Few Single-Qubit Measurements Suffice to Certify Any Quantum State

Meghal Gupta* William He† Ryan O'Donnell‡

July 11, 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 subexponentially 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).

Our algorithm also showcases the power of *adaptive measurements*: within each copy of the lab state, previous measurement outcomes dictate how subsequent qubit measurements are made. We show this adaptivity is necessary, by proving an exponential lower bound on the number of copies needed for any nonadaptive single-qubit measurement algorithm.

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 a main use of state certification is to verify that we can in fact prepare $|\mathsf{hyp}\rangle$, it is almost circular to allow measurement of the POVM $\{|\mathsf{hyp}\rangle\langle\mathsf{hyp}|, \mathrm{Id} - |\mathsf{hyp}\rangle\langle\mathsf{hyp}|\}$. What

*UC Berkeley, meghal@berkeley.edu

†Carnegie Mellon University, wrhe@cs.cmu.edu

‡Carnegie Mellon University, odonnell@cs.cmu.edu. Supported in part by a grant from Google Quantum AI.

we would 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 that use only single-qubit measurements: This would allow for efficient certification even when preparation is more complex and unreliable.

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 $0 < \varepsilon, \delta < 1$, oracle access to a pure state $|\mathsf{hyp}\rangle$ (via the model in Definition 15), 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, together with repetition and a Chernoff bound:

Theorem 1. There exists an algorithm that given oracle access to a pure state $|\mathsf{hyp}\rangle$ via the model in Definition 15 and *one* copy of a mixed state ρ_{lab}, makes only single-qubit measurements to ρ_{lab} and outputs:

- ACCEPT with probability at least $\mathrm{Fid} \coloneqq \langle\mathsf{hyp}|\rho_{\mathsf{lab}}|\mathsf{hyp}\rangle$;
- REJECT with probability at least $\mathrm{Infid}/n \coloneqq (1 - \langle\mathsf{hyp}|\rho_{\mathsf{lab}}|\mathsf{hyp}\rangle)/n$.

Our algorithm also shows the power of *adaptive* measurements. For each copy of ρ_{lab}, how our algorithm measures the next qubit sometimes depends on the outcomes of the previous measurements (though our algorithm is nonadaptive across copies). This is in contrast to the fully nonadaptive algorithm appearing in [HPS24]. The use of adaptivity turns out to be necessary; we show an exponential copy-complexity lower bound against nonadaptive algorithms. Thus, we

[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].

have a natural problem showing that adaptive single-qubit measurements algorithms have an an exponential advantage over nonadaptive ones.

To be precise, we say that an algorithm makes nonadaptive measurements if, for each copy of ρ_{lab} it receives, it measures in a product basis $\mathcal{B}_1 \otimes \cdots \otimes \mathcal{B}_n$ (each $\mathcal{B}_i = \{|b_i\rangle, |b_i^{\perp}\rangle\}$ a 1-qubit basis). We allow the algorithm to act adaptively across copies; that is, the product basis it uses for the tth copy may depend on measurement outcomes from the preceding copies. Then in Section 3 we prove:

Theorem 2. For $n \geq 1$, there exists an n-qubit state $|\mathsf{hyp}\rangle$ such that the following holds: Any certification algorithm making nonadaptive measurements that succeeds with probability at least $1/2 + 2^{-c_1 n}$ in distinguishing $\rho_{\mathsf{lab}} = |\mathsf{hyp}\rangle\langle\mathsf{hyp}|$ from $\langle\mathsf{hyp}|\rho_{\mathsf{lab}}|\mathsf{hyp}\rangle \leq 2^{-c_2 n}$ must use at least $2^{c_3 n}$ copies of ρ_{lab}. (Here $c_1, c_2, c_3 > 0$ are universal constants.)

Future directions. Several natural questions remain open for future work. We state two here:

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 $\langle\mathsf{hyp}|\rho_{\mathsf{lab}}|\mathsf{hyp}\rangle \geq 1 - \Omega(\varepsilon/n)$, rather than $1 - \Omega(\varepsilon)$. Can this dependence on n be improved or even eliminated? For instance, is it possible to design a certification algorithm with similar complexity that distinguishes between $\langle\mathsf{hyp}|\rho_{\mathsf{lab}}|\mathsf{hyp}\rangle \geq 1 - \varepsilon/2$ and $\langle\mathsf{hyp}|\rho_{\mathsf{lab}}|\mathsf{hyp}\rangle \leq 1 - \varepsilon$?

