Few Single-Qubit Measurements Suffice to Certify Any Quantum State

Meghal Gupta* William He† Ryan O'Donnell‡

June 13, 2025

Abstract

A fundamental task in quantum information science is *state certification*: testing whether a lab-prepared n-qubit state is close to a given hypothesis state. In this work, we show that *every* pure hypothesis state can be certified using only $O(n^2)$ single-qubit measurements applied to $O(n)$ copies of the lab state. Prior to our work, it was not known whether even sub-exponentially many single-qubit measurements could suffice to certify arbitrary states. This resolves the main open question of Huang, Preskill, and Soleimanifar (FOCS 2024, QIP 2024).

1 Introduction

A fundamental task in quantum information science is to test whether an unknown n-qubit state ρ_{lab} prepared in the lab is equal (or close) to a known target state $|\mathsf{hyp}\rangle$. This task is known as *quantum state certification*. It is essential for benchmarking quantum devices, validating the outcomes of quantum experiments, and verifying the correctness of practical implementations of quantum algorithms and protocols. See e.g. [BOW19, ZH19b, KR21, HPS24] for in-depth discussions of the importance and applications of quantum state certification.

More formally, we are given a classical description of (or some form of access to) a known pure state $|\mathsf{hyp}\rangle$, along with copies of an unknown (possibly mixed) lab state ρ_{lab}. Our goal is to decide whether the fidelity $\langle\mathsf{hyp}|\,\rho_{\mathsf{lab}}\,|\mathsf{hyp}\rangle$ is close to 1, in which case we Accept, or significantly smaller than 1, in which case we Reject.

If we ignore measurement complexity, the optimal-copy-complexity approach is straightforward: measure each copy of ρ_{lab} using the POVM $(|\mathsf{hyp}\rangle\langle\mathsf{hyp}|, \mathrm{Id} - |\mathsf{hyp}\rangle\langle\mathsf{hyp}|)$, and accept if the first outcome occurs frequently enough. This requires only $\Theta(1/\varepsilon)$ copies to distinguish $\langle\mathsf{hyp}|\,\rho_{\mathsf{lab}}\,|\mathsf{hyp}\rangle < 1-\varepsilon$ from $\langle\mathsf{hyp}|\,\rho_{\mathsf{lab}}\,|\mathsf{hyp}\rangle = 1$ (or even $\geq 1-\varepsilon/2$).

However, actually implementing this n-qubit measurement is roughly as hard as preparing the state $|\mathsf{hyp}\rangle$. Given that the main use of certification is to certify that we can in fact prepare $|\mathsf{hyp}\rangle$, this renders this certification algorithm pretty useless. What we'd actually like is a much simpler algorithm for certifying states—ideally something that's polynomially complex even when preparing $|\mathsf{hyp}\rangle$ is exponentially complex (as it is for most states). These considerations motivate certification algorithms based solely on single-qubit measurements: This would allow for efficient certification even when preparation is more complex and unreliable.

*UC Berkeley, meghal@berkeley.edu
†Carnegie Mellon University, wrhe@cs.cmu.edu
‡Carnegie Mellon University, odonnell@cs.cmu.edu

Prior to this work, it was unknown whether all pure states $|\mathsf{hyp}\rangle$ could be certified using only few single-qubit measurements.[1] Several algorithms had been developed for this task, but each required some significant concession. For example, some algorithms require exponentially many copies of ρ_{lab}: [FL11, SLP11, AGKE15]. Others apply only to restricted classes of hypothesis states or restricted noise models: [HMT06, FL11, AGKE15, HM15, MNS16, MTH17, TM18, GKEA18, HT19, LHZ19, LYS+19, YSG19, ZH19a, LHS+21, HPS24].

Indeed, given each of these prior results comes with caveats, it was natural to suspect that fully general certification using only polynomially many single-qubit measurements might be impossible. Even after Huang, Preskill, and Soleimanifar [HPS24] gave such an algorithm for Haar-random target states $|\mathsf{hyp}\rangle$ (which are typically highly entangled), they left it open to identify an explicit state $|\mathsf{hyp}\rangle$ for which certification with single-qubit measurements requires super-polynomially many copies.

Perhaps surprisingly, this work shows that there is no such state: Efficient certification with single-qubit measurements is possible for *all* quantum states. We present a simple, general quantum state certification algorithm that works for every pure hypothesis state $|\mathsf{hyp}\rangle$, and which uses only single-qubit measurements applied to $O(n/\varepsilon)$ copies of ρ_{lab}:

Main Theorem. There exists an algorithm that given parameters $\delta, \varepsilon > 0$, oracle access to a pure state $|\mathsf{hyp}\rangle$ via the model in Definition 5, and $O(n\varepsilon^{-1}\ln(1/\delta))$ copies of ρ_{lab}, makes only single-qubit measurements to the copies of ρ_{lab} and outputs:

- ACCEPT with probability at least $1-\delta$ if $\langle\mathsf{hyp}|\,\rho_{\mathsf{lab}}\,|\mathsf{hyp}\rangle \geq 1 - \frac{\varepsilon}{2n}$.
- REJECT with probability at least $1-\delta$ if $\langle\mathsf{hyp}|\,\rho_{\mathsf{lab}}\,|\mathsf{hyp}\rangle \leq 1-\varepsilon$.

