a \otimes P_B^b |\psi\rangle : a, b \in \mathcal{A}\}$.*

Proof. The proof proceeds in two steps. First, we show that S and $G_A(S)$ are resp. $(U_{\bar{A}} \otimes U_{\bar{B}})$- and $(V_{\bar{A}} \otimes U_{\bar{B}})$-equivalent to $A_c \otimes B_c$. Second, we prove that there exists $W \in \mathcal{U}(A)$ such that $G_A \otimes \mathrm{Id}_B =_S (V_{\bar{A}}^\dagger \otimes U_{\bar{B}}^\dagger)(T \otimes W \otimes \mathrm{Id}_{\bar{B}})(U_{\bar{A}} \otimes U_{\bar{B}})$.

Theorem 1 applied to $|\psi\rangle$ and $G_A G_B |\psi\rangle$ gives $U_{\bar{A}}, V_{\bar{A}} \in \mathcal{U}(\bar{A})$ and $U_{\bar{B}}, V_{\bar{B}} \in \mathcal{U}(\bar{B})$ such that S and $(G_A \otimes G_B)(S)$ are respectively $(U_{\bar{A}} \otimes U_{\bar{B}})$- and $(V_{\bar{A}} \otimes V_{\bar{B}})$-equivalent to $A_c \otimes B_c$. This implies that $(G_A \otimes \mathrm{Id}_B)(S)$ is $(V_{\bar{A}} \otimes U_{\bar{B}})$-equivalent to $A_c \otimes B_c$. That is, we have the required tensor equivalences for S and $G_A(S)$. If we define $|\chi\rangle_{AB}$ as $U_{\bar{A}} \otimes U_{\bar{B}} |\psi\rangle = |\phi^+\rangle_{A_c B_c} \otimes |\chi\rangle_{AB}$, we then have $S = U_A^\dagger \otimes U_B^\dagger (A_c \otimes B_c \otimes |\chi\rangle_{AB})$.

The simulation of $T|\phi^+\rangle$ by $G_A|\psi\rangle$ can be rewritten within the density matrix formalism as: $\mathrm{tr}\left((P_A^a \otimes P_B^b) G_A |\psi\rangle\langle\psi| G_A^\dagger\right) = \mathrm{tr}\left((|a\rangle\langle a| \otimes |b\rangle\langle b|)(T \otimes \mathrm{Id}_2)|\phi^+\rangle\langle\phi^+|(T^\dagger \otimes \mathrm{Id}_2)\right)$. Using the commutativity

of the trace operator and $(\mathrm{Id}_2 \otimes |b\rangle\langle b|)|\phi^+\rangle\langle\phi^+| = \frac{1}{2}|b\rangle\langle b| \otimes |b\rangle\langle b|$, we get: $\mathrm{tr}\left((G_A^\dagger P_A^a G_A \otimes P_B^b)|\psi\rangle\langle\psi|\right) = \frac{1}{2}\,\mathrm{tr}\left(T^\dagger|a\rangle\langle a|T|b\rangle\langle b|\right)$.

Define the positive semi-definite operator $R^a_{\bar{A}\bar{B}} = (U_{\bar{A}} \otimes U_{\bar{B}})G_A^\dagger P_A^a G_A (U_{\bar{A}}^\dagger \otimes U_{\bar{B}}^\dagger)$. Since $|\psi\rangle$ is tensor equivalent to $|\phi^+\rangle$, we have: $\mathrm{tr}\left(R^a_{\bar{A}\bar{B}}(|b\rangle\langle b|_{A_c} \otimes |b\rangle\langle b|_{B_c} \otimes |\chi\rangle\langle\chi|_{AB})\right) = \mathrm{tr}\left(T^\dagger|a\rangle\langle a|T|b\rangle\langle b|\right)$.