2 The Algorithm

In this section we provide an algorithm that proves Theorem 1.

2.1 DT Bases

At a high level, our algorithm will pick a random $k \in [n]$, measure the first $k-1$ qubits in the computational basis, then measure the last $n-k$ qubits in some carefully constructed basis, and finally measure the kth qubit. We begin with some definitions and facts that will help us understand the carefully constructed basis in which the last $n-k$ qubits are measured.

Definition 3. Let $\mathcal{T}$ be a depth-n binary tree $\mathcal{T}$ in which each internal node's two outgoing edges are labeled by orthogonal single-qubit states. By a slight abuse of notation, we identify $\mathcal{T}$ with the orthonormal basis $\{|\ell\rangle : \ell \text{ a leaf in } \mathcal{T}\}$, and call $\mathcal{T}$ a *decision tree (DT) basis* for $(\mathbb{C}^2)^{\otimes n}$.

Remark 4. Note that given an n-qubit DT basis $\mathcal{T}$, one can measure an n-qubit state in this basis by using adaptive single-qubit measurements. Indeed, a deterministic adaptive algorithm that measures qubits in the order $1 \ldots n$ is *equivalent* to a DT basis. We also comment that although $\mathcal{T}$ is a *basis of product states*, this is a more general object than a *product basis*, the latter being what a nonadaptive algorithm uses to measure each copy.

Definition 5. Recall that qudit $|\varphi\rangle \in \mathbb{C}^d$ is said to be a *phase state* in basis $\mathcal{L} = \{|1\rangle, \ldots, |d\rangle\}$ if it can be written as

$$|\varphi\rangle = \frac{1}{\sqrt{d}} \sum_{\ell=1}^{d} \omega_\ell |\ell\rangle \qquad \text{for some phases } \omega_\ell. \tag{1}$$

In other words, measuring in basis $\mathcal{L}$ yields each outcome with equal probability.

Lemma 6. Let ρ^0 and ρ^1 be single-qubit *mixed* states. Then there exists a 1-qubit basis $\mathcal{B} = \{|b\rangle, |b^\perp\rangle\}$ such that for $i = 0, 1$, measuring ρ^i in basis $\mathcal{B}$ yields each outcome $|b\rangle$ and $|b^\perp\rangle$ with probability $\frac{1}{2}$.

Proof. It suffices to choose qubit $|b\rangle$ 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 $\frac{1}{2}$. □

Corollary 7. Let $|\varphi^0\rangle$ and $|\varphi^1\rangle$ be m-qubit quantum states. Then there exists a decision tree basis $\mathcal{T}$ for $(\mathbb{C}^2)^{\otimes n}$ in which they are both phase states.[2]

Proof. For $k = 1 \dots m$, we inductively build the labels on the edges at depth at most k so that for both $i = 0, 1$ and all depth-k nodes w, the probability of obtaining outcome w when measuring $|\varphi^i\rangle$ with the tree (so far) is 2^{-k}. For the base case of $k = 1$, we apply Lemma 6; the resulting 1-qubit basis $\mathcal{B} = \{|b\rangle, |b^\perp\rangle\}$ serves as the edge labels out from the root of $\mathcal{T}$. Now to extend from k to $k+1$ we need, for each node w at depth k, a 1-qubit basis $\mathcal{B}_w = \{|b_w\rangle, |b_w^\perp\rangle\}$ such that measuring each of the reduced states $|(\varphi^0)^w\rangle, |(\varphi^1)^w\rangle$ in basis $\mathcal{B}_w$ yields each outcome with probability $\frac{1}{2}$. This may be obtained by applying Lemma 6 to $|(\varphi^0)^w\rangle, |(\varphi^1)^w\rangle$. □