Moreover, the algorithm runs in time linear in the number of measurements.

This theorem follows directly from Theorem 1 below, and repetition:

Theorem 1. There exists an algorithm that given oracle access to a pure state $|\mathsf{hyp}\rangle$ via the model in Definition 5 and 1 copy of a mixed state ρ_{lab}, makes only single-qubit measurements to ρ_{lab} and outputs:

- ACCEPT with probability at least $\langle\mathsf{hyp}|\,\rho_{\mathsf{lab}}\,|\mathsf{hyp}\rangle$.
- REJECT with probability at least $\frac{1-\langle\mathsf{hyp}|\rho_{\mathsf{lab}}|\mathsf{hyp}\rangle}{n}$.

Future directions. Several natural questions remain open for future work. We state two of them below:

First, a basic information-theoretic argument shows that any certification algorithm for a pure target state $|\mathsf{hyp}\rangle$ must use at least $\Omega(1/\varepsilon)$ copies of ρ_{lab}, even without restricting to single-qubit measurements. Can stronger lower bounds be proven for algorithms limited to single-qubit measurements? In particular, our algorithm uses $O(n/\varepsilon)$ copies — is this dependence on n necessary?

Second, our algorithm is only $1/n$-tolerant: To guarantee ρ_{lab} is accepted with high probability, it needs to satisfy $\langle\mathsf{hyp}|\,\rho_{\mathsf{lab}}\,|\mathsf{hyp}\rangle \geq 1 - O(\varepsilon/n)$, rather than $1-O(\varepsilon)$. Can this dependence on n be improved or even eliminated? For instance, is it possible to design a test that distinguishes between the cases $\langle\mathsf{hyp}|\,\rho_{\mathsf{lab}}\,|\mathsf{hyp}\rangle \geq 1-\varepsilon/2$ and $\langle\mathsf{hyp}|\,\rho_{\mathsf{lab}}\,|\mathsf{hyp}\rangle \leq 1-\varepsilon$?

[1] We remark that if $|\mathsf{hyp}\rangle$ is allowed to be a mixed state, it is known that certification in general requires exponentially many copies, even when arbitrarily complex measurements are allowed [CHW07, OW21].

1.1 Algorithm Overview

In this section, we informally describe our algorithm to test whether a candidate state $|\mathsf{lab}\rangle$ is equal to $|\mathsf{hyp}\rangle$ or has overlap at most $1-\varepsilon$ with $|\mathsf{hyp}\rangle$. We can decompose $|\mathsf{hyp}\rangle$ as

$$|\mathsf{hyp}\rangle = \frac{1}{\sqrt{2}} |e_0\rangle |\mathsf{hyp}^0\rangle + \frac{1}{\sqrt{2}} |e_1\rangle |\mathsf{hyp}^1\rangle ,$$

for some orthonormal basis $\{|e_0\rangle , |e_1\rangle\}$, where $|\mathsf{hyp}^0\rangle$ and $|\mathsf{hyp}^1\rangle$ are $(n-1)$-qubit states.[2]

Let U be any unitary operator satisfying $U|\mathsf{hyp}^1\rangle = |\mathsf{hyp}^0\rangle$. If $|\mathsf{lab}\rangle = |\mathsf{hyp}\rangle$, then if we similarly write

$$|\mathsf{lab}\rangle = \gamma_0 |e_0\rangle |\mathsf{lab}^0\rangle + \gamma_1 |e_1\rangle |\mathsf{lab}^1\rangle ,$$

it must be true that $\gamma_0 |\mathsf{lab}^0\rangle = \gamma_1 U |\mathsf{lab}^1\rangle$. The first step of our algorithm (Algorithm 1 with $k=1$) essentially checks how much this relation is violated for some specific U. Now we will pick U such that we can indeed check this relation with an algorithm that uses only single-qubit measurements. To do this, we select a particular basis $\mathcal{B}$ for $(\mathbb{C}^2)^{\otimes n-1}$ such that:

1. $|\mathsf{hyp}^0\rangle$ and $|\mathsf{hyp}^1\rangle$, when written in this basis, have coefficients with equal magnitudes.[3]
2. One can implement measurements in this basis by adaptively measuring single qubits at a time.

The existence of such a basis is shown in Lemma 4. The unitary U is then defined as the unique diagonal operator in $\mathcal{B}$ mapping $|\mathsf{hyp}^1\rangle$ to $|\mathsf{hyp}^0\rangle$.

Our algorithm first measures the last $n-1$ qubits of the state in basis $\mathcal{B}$. Given a particular outcome, denote by $|z\rangle$ what the first qubit would have been if $|\mathsf{lab}\rangle = |\mathsf{hyp}\rangle$. Next, the algorithm measures the first qubit in the basis $|z\rangle , |z^\perp\rangle$ and rejects if it gets the outcome $|z^\perp\rangle$ (which it never would if $|\mathsf{lab}\rangle = |\mathsf{hyp}\rangle$). The first part of the proof of Lemma 7 shows the rejection probability at this step is exactly $\frac{1}{2}\left\| \gamma_0 |\mathsf{lab}^0\rangle - \gamma_1 U |\mathsf{lab}^1\rangle \right\|^2$.