Observe that the operators $U_{\bar{B}}$ and $U_{\bar{B}}^\dagger$ can be removed from the definition of $R^a_{\bar{A}\bar{B}}$ without modifying it. Therefore the previous equation can be extended for all $b, b' \in \mathcal{A}$ to $\mathrm{tr}\left(R^a_{\bar{A}\bar{B}}(|b\rangle\langle b|_{A_c} \otimes |b'\rangle\langle b'|_{B_c} \otimes |\chi\rangle\langle\chi|_{AB})\right) = \mathrm{tr}\left(T^\dagger|a\rangle\langle a|T\right)$, since the value of the left hand side does not depend on b'.

Now applying standard techniques of tomography, we get that ${}_{AB}\langle\chi|_{B_c}\langle b'|R^a_{\bar{A}\bar{B}}|b'\rangle_{B_c}|\chi\rangle_{AB} = (T^\dagger|a\rangle\langle a|T)$, for every $b' \in \mathcal{A}$. Since $R^a_{\bar{A}\bar{B}}$ is a semi-definite operator, the above conclusion can be rewritten as

$$R^a_{\bar{A}\bar{B}} =_{A_c\otimes B_c\otimes|\chi\rangle_{AB}} (T^\dagger|a\rangle\langle a|T) \otimes \mathrm{Id}_{A\otimes\bar{B}}. \tag{1}$$

The tensor-equivalence of $G_A(S)$ with $A_c \otimes B_c$ also gives $P_A^a =_{G_A(S)} (V_{\bar{A}}^\dagger \otimes U_{\bar{B}}^\dagger)(|a\rangle\langle a| \otimes \mathrm{Id}_{A\otimes\bar{B}})(V_{\bar{A}} \otimes U_{\bar{B}})$. Since $S = U_A^\dagger \otimes U_B^\dagger(A_c \otimes B_c \otimes |\chi\rangle)$, this can be used to replace P_A^a inside Equation (1). We obtain $(|a\rangle\langle a| \otimes \mathrm{Id}_{A\otimes\bar{B}})(V_{\bar{A}} \otimes U_{\bar{B}})G_A(U_{\bar{A}}^\dagger \otimes U_{\bar{B}}^\dagger)(T^\dagger \otimes \mathrm{Id}_{A\otimes\bar{B}}) =_{A_c\otimes B_c\otimes|\chi\rangle} (V_{\bar{A}} \otimes U_{\bar{B}})G_A(U_{\bar{A}}^\dagger \otimes U_{\bar{B}}^\dagger)(T^\dagger \otimes \mathrm{Id}_{A\otimes\bar{B}})(|a\rangle\langle a| \otimes \mathrm{Id}_{A\otimes\bar{B}})$. Then, we can conclude using standard linear algebra techniques that there exists $W \in \mathcal{U}(A)$ such that $G_A =_S (V_{\bar{A}}^\dagger \otimes U_{\bar{B}}^\dagger)(T \otimes W \otimes \mathrm{Id}_{\bar{B}})(U_{\bar{A}} \otimes U_{\bar{B}})$. □

Many-qubit Gate Testing. We now consider n-qubit real gates. We present our main result for testing gates using a slightly different formulation than in Theorem 2, which will be useful for the proof of Theorem 4. The proof is omitted since it is similar to the second step of the proof of Theorem 2.

Note that we will use that any real gate on one register of the state $|\Phi_n^+\rangle$ can be undone by doing the same real gate on the other register.