2.2 Our Algorithm and Its Key Subtest

Let $|\mathsf{hyp}\rangle$ be the n-qubit state to be certified. In our proof of Theorem 1, we may assume without loss of generality that the lab state is a pure one, $|\mathsf{lab}\rangle$. This is because we can regard ρ_{lab} as a probability distribution over pure states, since our algorithm may only perform measurements to a single copy of lab. (This equivalence can be shown by linearity of expectation.) Also, for expositional simplicity, in this section we regard $|\mathsf{hyp}\rangle$ as completely "known"; we will not be concerned with the complexity of interacting with $|\mathsf{hyp}\rangle$. The straightforward details of the access model we actually assume, and the running time, are deferred to Section 2.4.

We will use a collection of DT bases $\mathcal{T}_x$, for $x \in \{0,1\}^{\leq n}$. For all $1 \leq k \leq n$ and all binary strings $x \in \{0,1\}^{k-1}$, let $|\mathsf{hyp}^x\rangle$ and $|\mathsf{lab}^x\rangle$ be the reduced states of $|\mathsf{hyp}\rangle$ and $|\mathsf{lab}\rangle$, respectively, after measuring the first $k-1$ qubits of these states in the computational basis and observing x. For all $x \in \{0,1\}^{\leq n}$, define the DT basis $\mathcal{T}_x$ so that in this basis, both $|\mathsf{hyp}^{x0}\rangle$ and $|\mathsf{hyp}^{x1}\rangle$ are phase states; we know this DT basis exists by Corollary 7.

We may now state our algorithm:

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

Input: Knowledge of $|\mathsf{hyp}\rangle$ and DT bases $\mathcal{T}_x$; and, one copy of an unknown state $|\mathsf{lab}\rangle$.
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 computational basis, obtaining $x \in \{0,1\}^{k-1}$.
3: **Measure** the last $n-k$ qubits of $|\mathsf{lab}^x\rangle$ in the basis $\mathcal{T}_x$, obtaining ℓ.
4: Let $|\mathsf{lab}'\rangle$ be the resulting 1-qubit state; let $|\mathsf{hyp}'\rangle$ denote $|\mathsf{hyp}\rangle$ conditioned on outcomes x, ℓ. **Measure** $|\mathsf{lab}'\rangle$ in a basis containing $|\mathsf{hyp}'\rangle$, and **Output** ACCEPT iff the outcome is $|\mathsf{hyp}'\rangle$.

Definition 8. We refer to Steps 3–4 of our algorithm as the *subtest* performed on the $(n-k)$-qubit states $|\mathsf{hyp}^x\rangle$ and $|\mathsf{lab}^x\rangle$, with DT basis $\mathcal{T}_x$. We will also use the notation $\text{SUBTEST}_{\mathcal{T}_x}(|\mathsf{lab}^x\rangle : |\mathsf{hyp}^x\rangle)$.

[2] This corollary can also be obtained from the algorithm in [ZZJ20, Sec. III], by taking its matrix $\tilde{M}$ to be $(1+\mathrm{i})|\varphi^0\rangle\langle\varphi^0| - |\varphi^1\rangle\langle\varphi^1| - \mathrm{i} \cdot \mathrm{Id}/2^n$.

The key to analyzing the CERTIFY algorithm is to compare the subtest acceptance probability to the following quantity:

Definition 9. For $(n-k+1)$-qubit states $|\mathsf{lab}^x\rangle, |\mathsf{hyp}^x\rangle$ as in CERTIFY, we define their *fidelity gap* to be

$$\Delta(|\mathsf{lab}^x\rangle : |\mathsf{hyp}^x\rangle) \coloneqq \mathop{\mathbf{E}}_{b}\left[\left|\langle \mathsf{hyp}^{xb}|\mathsf{lab}^{xb}\rangle\right|^2\right] - \left|\langle \mathsf{hyp}^x|\mathsf{lab}^x\rangle\right|^2. \tag{2}$$

Here the expectation is over the random outcome $b \in \{0,1\}$ obtained when measuring the first qubit of $|\mathsf{lab}^x\rangle$ in the computational basis.