If the algorithm does not reject, this implies the relation $\gamma_0 |\mathsf{lab}^0\rangle = U \gamma_1 |\mathsf{lab}^1\rangle$ approximately holds. Therefore, if $|\mathsf{lab}\rangle$ were far from $|\mathsf{hyp}\rangle$, it must be that this distance can be attributed to $|\mathsf{lab}^0\rangle$ being far from $|\mathsf{hyp}^0\rangle$ and/or $|\mathsf{lab}^1\rangle$ being far from $|\mathsf{hyp}^1\rangle$. We can check whether this is the case by measuring the first qubit of a copy of $|\mathsf{lab}\rangle$ in the $\{|e_0\rangle , |e_1\rangle\}$ basis to get a random outcome $x \in \{0,1\}$, and then apply the above test to the reduced state on the last $n-1$ qubits $|\mathsf{hyp}^x\rangle$ by writing it as

$$|\mathsf{hyp}^x\rangle = \frac{1}{\sqrt{2}} |e_{x0}\rangle |\mathsf{hyp}^{x0}\rangle + \frac{1}{\sqrt{2}} |e_{x1}\rangle |\mathsf{hyp}^{x1}\rangle \tag{1}$$

and then applying the same algorithm. This essentially checks if we can "blame" the second qubit instead of the first one for $|\mathsf{lab}\rangle$ being far from $|\mathsf{hyp}\rangle$.

In general, we can select a uniformly random qubit k on which to perform the above check as follows. First, measure the first $k-1$ qubits in the basis given by building up the $|e_x\rangle$'s so the coefficients in the decomposition are always $\frac{1}{\sqrt{2}}$, yielding a random outcome $x \in \{0,1\}^{k-1}$. Then, run our algorithm on the resulting post-measurement state $|\mathsf{lab}^x\rangle$.

[2] We do this only for simplicity of our calculations; we could have stuck with the $\{|0\rangle , |1\rangle\}$ basis at the expense of introducing variable coefficients in the analysis.

[3] It is also possible to have both of these magnitudes equal to $\frac{1}{\sqrt{2}}$, and we will make this choice to simplify our calculations.

In the proof of Lemma 7, we formalize the intuition that for any $|\mathsf{lab}\rangle$, on average each of the n qubits carries at least $\frac{\varepsilon}{n}$ blame. That is,

$$\mathbf{E}_k \mathbf{E}_x \left[\frac{1}{2} \left\| \gamma_{x0} |\mathsf{lab}^{x0}\rangle - \gamma_1 U_x |\mathsf{lab}^{x1}\rangle \right\|^2 \right] \geq \frac{\varepsilon}{n},$$

and so the algorithm rejects with at least $\frac{\varepsilon}{n}$ probability. To argue this formally, we define a potential function $\Phi^k(|\mathsf{hyp}\rangle, |\mathsf{lab}\rangle)$ in Equation (3). It satisfies $\Phi^0 = 1 - \varepsilon$ and $\Phi^k = 1$, so on average $\Phi^k - \Phi^{k-1} \geq \frac{\varepsilon}{n}$, and also

$$\Phi^k - \Phi^{k-1} = \mathbf{E}_x \left[\frac{1}{2} \left\| \langle \mathsf{hyp}^{x_0}| \left(\gamma_{x0} |\mathsf{lab}^{x0}\rangle - \gamma_1 U_x |\mathsf{lab}^{x1}\rangle \right) \right\|^2 \right] \leq \mathbf{E}_x \left[\frac{1}{2} \left\| \gamma_{x0} |\mathsf{lab}^{x0}\rangle - \gamma_1 U_x |\mathsf{lab}^{x1}\rangle \right\|^2 \right],$$

so the layer k algorithm fails with at least this probability.

Comparison with [HPS24]. In our framework, the algorithm from [HPS24] can essentially be viewed as follows: randomly order the qubits and run our algorithm at layer n using the computational basis.[4] That is, check whether each pair of adjacent leaf nodes has the correct ratio of amplitudes, including phase. Their analysis effectively shows that applying the layer n version of our algorithm to a random qubit ordering suffices to certify most states. Our algorithm can be seen as a generalization, where we also compare nodes higher up in the tree and prove rigorously that for *any* target state, some layer must necessarily be to blame.

2 The Algorithm

2.1 Setup

2.1.1 Decision Tree Basis

We begin by defining the notion of a decision tree basis $(\mathbb{C}^2)^{\otimes n}$, which we make use of in our algorithm. Decision tree bases are exactly those orthonormal bases induced by fixing an ordering of qubits, and then measuring them in order, adaptively based on the previous outcomes observed.

Definition 2. Let $\mathcal{T}$ be a depth-n binary tree $\mathcal{T}$ in which each internal node's two children are labeled by orthogonal single-qubit states. For each root-to-leaf path $x \in \{0,1\}^n$, write $|e_x\rangle$ for the n-qubit product state given by the tensor product of the states along the path. Abusing notation, we identify $\mathcal{T}$ with the orthonormal basis $\{|x\rangle : x \text{ in } \{0,1\}^n\}$, and call $\mathcal{T}$ a *decision tree (DT) basis* for $(\mathbb{C}^2)^{\otimes n}$.