Theorem 3. *Let $T \in \mathcal{O}(2^n)$. Let $H = A \otimes B \otimes C$, where $A = \bigotimes_i A^i$ and $B = \bigotimes_i B^i$. Let $G_A \in \mathcal{U}(A)$ and $G_B \in \mathcal{U}(B)$. Let $|\Psi\rangle \in H$ and $U_{\bar{A}}, V_{\bar{A}} \in \bigotimes_i \mathcal{U}(\bar{A}_i)$ and $U_{\bar{B}}, V_{\bar{B}} \in \bigotimes_i \mathcal{U}(\bar{B}_i)$ be such that:*
1. $|\Psi\rangle$ is $(U_{\bar{A}} \otimes U_{\bar{B}})$-equivalent to $|\Phi_n^+\rangle$ on S with respect to $(P_A^a \otimes P_B^b)_{a,b\in\mathcal{A}^n}$,
2. $G_AG_B|\Psi\rangle$ is $(V_{\bar{A}} \otimes V_{\bar{B}})$-equivalent to $|\Phi_n^+\rangle$ on $(G_A \otimes G_B)(S)$ with respect to $(P_A^a \otimes P_B^b)_{a,b\in\mathcal{A}^n}$,
3. $G_A|\Psi\rangle$ simulates $(T \otimes \mathrm{Id}_{2^n})|\Phi_n^+\rangle$ with respect to $(P_A^a \otimes P_B^b \otimes \mathrm{Id}_C)_{a,b\in\mathcal{A}^n}$,
where $S = \mathrm{span}\{P_A^a \otimes P_B^b|\psi\rangle : a, b \in \mathcal{A}^n\}$. Then G_A is $(U_{\bar{A}} \otimes U_{\bar{B}}, V_{\bar{A}} \otimes U_{\bar{B}})$-equivalent to T on S.

As Theorems 2 & 3 exemplify, there is one restriction to the class of gates we are able to test. The ideal gates must have real-valued coefficients. Note that we are not making any assumptions about the physical implementation of gates, but rather on the ideal gates they are supposed to simulate. The problem lies in the fact that any complex gate of dimension d can be simulated using real

gates and appropriate measurement devices on a $2d$-dimensional Hilbert space, in a rather standard way [7]. On the positive side, this remark means that our restriction is not a limitation, as any quantum computation can be performed with real gates and real gates can be tested.

3.3 Circuit Testing

Now we state our main theorem and its corollary which relates elementary tests of sources and gates with the simulation of a whole circuit. They derive from Corollary 1 and Theorem 3, in the sense that (i) under certain conditions simulation implies equivalence, (ii) equivalence statements can be composed and (iii) that equivalence implies simulation.

Assume that some Hilbert space H has a tensor product decomposition $H = \bigotimes_{i=1}^{n} A^i \bigotimes B^i$. For any subset $I \subseteq \{1, 2, \ldots, n\}$, let H^I denote the Hilbert space $\bigotimes_{i\in I} A^i \bigotimes_{i\in I} B^i$, and $|\Phi^+\rangle_I$ the EPR state $|\Phi^+_{|I|}\rangle$ over $\bigotimes_{i\in I} A^i_c \bigotimes_{i\in I} B^i_c$.

Theorem 4. *Let $H = A \otimes B$, where $A = \bigotimes_i A^i$ and $B = \bigotimes_i B^i$. Let $I^1, I^2, \ldots, I^t \subseteq \{1, 2, \ldots, n\}$. Let $G^j_A \in \mathcal{U}(A^{I^j})$, $G^j_B \in \mathcal{U}(B^{I^j})$ and $T^j \in \mathcal{O}(A^{I^j}_c)$. Let $|\Psi\rangle \in A \otimes B$. Define inductively $|\Psi'^j\rangle = (G^j_A \otimes \mathrm{Id}_B)|\Psi^{j-1}\rangle$ and $|\Psi^j\rangle = (G^j_A \otimes G^j_B)|\Psi^{j-1}\rangle$, where $|\Psi^0\rangle = |\Psi'^0\rangle = |\Psi\rangle$. Assume:*
1. $|\Psi\rangle$ simulates $|\phi^+\rangle$ with respect to $(P^{a^i}_{A^i} \otimes P^{b^i}_{B^i})_{a^i,b^i\in\mathcal{A}}$, for every $i = 1, 2, \ldots, n$.
2. For $j = 1, \ldots, t$: $|\Psi^j\rangle$ simulates $|\phi^+\rangle$ with respect to $(P^{a^i}_{A^i} \otimes P^{b^i}_{B^i})_{a^i,b^i\in\mathcal{A}}$, for every $i \in I^j$.
3. For $j = 1, \ldots, t$: $|\Psi'^j\rangle$ simulates $T^j|\Phi^+\rangle_{I^j}$ w.r.t. $\left(P^a_{A^{I^j}} \otimes P^b_{B^{I^j}}\right)_{a,b\in\mathcal{A}^{I^j}}$.
Then $G^t_A G^{t-1}_A \cdots G^1_A$ is tensor equivalent to $T^t T^{t-1} \cdots T^1$ on $S = \mathrm{span}(P^a_A \otimes P^b_B|\Psi\rangle : a, b \in \mathcal{A}^n)$.