Remark 10. $\Delta(|\mathsf{lab}^x\rangle : |\mathsf{hyp}^x\rangle) \geq 0$ always. This follows from the data processing inequality for fidelity, and is also a direct consequence of the Cauchy–Schwarz inequality.

The central analysis in our proof will be the following:

Theorem 11. With $\mathcal{T}_x$ being a (DT) basis in which $|\mathsf{hyp}^{x0}\rangle$ and $|\mathsf{lab}^{x1}\rangle$ are both phase states, the following holds:

$$\mathbf{Pr}[\textsc{SubTest}_{\mathcal{T}_x}(|\mathsf{lab}^x\rangle : |\mathsf{hyp}^x\rangle) \text{ rejects}] \geq \Delta(|\mathsf{lab}^x\rangle : |\mathsf{hyp}^x\rangle), \tag{3}$$

$$\mathbf{Pr}[\textsc{SubTest}_{\mathcal{T}_x}(|\mathsf{lab}^x\rangle : |\mathsf{hyp}^x\rangle) \text{ accepts}] \geq \left|\langle \mathsf{hyp}^x|\mathsf{lab}^x\rangle\right|^2. \tag{4}$$

We defer the proof of Theorem 11 to Section 2.3 and conclude assuming it holds. For now, we use Theorem 11 to complete the analysis of our algorithm CERTIFY.

Proposition 12. It holds that

$$\mathop{\mathbf{E}}_{x}\left[\Delta(|\mathsf{lab}^x\rangle : |\mathsf{hyp}^x\rangle)\right] = \frac{1}{n}\cdot\left(1 - \left|\langle \mathsf{hyp}|\mathsf{lab}\rangle\right|^2\right)$$

Here, x is sampled by performing steps 1–2 of our algorithm. In other words, x is sampled by first choosing a uniformly random $k \in [n]$ and then measuring the first $k-1$ qubits of $|\mathsf{lab}\rangle$ to obtain x.

Proof. For $0 \leq k \leq n$, define the quantity

$$\Phi^k \coloneqq \mathop{\mathbf{E}}_{x}\left[\left|\langle \mathsf{hyp}^x|\mathsf{lab}^x\rangle\right|^2\right]. \tag{5}$$

where x is sampled by measuring the first k qubits of $|\mathsf{lab}\rangle$. Then,

$$\mathop{\mathbf{E}}_{x}\left[\Delta(|\mathsf{lab}^x\rangle : |\mathsf{hyp}^x\rangle)\right] = \mathop{\mathbf{E}}_{k\in[n]}\left[\mathop{\mathbf{E}}_{\substack{x,\\|x|=k-1}}\mathop{\mathbf{E}}_{b}\left[\left|\langle \mathsf{hyp}^{xb}|\mathsf{lab}^{xb}\rangle\right|^2\right] - \mathop{\mathbf{E}}_{\substack{x,\\|x|=k-1}}\left[\left|\langle \mathsf{hyp}^x|\mathsf{lab}^x\rangle\right|^2.\right]\right] \tag{6}$$

$$= \mathop{\mathbf{E}}_{k\in[n]}\left[\mathop{\mathbf{E}}_{\substack{x,\\|x|=k}}\left[\left|\langle \mathsf{hyp}^{xb}|\mathsf{lab}^{xb}\rangle\right|^2\right] - \mathop{\mathbf{E}}_{\substack{x,\\|x|=k-1}}\left[\left|\langle \mathsf{hyp}^x|\mathsf{lab}^x\rangle\right|^2.\right]\right] \tag{7}$$

$$= \mathop{\mathbf{E}}_{k\in[n]}\left[\Phi^k - \Phi^{k-1}\right] \tag{8}$$

$$= \frac{1}{n}\cdot(\Phi^n - \Phi^0) = \frac{1}{n}\cdot\left(1 - \left|\langle \mathsf{hyp}|\mathsf{lab}\rangle\right|^2\right), \tag{9}$$

where the last line follows by a telescoping sum. □

It thus follows that

$$\mathbf{Pr}[\textsc{Certify} \text{ rejects}] = \mathop{\mathbf{E}}_{x} \mathbf{Pr}[\textsc{SubTest}_{\mathcal{T}_x}(|\mathsf{lab}^x\rangle : |\mathsf{hyp}^x\rangle) \text{ rejects}] \tag{10}$$