We begin by defining a decision tree basis for a quantum state on n qubits, which we will make use of in our algorithm. Decision tree bases are exactly those bases induced by fixing an ordering of qubits, and then measuring them in order, adaptively based on the previous outcomes observed.

Definition 3. Let ρ be the mixed state of a qudit. We will call ρ a *phase state* with respect to basis $\mathcal{B} = \{|x\rangle : x \in [d]\}$ of $\mathbb{C}^d$ if ρ's density matrix in this basis has all diagonal entries equal to $\frac{1}{d}$; in other words, if measuring ρ in basis $\mathcal{B}$ yields the uniform distribution on outcomes. For pure states, this means ρ is of the form $\frac{1}{\sqrt{d}} \sum_x \omega_x |x\rangle$ where $|\omega_x| = 1$ for all $x \in [d]$.

[4] As our algorithm is stated, it uses an adaptive basis to ensure all amplitudes have magnitude $\frac{1}{\sqrt{2}}$, but this assumption is not necessary.

Lemma 4. Let $|\psi^0\rangle$ and $|\psi^1\rangle$ be n-qubit quantum states. There exists a decision tree basis $\{|e_x\rangle\}_{x\in\{0,1\}^n}$ for $(\mathbb{C}^2)^{\otimes n}$ in which they are both phase states.

Proof. By induction, it suffices to show that there is basis $\{|b\rangle, |b^\perp\rangle\}$ for the first qubit such that measuring ρ^i in this basis gives each outcome with probability $1/2$, for $i = 0, 1$. For this, we may as well trace out qubits $2 \dots n$ and assume ρ^0, ρ^1 are 1-qubit mixed states. Now it suffices to choose state $|b\rangle$ so that its Bloch sphere representation is orthogonal to that of ρ^0, ρ^1 (this choice is unique up to sign unless ρ^0, ρ^1 are collinear in the Bloch ball). For such a $|b\rangle$, and its Bloch-antipode $|b^\perp\rangle$, measuring ρ^i with respect to $\{|b\rangle, |b^\perp\rangle\}$ indeed gives each outcome with probability $1/2$, as desired. □

2.1.2 Access Model for $|\mathsf{hyp}\rangle$

A certification algorithm cannot expect to have access to the target state in any arbitrary classical form. For example, it should not rely on having the entire state in the computational basis and performing arbitrary classical pre-processing on it. Instead, we work in a restricted *oracle access model*. Following Huang *et al.* [HPS24], the oracle answers queries of the form $\langle x|\mathsf{hyp}\rangle$ for any computational-basis string $x \in \{0,1\}^n$. We adopt the natural extension of this idea: the algorithm may request amplitudes in *any* product basis.

Definition 5. Given a state $|\psi\rangle$, the access model supports the following type of query: For any operator $\Pi = \Pi_1 \otimes \cdots \otimes \Pi_n$ that is a tensor product of single-qubit projectors in $\mathbb{C}^{2\times 2}$, the query Π returns the value $\langle\psi|\,\Pi\,|\psi\rangle$. Note that it is possible for $\Pi_\ell = \mathrm{Id}$.

Essentially, this access model allows us to query for the probability of any specific outcome when measuring any subset of qubits of $|\psi\rangle$ in an arbitrary product basis. We will show that this access model allows us to adaptively compute a DT basis as in Lemma 4 and implement the corresponding measurements efficiently.

Lemma 6. Given access to $|\psi^0\rangle$ and $|\psi^1\rangle$ via this model, one can implement a measurement in a DT basis in which both $|\psi^0\rangle$ and $|\psi^1\rangle$ are phase states using $O(n)$ time.

Proof. The algorithm will be to initialize $\ell = 0$, $|\psi^0_\ell\rangle = |\psi^0\rangle$, $|\psi^1_\ell\rangle = |\psi^1\rangle$, and a tensor product of projections $\Pi_t = \mathrm{Id}$ that corresponds to the measurement outcomes observed up to the ℓth single-qubit measurement. While $\ell < n$, we compute the reduced states $\rho^0 = \mathrm{Tr}_{[k]\setminus\{\ell+1\}}(|\psi^0_\ell\rangle\langle\psi^0_\ell|)$ and $\rho^1 = \mathrm{Tr}_{[k]\setminus\{\ell+1\}}(|\psi^1_\ell\rangle\langle\psi^1_\ell|)$. This can be done by querying the oracle for the quantities

$$\langle\psi^0|\,\Pi(|b\rangle\langle b|\otimes \mathrm{Id})\Pi_\ell\,|\psi^0\rangle \;\text{ and }\; \langle\psi^1|\,\Pi_\ell(|b\rangle\langle b|\otimes \mathrm{Id})\Pi\,|\psi^1\rangle$$

for $b \in \{0, +, i\}$ and performing a single-qubit quantum state reconstruction algorithm. Here the operator $|b\rangle\langle b|\otimes \mathrm{Id}$ acts nontrivially only on the ℓth qubit.