Corollary 2. *Let $|\Psi\rangle \in H$ satisfy the hypothesis of Theorem 4 for some decomposition of $G_A \in \mathcal{U}(A)$ and $T \in \mathcal{U}(A_c)$ into t gates acting only on a constant number of qubits. Then, for every $x \in \{0, 1\}^n$, the state $\sqrt{2^n}\,\mathrm{tr}_B(P^x_B|\Psi\rangle)$ simulates $|x\rangle_{A_c}$ with respect to $(P^w_A)_{w\in\mathcal{A}^n}$. Moreover G_A simulates T with respect to the above identification, and the number of statistics to be checked is in $O(t)$.*

4 Robustness of Testing

Until now, our interest has been focused on the possibility of self-testing a quantum circuit when outcome probabilities are known with perfect accuracy. To be of practical interest, our results must be extended to the situation of finite accuracy. We show below that it is possible and that the relevant results for testing are robust in the following way: if the statistics are close to the ideal ones, then the states, the measurements and the gates are also close to ones that are equivalent to the ideal ones. This notion of robustness follows the ones of [8, 9] for classical computing and of [4] for quantum computing.

The proofs of this section follow the structure of the exact case, and are omitted due to the lack of space. They will be in the full version of the paper. We first state the robustness of Theorem 1.

Theorem 5. *Let $H = A \otimes B \otimes C$, and $|\psi\rangle \in H$ that ε-simulates $|\phi^+\rangle$ with respect to $(P_A^a \otimes P_B^b \otimes \mathrm{Id}_C)_{a,b\in\mathcal{A}}$. Then there exist $U_{\bar{A}} \in \mathcal{U}(\bar{A})$ and $U_{\bar{B}} \in \mathcal{U}(\bar{B})$ such that $|\psi\rangle$ is $(O(\varepsilon^{1/4}), (U_{\bar{A}} \otimes U_{\bar{B}}))$-equivalent to $|\phi^+\rangle$ on S.*

This result can be generalized to the case of a source producing a state $|\Psi\rangle$ that simulates n EPR pairs. In such case equivalence holds within $O(4^n\varepsilon^{1/4})$.

Corollary 3. *Let $H = A \otimes B \otimes C$, where $A = \bigotimes_i A^i$ and $B = \bigotimes_i B^i$. Let $|\Psi\rangle \in H$ be a state that ε-simulates $|\phi^+\rangle$ with respect to $(P_{A^i}^{a^i} \otimes P_{B^i}^{b^i})_{a^i,b^i\in\mathcal{A}}$, for every $i = 1, 2, \ldots, n$. Then, $|\Psi\rangle$ is $O(4^n\varepsilon^{1/4})$-equivalent to $|\Phi_n^+\rangle$.*

Another corollary we will use in the context of circuit testing concerns the case of n sources of EPR pairs that are tested simultaneously. This is qualitatively different from the previous situation as the state $|\Psi\rangle$ that is tested is assumed to be separable across the tensor product decomposition of H into $H^i = A^i \otimes B^i$.

Corollary 4. *Let $H = A \otimes B \otimes C$, where $A = \bigotimes_i A^i$ and $B = \bigotimes_i B^i$. Let $|\Psi\rangle \in H$ be a separable state across the tensor product decomposition of H into $A_i \otimes B_i$, and such that it ε-simulates $|\phi^+\rangle$ with respect to $(P_{A^i}^{a^i} \otimes P_{B^i}^{b^i})_{a^i,b^i\in\mathcal{A}}$, for every $i = 1, 2, \ldots, n$. Then, $|\Psi\rangle$ is $O(n\varepsilon^{1/4})$-equivalent to $|\Phi_n^+\rangle$.*

Now we concentrate on the robustness of Theorem 3. Note that the exponential dependency in the number n of qubits is not a problem, since we will use this theorem for constant n only (typically $n \leq 3$).