$$\geq \mathop{\mathbf{E}}_{x} [\Delta(|\mathsf{lab}^x\rangle : |\mathsf{hyp}^x\rangle)] \tag{11}$$

$$= \frac{1}{n} \cdot \left(1 - \left|\langle \mathsf{hyp}|\mathsf{lab}\rangle\right|^2\right) \tag{12}$$

as claimed. As for the acceptance probability,

$$\mathbf{Pr}[\textsc{Certify} \text{ accepts}] = \mathop{\mathbf{E}}_{x} \mathbf{Pr}[\textsc{SubTest}_{\mathcal{T}_x}(|\mathsf{lab}^x\rangle : |\mathsf{hyp}^x\rangle) \text{ accepts}] \tag{13}$$

$$\geq \mathop{\mathbf{E}}_{x} \left[\left|\langle \mathsf{hyp}^x|\mathsf{lab}^x\rangle\right|^2\right] \tag{14}$$

$$\geq \left|\langle \mathsf{hyp}|\mathsf{lab}\rangle\right|^2, \tag{15}$$

where the last inequality follows by Remark 10. This concludes the proof of Theorem 1.

2.3 Analysis of the Subtest (Proof of Theorem 11)

We will analyze $\textsc{SubTest}_{\mathcal{T}}(|V\rangle : |U\rangle)$ for any two m qubit states $|V\rangle$ and $|U\rangle$ and any $m-1$ qubit orthonormal basis $\mathcal{L}$ in which $|U^0\rangle$ and $|U^1\rangle$ are both phase states. (Here, $|U^b\rangle$ denotes the reduced state if one were to measure the first qubit of $|U\rangle$ and observe b.) We denote the basis vectors of $\mathcal{L}$ by $|\ell\rangle$, where $\ell \in [2^{m-1}]$. Write

$$|U\rangle = |0\rangle \otimes u^0 + |1\rangle \otimes u^1, \qquad |V\rangle = |0\rangle \otimes v^0 + |1\rangle \otimes v^1. \tag{16}$$

Since both $|U^0\rangle$ and $|U^1\rangle$ are phase states in the basis $\mathcal{L}$, there is a unitary D that is diagonal in $\mathcal{L}$ such that $|U^1\rangle = D|U^0\rangle$. Define $\widetilde{v}^1 := D^\dagger v^1$.

Proposition 13. It holds that

$$\mathbf{Pr}[\textsc{SubTest} \text{ accepts}] = \left\|a^0 v^0 + a^1 \widetilde{v}^1\right\|^2. \tag{17}$$

Proof. Write $v^0 = \sum_\ell v^0_\ell |\ell\rangle$ and similarly decompose v^1 and $\widetilde{v}^1$. Denote the first qubit of $|V\rangle$ conditioned on observing $|\ell\rangle$ by $|V_\ell\rangle$, and the first qubit of $|U\rangle$ conditioned on observing $|\ell\rangle$ by $|U_\ell\rangle := a^0|0\rangle + a^1\zeta_\ell|1\rangle$, where ζ_ℓ denotes the diagonal entry of D corresponding to the basis vector $|\ell\rangle$. Then, the probability of the subtest accepting is the expected fidelity of $|U_\ell\rangle$ and $|V_\ell\rangle$ upon measuring $|V\rangle$:

$$\mathop{\mathbf{E}}_{\ell} \left|\langle U_\ell|V_\ell\rangle\right|^2 = \sum_\ell \left|\langle U_\ell|(v^0_\ell|0\rangle + v^1_\ell|1\rangle)\right|^2 = \sum_\ell \left|a^0 v^0_\ell + a^1\overline{\zeta_\ell} v^1_\ell|1\rangle)\right|^2 = \sum_\ell \left|a^0 v^0_\ell + a^1 \widetilde{v}^1_\ell|1\rangle)\right|^2,$$

where the last equality uses that $\widetilde{v}^1_\ell = \overline{\zeta_\ell} v^1_\ell$. Using the Pythagorean theorem now yields the claimed Equation (17). □

We will relate this to the rejection probability with the following fact:

Fact 14. Given vectors $w^0, w^1 \in \mathbb{C}^m$ and real numbers $c^0, c^1 \in \mathbb{R}$ such that $(c^0)^2 + (c^1)^2$, it holds that

$$\left\|c^0 w^0 + c^1 w^1\right\|^2 + \left\|c^1 w^0 - c^0 w^1\right\|^2 = \|w^0\|^2 + \|w^1\|^2. \tag{18}$$

This follows easily by expanding the left-hand side and seeing that the cross-terms cancel.