As in Lemma 4 let $|e_\ell\rangle$ be perpendicular to both ρ^0 and ρ^1 on the Bloch sphere and measure the the ℓth qubit in the basis $|e_\ell\rangle, |e_\ell^\perp\rangle$. Then set $\Pi_{\ell+1} = \Pi_\ell \otimes |b\rangle\langle b| \otimes \mathrm{Id}$, where $|b\rangle \in \{|e_\ell\rangle, |e_\ell^\perp\rangle\}$ was the outcome of this measurement. Then $|\psi^0_{\ell+1}\rangle \propto \Pi_{\ell+1}\,|\psi^0\rangle$ and $|\psi^1_{\ell+1}\rangle \propto \Pi_{\ell+1}\,|\psi^1\rangle$ and increase ℓ by 1.

Repeating for all ℓ gives a measurement outcome in a DT basis satisfying the conclusion of Lemma 4. Computing the ℓth measurement takes constant time, while updating the query also takes constant time, so the overall runtime is $O(n)$. □

2.1.3 Our Notation

We have a pure hypothesis state $|\mathsf{hyp}\rangle$ to which we have access via Definition 5 and a pure lab state $|\mathsf{lab}\rangle$ on which we can perform single-qubit measurements. For $k \in \{0, 1, \ldots, n\}$, write

$$|\mathsf{hyp}\rangle = \sum_{x\in\{0,1\}^k} \frac{1}{2^{k/2}} |e_x\rangle |\mathsf{hyp}^x\rangle, \qquad |\mathsf{lab}\rangle = \sum_{x\in\{0,1\}^k} \alpha_x |e_x\rangle |\mathsf{lab}^x\rangle \text{ [5]} \tag{2}$$

so that the $|e_x\rangle$ forms the DT basis given by implementing the measurement protocol in Lemma 6 for $|\mathsf{hyp}\rangle$. We note that we can also simulate oracle access to $|\mathsf{hyp}^x\rangle$ for any x given oracle access to $|\mathsf{hyp}\rangle$.

2.1.4 Potential Function

Define the potential

$$\Phi^k(|\mathsf{hyp}\rangle, |\mathsf{lab}\rangle) \coloneqq \sum_{x\in\{0,1\}^k} |\alpha_x|^2 \left|\langle \mathsf{hyp}^x | \mathsf{lab}^x\rangle\right|^2 = \mathop{\mathbf{E}}_x \left[\left|\langle \mathsf{hyp}^x | \mathsf{lab}^x\rangle\right|^2\right]. \tag{3}$$

Note that $\Phi^0(|\mathsf{hyp}\rangle, |\mathsf{lab}\rangle) = \left|\langle \mathsf{hyp} | \mathsf{lab}\rangle\right|^2$ and $\Phi^n(|\mathsf{hyp}\rangle, |\mathsf{lab}\rangle) = 1$. Next, define the potential differences

$$\Delta^k(|\mathsf{hyp}\rangle, |\mathsf{lab}\rangle) \coloneqq \Phi^k(|\mathsf{hyp}\rangle, |\mathsf{lab}\rangle) - \Phi^{k-1}(|\mathsf{hyp}\rangle, |\mathsf{lab}\rangle). \tag{4}$$

2.2 The Algorithm and Analysis

Algorithm 1 CERTIFY$(|\mathsf{hyp}\rangle, \rho_{\mathsf{lab}})$

Input: Oracle access to $|\mathsf{hyp}\rangle$, one copy of ρ_{lab}.
Output: ACCEPT or REJECT.

1: **Sample** $k \in [n]$ uniformly at random.
2: **Measure** the first $k-1$ qubits of $|\mathsf{lab}\rangle$ in the decision tree basis $\{|e_x\rangle\}$ to obtain outcome $x \in \{0,1\}^{k-1}$ (efficient due to Lemma 6).
3: Express the reduced state on the last $n-k+1$ qubits as $\left|(e_{x0})_k\right\rangle u^0 + \left|(e_{x1})_k\right\rangle u^1$. **Measure** the last $n-k$ qubits of ρ_{lab} in a DT basis where both u^0 and u^1 are scalar multiples of phase states (efficient due to Lemma 6).
4: **Compute** $|\mathsf{hyp}'\rangle$[6], which we define to be the state of the kth qubit of $|\mathsf{hyp}\rangle$, conditioned on measuring x on the first $k-1$ qubits and y on the last $n-k$ qubits.
5: **Measure** the kth qubit of the reduced state of $|\mathsf{lab}\rangle$ in the basis $\{|\mathsf{hyp}'\rangle, |\mathsf{hyp}'^{\perp}\rangle\}$.
6: **Output** ACCEPT if the outcome is $\left|\mathsf{hyp}'\right\rangle$, else REJECT.

We analyze Algorithm 1 in the case where $\rho_{\mathsf{lab}} = |\mathsf{lab}\rangle\langle\mathsf{lab}|$ is a pure state; we will later show that the mixed state case follows easily.

In the following, we let $|\mathsf{hyp}^{xb}\rangle$ be the reduced given by measuring $|\mathsf{hyp}\rangle$ in the first decision tree basis and getting an x, and then measuring the kth qubit and getting a b. Similarly define $|\mathsf{lab}^{xb}\rangle$, $|\mathsf{hyp}^x\rangle$, and $|\mathsf{lab}^x\rangle$.