Theorem 6. *Let $T \in \mathcal{O}(2^n)$. Let $H = A \otimes B \otimes C$, where $A = \bigotimes_i A^i$ and $B = \bigotimes_i B^i$. Let $G_A \in \mathcal{U}(A)$ and $G_B \in \mathcal{U}(B)$. Let $|\Psi\rangle \in H$ and $U_{\bar{A}}, V_{\bar{A}} \in \bigotimes_i \mathcal{U}(\bar{A}_i)$ and $U_{\bar{B}}, V_{\bar{B}} \in \bigotimes_i \mathcal{U}(\bar{B}_i)$ be such that:*
1. $|\Psi\rangle$ is $(\varepsilon, (U_{\bar{A}} \otimes U_{\bar{B}}))$-equivalent to $|\Phi_n^+\rangle$ on S with respect to $(P_A^a \otimes P_B^b)_{a,b\in\mathcal{A}^n}$,
2. $G_A \otimes G_B|\Psi\rangle$ is $(\varepsilon, (V_{\bar{A}} \otimes V_{\bar{B}}))$-equivalent to $|\Phi_n^+\rangle$ on $(G_A \otimes G_B)(S)$ with respect to $(P_A^a \otimes P_B^b)_{a,b\in\mathcal{A}^n}$,
3. $G_A|\Psi\rangle$ ε-simulates $(T \otimes \mathrm{Id}_{2^n})|\Phi_n^+\rangle$ with respect to $(P_A^a \otimes P_B^b \otimes \mathrm{Id}_C)_{a,b\in\mathcal{A}^n}$.
Then $G_A \otimes \mathrm{Id}_B$ is $(2^{O(n)}\sqrt{\varepsilon}, (U_{\bar{A}} \otimes U_{\bar{B}}, V_{\bar{A}} \otimes U_{\bar{B}}))$-equivalent to $T \otimes \mathrm{Id}_{\bar{B}_c}$ on S.

5 Testing a Circuit on a Specific Input

We have seen in Section 3 how to test the implementation of a circuit on a whole subspace S of the input space. Surprisingly, this is much easier than to test a circuit on a particular input. In fact, using EPR pairs allows for the simultaneous testing of all possible inputs, while making the selection of a particular one difficult. The obvious choice would be to post-select the outcome of the B-side measurements of the EPR pairs. Unfortunately, the selected input state would then be prepared with exponentially small probability.

We circumvent the aforementioned difficulty using the fact that our circuits can have classically controlled feedback that decides which gates need to be applied based on some measurement results. Given a circuit for a unitary transformation T and an input x, we first measure the B-side of the (alleged) EPR

states. This yields a classical state y on the A-side. Second, we design a circuit $T_{x,y}$ whose purpose is to flip the corresponding bits of y in order to get the input x, and to apply the original circuit for T. Third, we run the modified circuit on the state y that was prepared on the A-side. Finally, we test that this modified circuit implemented the correct computation. This includes verifying the gates and the preparation of all input states $|x'\rangle$—and in particular the preparation of $|x\rangle$—obtained by measuring $|\Psi\rangle$ on the B-side. See Figure 1 for an example.