Now, plugging in $w^0 = v^0$, $w^1 = \widetilde{v}^1$, $c^0 = a^0$ and $c^1 = a^1$ into Fact 14, we see that

$$\mathbf{Pr}[\textsc{SubTest} \text{ outputs } \textsc{Rejects}] = 1 - \mathbf{Pr}[\textsc{SubTest} \text{ outputs } \textsc{Accept}] = \left\| a^1 v^0 - a^0 \widetilde{v}^1 \right\|^2. \quad (19)$$

We now relate these quantities to fidelities. Note that we have $|V^b\rangle = \frac{v^b}{\|v^b\|}$ and $|U^b\rangle = \frac{u^b}{a^b}$ for $b = 0, 1$. Thus

$$\left|\langle U|V\rangle\right|^2 = \left|a^0 \cdot \langle U^0|v^0 + a^1 \cdot \langle U^1|v^1\right|^2 = \left|a^0 \cdot \langle U^0|v^0 + a^1 \cdot \langle U^0|\widetilde{v}^1\right|^2 \quad (20)$$

$$= \left|\langle U^0| \left(a^0 v^0 + a^1 \widetilde{v}^1\right)\right|^2 \leq \left\|a^0 v^0 + a^1 \widetilde{v}^1\right\|^2, \quad (21)$$

where we used $\langle U^1|v^1 = \langle U^0|D^\dagger D\widetilde{v}^1 = \langle U^0|\widetilde{v}^1$. In combination with Equation (17), this shows the subtest acceptance probability is at least the fidelity $\left|\langle U|V\rangle\right|^2$, confirming Equation (4). On the other hand,

$$\Delta(|V\rangle : |U\rangle) = \|v^0\|^2 \cdot \left|\langle U^0|V^0\rangle\right|^2 + \|v_1\|^2 \cdot \left|\langle U^1|V^1\rangle\right|^2 - \left|\langle U|V\rangle\right|^2 \quad (22)$$

$$= \left|\langle U^0|v^0\right|^2 + \left|\langle U^1|v^1\right|^2 - \left|a^0 \cdot \langle U^0|v^0 + a^1 \cdot \langle U^1|v^1\right|^2 \quad (23)$$

$$= \left|a^1 \cdot \langle U^0|v^0 - a^0 \cdot \langle U^1|v^1\right|^2 \quad (24)$$

$$= \left|\langle U^0| \left(a^1 v^0 - a^0 \widetilde{v}^1\right)\right|^2 \leq \left\|a^1 v^0 - a^0 \widetilde{v}^1\right\|^2. \quad (25)$$

In going to the second line we used the expression for $\left|\langle U|V\rangle\right|^2$ from Equation (21). In going to the third line we used Fact 14 with $w^b = |U^b\rangle\langle V^0|v^b$ and $c^b = a^b$ for $b \in \{0, 1\}$. In going to the fourth line we used $\langle U^1|v^1 = \langle U^0|\widetilde{v}^1$ again. In combination with Equation (19), this shows the subtest rejection probability is at least $\Delta(|V\rangle : |U\rangle)$, confirming Equation (3).

2.4 Access Model and Computational Efficiency

We now clarify the access model to $|\mathsf{hyp}\rangle$ that our algorithm works under, and analyze the running time in this access model. Essentially, we show that Algorithm 1 does not require computation of all the $\mathcal{T}_x$'s; rather, computation of a suitable $\mathcal{T}_x$ can be done on the fly.