[6] This can be done efficiently due to a similar argument as Lemma 6: We can obtain the probabilities for measuring each of $|0\rangle$, $|+\rangle$, and $|i\rangle$ in their corresponding bases on the kth qubits and use this to recover $|\mathsf{hyp}'\rangle$.

Lemma 7. Assume that $|\mathsf{hyp}^x\rangle$ is a phase state with respect to the $n-k+1$-qubit basis $\mathcal{B}\otimes\mathcal{T} \coloneqq \{|b\rangle\,|y\rangle \;:\; |b\rangle \in \mathcal{B}, |y\rangle \in \mathcal{T}\}$, where $\mathcal{T}$ is some $(n-k)$-qubit basis. Then the probability that Algorithm 1 rejects, given the outcome $x \in \{0,1\}^{k-1}$, is at least

$$\mathbf{E}_b\left[\left|\langle \mathsf{hyp}^{xb}|\mathsf{lab}^{xb}\rangle\right|^2\right] - \left|\langle \mathsf{hyp}^{x}|\mathsf{lab}^{x}\rangle\right|^2. \tag{5}$$

The expectation is over measuring $|\mathsf{lab}^x\rangle$ in the $\mathcal{B}$ basis.

Proof. Without loss of generality assume that $\mathcal{B} = \{|0\rangle, |1\rangle\}$, and write

$$|\mathsf{hyp}^x\rangle = |0\rangle\otimes u^0 + |1\rangle\otimes u^1, \qquad |\mathsf{lab}^x\rangle = |0\rangle\otimes v^0 + |1\rangle\otimes v^1. \tag{6}$$

The fact that $|\mathsf{hyp}^x\rangle$ is a phase state in the basis $\mathcal{B}\otimes\mathcal{T}$ means that we can write

$$u^0 = \frac{1}{\sqrt{2^n}}(\omega_1, \omega_2, \ldots, \omega_{2^{n-1}}), \qquad u^1 = \frac{1}{\sqrt{2^n}}(\omega_1\zeta_1, \omega_2\zeta_2, \ldots, \omega_{2^{n-1}}\zeta_{2^{n-1}}) \tag{7}$$

for some phases ω_y and ζ_y. Let $U_\zeta \coloneqq \mathrm{diag}(\zeta_1, \ldots, \zeta_{2^{n-1}})$, so $u^1 = U_\zeta \cdot u^0$, and write $\widetilde{v}^1 \coloneqq U_\zeta^\dagger v^1$ for the vector whose jth component is $\overline{\zeta}_j \cdot v^1_j$. We now claim that

$$\mathbf{Pr}\big[\text{test accepts } |\mathsf{lab}^x\rangle\big] = \left\|\frac{v^0 + \widetilde{v}^1}{\sqrt{2}}\right\|^2. \tag{8}$$

To see this, note that the probability of obtaining y in the first step of the test (measuring in the $\mathcal{T}$ basis) is $p_y \coloneqq |v^0_y|^2 + |v^1_y|^2$. Conditioned on obtaining y we have $|\mathsf{lab}'\rangle = p_y^{-\frac{1}{2}}(v^0_y\,|0\rangle + v^1_y\,|1\rangle)$, and $|\mathsf{hyp}'\rangle = \frac{1}{\sqrt{2}}\omega_y(|0\rangle + \zeta_y\,|1\rangle)$. Then the conditional probability of accepting in the final step of the test is

$$\left|\langle\psi'|\varphi'\rangle\right|^2 = p_y^{-1}\left|\frac{v^0_y}{\sqrt{2}} + \frac{\overline{\zeta}_y\cdot v^1_y}{\sqrt{2}}\right|^2 = p_y^{-1}\left|\frac{v^0_y + \widetilde{v}^1_y}{\sqrt{2}}\right|^2. \tag{9}$$

Summing p_y times the above, over y, yields the claimed Equation (8). Moreover, since $\|v^0\|^2 + \|\widetilde{v}^1\|^2 = \|v^0\|^2 + \|v^1\|^2 = 1$, the parallelogram law implies

$$\mathbf{Pr}\big[\text{test rejects } |\mathsf{lab}^x\rangle\big] = 1 - \mathbf{Pr}\big[\text{test accepts } |\mathsf{lab}^x\rangle\big] = \left\|\frac{v^0 - \widetilde{v}^1}{\sqrt{2}}\right\|^2. \tag{10}$$