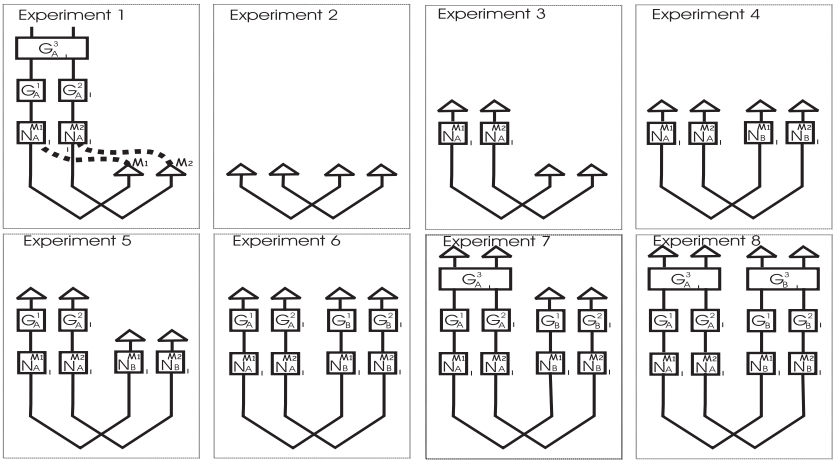

Fig. 1. The experiments to test the circuit consisting of gates $G_A^3 G_A^2 G_A^1$ on input $|00\rangle$. We first run the computation (Experiment 1) once on the modified circuit, where the intermediate measurements on the B-side yield the outcomes M_1, M_2. We now wish to check that the output of the circuit is correct. We carry on implementing Experiments 2 through 8 each a number of times in $\log(n/\gamma)/\varepsilon^8$, where ε is the required precision and γ is some confidence parameter.

The parameters of our test is a circuit for $T \in \mathcal{U}(2^n)$, that is a gate decomposition $T^t T^{t-1} \cdots T^1 = T$; a binary string $x \in \{0,1\}^n$; a precision $\varepsilon > 0$; and a confidence $\gamma > 0$. We assume that each gate T^i acts on a constant number of qubits (say ≤ 3). The input is a source of quantum states $|\Psi\rangle$ spread over n pairs of quantum registers; gates G_A^j and G_B^j acting on the same register numbers as T^j, for every j; auxiliary gates N_A^i acting on the i-th register of A; and orthogonal measurements $(P_{A^i}^a, P_{A^i}^{a+\pi/2})_{a \in \mathcal{A}_0}$ and $(P_{B^i}^b, P_{B^i}^{b+\pi/2})_{b \in \mathcal{A}_0}$. The goal is to test that, firstly, $\sqrt{2^n}\,\mathrm{tr}_B(P_B^b|\Psi\rangle)$ simulates $|b\rangle$ and that, secondly, the implemented circuit G_A simulates T.

Circuit Test $(T^1, T^2, \ldots, T^t \in \mathcal{U}(2^n), x \in \{0,1\}^n, \varepsilon > 0, \gamma > 0)$

1. Prepare a state $|\Psi\rangle$ of n EPR states into n pairs on $A^1 \otimes B^1, \ldots, A^n \otimes B^n$
2. Measure the B-side of $|\Psi\rangle$ using $(P_B^b)_{b \in \{0,\pi/2\}^n}$ and let y be the outcome
3. Let $T_{x,y}$ be the circuit that changes the input $|y\rangle$ into $|x\rangle$ and applies T

4. Prepare on the A-side the circuit G_A implementing $T_{x,y}$ using the t gates G_A^j and at most n gates N_A^i. Let $t' \leq t+n$ be the total number of gates
5. Run the circuit on the A-side and measure using $(P_A^a)_{a\in\{0,\pi/2\}^n}$
6. Approximate all the following statistics by repeating $O(\frac{\log(n/\gamma)}{\varepsilon})$ times the following measurements (where we use the notation of Theorem 4):
   (a) Measure $|\Psi\rangle$ using $(P_{A^i}^{a^i} \otimes P_{B^i}^{b^i})_{a^i,b^i\in\mathcal{A}_0}$, for every $i = 1, 2, \ldots, n$
   (b) For $j = 1, \ldots, t'$: Measure $|\Psi^j\rangle$ using $(P_{A^i}^{a^i} \otimes P_{B^i}^{b^i})_{a^i,b^i\in\mathcal{A}}$, for every $i \in I^j$
   (c) For $j = 1, \ldots, t'$: Measure $|\Psi'^j\rangle$ using $(P_{A^{Ij}}^{a} \otimes P_{B^{Ij}}^{b})_{a,b\in\mathcal{A}_0^{I^j}}$
7. Accept if all the statistics are correct up to an additive error ε

Theorem 7. *Let $T^1, T^2, \ldots, T^t \in \mathcal{U}(2^n), x \in \{0,1\}^n, \varepsilon > 0, \gamma > 0$.*

*If **Circuit Test**$(T^1, T^2, \ldots, T^t, x, \varepsilon, \gamma)$ accepts then, with probability $1-O(\gamma)$, the outcome probability distribution of the circuit (in step 5) is at total variance distance $O((t+n)\varepsilon^{1/8})$ from the distribution that comes from the measurement of $T^tT^{t-1}\cdots T^1|x\rangle$ by $(|a\rangle\langle a|)_{a\in\{0,\pi/2\}^n}$.*

*Conversely, if **Circuit Test**$(T^1, T^2, \ldots, T^t, x, \varepsilon, \gamma)$ rejects then, with probability $1 - O(\gamma)$, at least one of the state $|\Psi\rangle$, the gates G_A^i, G_B^i and N_A^i is not $O(\varepsilon)$-equivalent to respectively either $|\Phi_n^+\rangle$, $(|a\rangle\langle a|_{A_c^i})_{a\in\mathcal{A}}$, $(|b\rangle\langle b|_{B_c^i})_{b\in\mathcal{A}})$, T^i, ${}^t(T^i)$ and $\mathrm{NOT}_{A_c^i}$, on $S = \mathrm{span}(P_A^a \otimes P_B^b|\Psi\rangle : a, b \in \mathcal{A}^n)$ with respect to the projections $(P_A^a \otimes P_B^b)_{a,b\in\mathcal{A}^n}$.*

*Moreover **Circuit Test**$(T^1, T^2, \ldots, T^t, x, \varepsilon, \gamma)$ consists of $O(\frac{tn}{\varepsilon}\log(n/\gamma))$ samplings.*

Proof. We first describe the use of the hypotheses we made in Section 1. The assumption (H4) of trusted classical control is used to ensure that the circuit has the same behavior on $P_B^y|\Psi\rangle$ as it would have on $|\Psi\rangle$. Hypothesis (H3) implies that we can repeat several times the same experiment, and hypotheses (H1) and (H2) allow us to state which parts of our system are separated from the others.

First, using the Chernoff-Hoeffding bound, we know that the expectation of any bounded random variable can be approximated within precision $O(\varepsilon)$ with probability $1 - O(\gamma)$ by $\frac{\log(1/\gamma)}{\varepsilon^2}$ independent samplings. Moreover if the expectation is lower bounded by a constant, then $\frac{\log(1/\gamma)}{\varepsilon}$ independent samplings are enough. In our case, the random variable is the two possible outcomes of a measurement. Call them 0 or 1. Since we can count both 0 and 1 outcomes, one of the corresponding probabilities is necessarily at least $1/2$. Therefore we get that each statistics we have from **Circuit Test** are approximated within precision $O(\varepsilon)$ with probability $1 - O(\gamma)$. From now on, we assume that all statistics are given within this precision.

First, we prove the robustness of **Circuit Test**. We derive the correct simulation of the implemented circuit using the approximate version of Corollary 2, that we get using Theorems 5 and 6. More precisely, using Corollary 4 for the initial source we get that $|\Psi\rangle$ is $O(n\varepsilon^{1/4})$-equivalent to $|\Phi_n^+\rangle$ on S. For other steps, due to the application of the j-th gate, the state $|\Psi^j\rangle$ is not necessarily a separable state across the n-registers. So we apply Corollary 3 on the registers where the j-th gate is applied, that is on a constant number of register, which gives

the required $O(\varepsilon^{1/4})$-equivalence on the corresponding registers. Then, Theorem 6 concludes that the j-th gate is $O(j\varepsilon^{1/8})$-equivalent to the expected one, similarly for the intermediate states of the circuit and for the measurements. Note the error propagation is controlled by two properties: the stability of the ℓ_2 operator-norm by tensor product composition, and the triangle inequality.