We now analyze the fidelity difference on the right-hand side of Equation (5). We have $|\mathsf{lab}^{xb}\rangle = \frac{v^b}{\|v^b\|}$ and $|\mathsf{hyp}^{xb}\rangle = \frac{u^b}{1/\sqrt{2}}$ for $b = 0, 1$. Thus

$$\begin{aligned}
&\mathbf{E}_b\left[\left|\langle \mathsf{hyp}^{xb}|\mathsf{lab}^{xb}\rangle\right|^2\right] - \left|\langle \mathsf{hyp}^{x}|\mathsf{lab}^{x}\rangle\right|^2 && (11)\\
&= \|v^0\|^2\cdot\left|\langle \mathsf{hyp}^{x0}|\mathsf{lab}^{x0}\rangle\right|^2 + \|v_1\|^2\cdot\left|\langle \mathsf{hyp}^{x1}|\mathsf{lab}^{x1}\rangle\right|^2 - \left|\langle \mathsf{hyp}^{x}|\mathsf{lab}^{x}\rangle\right|^2 && (12)\\
&= \left|\langle \mathsf{hyp}^{x0}|\,v^0\right|^2 + \left|\langle \mathsf{hyp}^{x1}|\,v^1\right|^2 - \tfrac{1}{2}\left|\langle \mathsf{hyp}^{x0}|\,v^0 + \langle \mathsf{hyp}^{x1}|\,v^1\right|^2 && (13)\\
&= \tfrac{1}{2}\left|\langle \mathsf{hyp}^{x0}|\,v^0 - \langle \mathsf{hyp}^{x1}|\,v^1\right|^2 = \left|\langle \mathsf{hyp}^{x0}|\left(\frac{v^0 - \widetilde{v}^1}{\sqrt{2}}\right)\right|^2, && (14)
\end{aligned}$$

where in the last line we used the parallelogram law for complex numbers and the fact that $\langle \mathsf{hyp}^{x1}|\,v^1 = \langle \mathsf{hyp}^{x0}|\,U_\zeta^\dagger U_\zeta \widetilde{v}^1 = \langle \mathsf{hyp}^{x0}|\,\widetilde{v}^1$. But now Equation (14) $\le$ Equation (10) is immediate. □

Corollary 8. If $\left|\langle \mathsf{hyp}|\mathsf{lab}\rangle\right|^2 \leq 1-\varepsilon$ then Algorithm 1 rejects with probability at least ε/n.

Proof. For any particular k, the probability that Algorithm 1 rejects given that particular choice of k by Lemma 7 at least

$$\mathop{\mathbf{E}}_{x}\left[\mathbf{E}_b\left[\left|\langle \mathsf{hyp}^{xb}|\mathsf{lab}^{xb}\rangle\right|^2\right]-\left|\langle \mathsf{hyp}^{x}|\mathsf{lab}^{x}\rangle\right|^2\right]=\Delta^k.$$

Averaging over the k while noting that $\sum_k \Delta_k = 1-\Phi^0(|\mathsf{hyp}\rangle, |\mathsf{lab}\rangle) \geq \varepsilon$ yields the result. □

This shows that the layer k algorithm rejects any $|\mathsf{lab}\rangle$ that has large Δ^k. We would also like to show that if $|\mathsf{lab}\rangle$ is close to $|\mathsf{hyp}\rangle$ then it is not rejected w.h.p. For this we bound:

Lemma 9. If $\left|\langle \mathsf{hyp}|\mathsf{lab}\rangle\right|^2 \geq 1-\varepsilon$ then Algorithm 1 rejects with probability at most ε.

Proof. We have that $1-\Phi^k(|\mathsf{hyp}\rangle, |\mathsf{lab}\rangle) \geq 1-\varepsilon$. As in the proof of Lemma 7 we have that for any outcome x observed by measuring the first $k-1$ qubits,

$$\mathbf{E}_b\left[\left|\langle \mathsf{hyp}^{xb}|\mathsf{lab}^{xb}\rangle\right|^2\right]-\left|\langle \mathsf{hyp}^{x}|\mathsf{lab}^{x}\rangle\right|^2 = 1-\left\||\mathsf{hyp}^{x0}\rangle\langle \mathsf{hyp}^{x0}|\left(\frac{v^{x0}-\widetilde{v}^{x1}}{\sqrt{2}}\right)\right\|^2 \geq 1-\left\|\frac{v^0-\widetilde{v}^1}{\sqrt{2}}\right\|^2.$$

Here the v^0 and $\widetilde{v}^1$ are what we defined in the proof of Lemma 7. Averaging over the x, we find that the left-hand side is equal to $\Delta^k \leq \varepsilon$, while the right-hand side is equal to the probability of rejection, given the choice of k. Averaging over k gives the result. □

Combining Corollary 8 and Lemma 9 proves Theorem 1, since we can regard ρ_{lab} as a probability distribution over pure states $|\mathsf{lab}_t\rangle$, and

$$\begin{aligned}\mathbf{Pr}\left[\text{test rejects } \rho_{\mathsf{lab}}\right] &= \mathop{\mathbf{E}}_{t}\left[\mathbf{Pr}\left[\text{test rejects } |\mathsf{lab}_t\rangle\right]\right] \\ &\geq \frac{1}{n}-\frac{1}{n}\mathop{\mathbf{E}}_{t}\left[\langle \mathsf{hyp}|\mathsf{lab}\rangle\langle \mathsf{lab}|\mathsf{hyp}\rangle\right] = \frac{1}{n}-\frac{1}{n}\langle \mathsf{hyp}|\rho_{\mathsf{lab}}|\mathsf{hyp}\rangle.\end{aligned}$$

A similar calculation for the upper bound by Lemma 9 completes the proof. Finally, we prove Main Theorem from Theorem 1.