Then, we focus on the run of $T_{x,y}$ in Step 5. We have to justify that the (normalized) outcome state $\sqrt{2^n}P_B^y|\Psi\rangle \in S$ of the measurement $(P_B^b)_{b\in\{0,\pi/2\}^n}$ is $O(n\varepsilon^{1/4})$-equivalent to $|y\rangle$ with respect to $(P_A^a)_{a\in\{0,\pi/2\}^n}$ on $P_B^y(S)$. Recall that by assumption the initial state $|\Psi\rangle$ is separable across the n pairs of registers, namely $|\Psi\rangle = \bigotimes_i |\psi^i\rangle$ with $|\psi^i\rangle \in A^i \otimes B^i$. For each pair of registers $A^i \otimes B^i$, using Theorem 5 we get that $|\psi^i\rangle$ is $O(\varepsilon^{1/4})$-equivalent to $|\phi^+\rangle$ with respect to $(P_{A^i}^{a^i} \otimes P_{B^i}^{b^i})_{a^i,b^i\in\mathcal{A}}$ on $S^i = \mathrm{span}(P_{A^i}^{a^i} \otimes P_{B^i}^{b^i}|\psi^i\rangle : a^i, b^i \in \mathcal{A})$. In particular the projections $P_{A^i}^{a^i} \otimes P_{B^i}^{b^i}$ are also $O(\varepsilon^{1/4})$-equivalent to $|a^i\rangle\langle a^i| \otimes |b^i\rangle\langle b^i|$ on S^i. Therefore the normalized outcome state $\sqrt{2}P_B^{y^i}|\psi^i\rangle$ (which is in S^i) is $O(\varepsilon^{1/4})$-equivalent to $|y^i\rangle$ with respect to $(P_{A^i}^{a^i})_{a^i\in\{0,\pi/2\}}$ on $P_{B^i}^{y^i}(S^i)$. We then get our equivalence for the whole outcome state using those intermediate equivalences together with the stability of the ℓ_2 operator-norm by tensor product composition, and the triangle inequality of the norm. Finally, we combine the above approximate equivalences, one for the circuit and one for the input, and get that the outcome distribution is at total variation distance at most $O((t+n)\varepsilon^{1/8})$ from the expected one.

The second part of the theorem is the soundness of **Circuit Test**. Since ℓ_2-distance between states bounds the statistics bias of their measures, the proof of the contraposition directly follows: if our objects are ε-equivalent to the specification, then their statistics have a bias which is upper bounded by $O(\varepsilon)$.

□

References

1. Blum, M., Kannan, S.: Designing programs that check their work. J. ACM **42**(1) (1995) 269–291
2. Blum, M., Luby, M., Rubinfeld, R.: Self-testing/correcting with applications to numerical problems. J. Computer and System Sciences **47**(3) (1993) 549–595
3. Mayers, D., Yao, A.: Quantum cryptography with imperfect apparatus. In: Proceedings of 39th IEEE FOCS. (1998) 503–509
4. Dam, W., Magniez, F., Mosca, M., Santha, M.: Self-testing of universal and fault-tolerant sets of quantum gates. In: Proc. of 32nd ACM STOC. (2000) 688–696
5. Buhrman, H., Fortnow, L., Newman, I., Röhrig, H.: Quantum property testing. In: Proc. of 14th ACM-SIAM SODA. (2003) 480–488
6. Friedl, K., Magniez, F., Santha, M., Sen, P.: Quantum testers for hidden group properties. In: Proc. of the 28th MFCS. (2003) 419–428
7. Rudolph, T., Grover, L.: A 2–rebit gate universal for quantum computing (2002)
8. Rubinfeld, R., Sudan, M.: Robust characterizations of polynomials with applications to program testing. SIAM J. Computing **25**(2) (1996) 23–32
9. Rubinfeld, R.: On the robustness of functional equations. SIAM J. Computing **28**(6) (1999) 1972–1997