Proof. Run the one-copy tester of Theorem 1 independently on $O(n\varepsilon^{-1}\ln(1/\delta))$ copies of ρ_{lab}. If $\langle \mathsf{hyp}|\rho_{\mathsf{lab}}|\mathsf{hyp}\rangle \geq 1-\frac{\varepsilon}{2n}$, the probability that each copy rejects is at most $\frac{\varepsilon}{2}$ by Theorem 1. On the other hand, if $\langle \mathsf{hyp}|\rho_{\mathsf{lab}}|\mathsf{hyp}\rangle \geq 1-\varepsilon$, the probability that each copy rejects is at least ε. By a Chernoff bound, $O(n\varepsilon^{-1}\ln(1/\delta))$ samples suffice to distinguish between the two cases. □

Acknowledgments

We thank Mihir Singhal for helpful discussions and Omar Alrabiah for checking calculations. We also thank ChatGPT for assistance. MG and WH are grateful to Angelos Pelecanos for his daily presence in Soda Hall.

References

[AGKE15] Leandro Aolita, Christian Gogolin, Martin Kliesch, and Jens Eisert. Reliable quantum certification of photonic state preparations. *Nature Communications*, 6(1):8498, 2015.

[BOW19] Costin Bădescu, Ryan O'Donnell, and John Wright. Quantum state certification. In *Symposium on Theory of Computing (STOC)*, pages 503–514. ACM, 2019.

[CHW07] Andrew Childs, Aram Harrow, and Paweł Wocjan. Weak Fourier–Schur sampling, the hidden subgroup problem, and the quantum collision problem. In *Symposium on Theoretical Aspects of Computer Science (STACS)*, volume 4393, pages 598–609. Springer, Berlin, 2007.

[FL11] Steven Flammia and Yi-Kai Liu. Direct fidelity estimation from few Pauli measurements. *Physical Review Letters*, 106(23):230501, 2011.

[GKEA18] Marek Gluza, Martin Kliesch, Jens Eisert, and Leandro Aolita. Fidelity witnesses for fermionic quantum simulations. *Physical Review Letters*, 120(19):190501, 2018.

[HM15] Masahito Hayashi and Tomoyuki Morimae. Verifiable measurement-only blind quantum computing with stabilizer testing. *Physical review letters*, 115(22):220502, 2015.

[HMT06] Masahito Hayashi, Keiji Matsumoto, and Yoshiyuki Tsuda. A study of LOCC-detection of a maximally entangled state using hypothesis testing. *Journal of Physics A: Mathematical and General*, 39(46):14427, 2006.

[HPS24] Hsin-Yuan Huang, John Preskill, and Mehdi Soleimanifar. Certifying almost all quantum states with few single-qubit measurements. In *Symposium on Foundations of Computer Science (FOCS)*, pages 1202–1206. IEEE, 2024.

[HT19] Masahito Hayashi and Yuki Takeuchi. Verifying commuting quantum computations via fidelity estimation of weighted graph states. *New Journal of Physics*, 21(9):093060, 2019.

[KR21] Martin Kliesch and Ingo Roth. Theory of quantum system certification. *PRX Quantum*, 2(1):010201, 2021.

[LHS+21] Zihao Li, Yun-Guang Han, Hao-Feng Sun, Jiangwei Shang, and Huangjun Zhu. Verification of phased Dicke states. *Physical Review A*, 103(2):022601, 2021.

[LHZ19] Zihao Li, Yun-Guang Han, and Huangjun Zhu. Efficient verification of bipartite pure states. *Physical Review A*, 100(3):032316, 2019.

[LYS+19] Ye-Chao Liu, Xiao-Dong Yu, Jiangwei Shang, Huangjun Zhu, and Xiangdong Zhang. Efficient verification of Dicke states. *Physical Review Applied*, 12(4):044020, 2019.

[MNS16] Tomoyuki Morimae, Daniel Nagaj, and Norbert Schuch. Quantum proofs can be verified using only single-qubit measurements. *Physical Review A*, 93(2):022326, 2016.

[MTH17] Tomoyuki Morimae, Yuki Takeuchi, and Masahito Hayashi. Verification of hypergraph states. *Physical Review A*, 96(6):062321, 2017.

[OW21] Ryan O'Donnell and John Wright. Quantum spectrum testing. *Communications in Mathematical Physics*, 387(1):1–75, 2021.

[SLP11] Marcus da Silva, Olivier Landon-Cardinal, and David Poulin. Practical characterization of quantum devices without tomography. *Physical Review Letters*, 107(21):210404, 2011.

[TM18] Yuki Takeuchi and Tomoyuki Morimae. Verification of many-qubit states. *Physical Review X*, 8(2):021060, 2018.

[YSG19] Xiao-Dong Yu, Jiangwei Shang, and Otfried Gühne. Optimal verification of general bipartite pure states. *npj Quantum Information*, 5(1):112, 2019.

[ZH19a] Huangjun Zhu and Masahito Hayashi. Efficient verification of hypergraph states. *Physical Review Applied*, 12(5):054047, 2019.

[ZH19b] Huangjun Zhu and Masahito Hayashi. Statistical methods for quantum state verification and fidelity estimation. *Physical Review A*, 99(5):052346, 2019.