It is not reasonable to give the certification algorithm a classical description of $|\mathsf{hyp}\rangle$, as this may be exponentially large; and indeed, our algorithm does not require this. Instead, we work in a reasonable *oracle access model*, similar to the one in Huang et al. [HPS24]. In that work, it is assumed that the oracle provides the value of $\langle x|\mathsf{hyp}\rangle$ for any queried computational-basis string $x \in \{0, 1\}^n$. Here, we adopt a slight natural extension of this model: the algorithm may request amplitudes in *any* product basis.

Definition 15. We consider oracle access to a state $|\psi\rangle$ supporting 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 on $\mathbb{C}^2$, the querying with Π returns the value $\langle\psi|\Pi|\psi\rangle$. Note that it is possible for individual tensor factors to be $\Pi_k = \mathrm{Id}$.

Essentially, this access model allows us to query for the probability of any specific outcome when measuring any subset of qubits of $|\mathsf{hyp}\rangle$ in an arbitrary product basis. We will show that this access model allows us to adaptively compute a DT basis as in Corollary 7 and implement the corresponding measurements efficiently.

Lemma 16. Given access to $|\psi^0\rangle$ and $|\psi^1\rangle$ via this model, we can implement measuring in the DT basis defined in Corollary 7 (making $|\psi^0\rangle$ and $|\psi^1\rangle$ phase states), using $O(n)$ time and single-qubit measurements.

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

$$\langle\psi^0|\Pi|\psi^0\rangle \text{ and } \langle\psi^1|\Pi|\psi^1\rangle, \text{ where } \Pi = \Pi_t \otimes |b\rangle\langle b| \otimes \mathrm{Id}^{\otimes(n-t-1)}.$$

for $b \in \{0, +, \mathrm{i}\}$ and performing a single-qubit quantum state reconstruction algorithm.

As in Corollary 7, let $|e_t\rangle$ be perpendicular to both ρ^0 and ρ^1 on the Bloch sphere and measure the the tth qubit in the basis $|e_t\rangle, |e_t^\perp\rangle$. Then set $\Pi_{t+1} = \Pi_t \otimes |b\rangle\langle b| \otimes \mathrm{Id}$, where $|b\rangle \in \{|e_t\rangle, |e_t^\perp\rangle\}$ was the outcome of this measurement. Then $|\psi_{t+1}^0\rangle \propto \Pi_{t+1}|\psi^0\rangle$ and $|\psi_{t+1}^1\rangle \propto \Pi_{t+1}|\psi^1\rangle$ and we increase t by 1. Repeating for all t gives a measurement outcome in a DT basis satisfying the conclusion of Corollary 7. Computing the tth measurement and updating the query take $O(1)$ time, so the overall runtime is $O(n)$. □

Given Lemma 16, we see that Algorithm 1 can be implemented in time $O(n)$ under the access model of Definition 15. For measurement in the decision tree basis $\mathcal{T}_x$ (where x is the outcome of measuring the first $k-1$ qubits), we use Lemma 16 with $|\psi^0\rangle = |\mathsf{hyp}^{x0}\rangle$ and $|\psi^1\rangle = |\mathsf{hyp}^{x1}\rangle$.

3 Lower Bound

A simple geometric fact is at heart of our lower bound proof:

Claim 17. There exist single-qubit states $|\chi_0\rangle, |\chi_1\rangle, |\chi_2\rangle, |\chi_3\rangle$ such that the following holds. For all 1-qubit bases $\{|\varphi\rangle, |\varphi^\perp\rangle\}$, there exists $b \in \{1, 2, 3\}$

$$\left|\langle\varphi|\chi_0\rangle\langle\chi_b|\varphi\rangle\right| + \left|\langle\varphi^\perp|\chi_0\rangle\langle\chi_b|\varphi^\perp\rangle\right| \tag{26}$$

for at least one of $b \in \{1, 2, 3\}$.

Proof. We let these four vectors form, say a regular tetrahedron on the Bloch sphere as in the SIC-POVM. □

3.1 The Hard-to-Certify State

Definition 18. For $C \coloneqq (c^1 \dots c^N) \in \{0, 1, 2, 3\}^n$, define the vector

$$v_C \coloneqq \frac{1}{\sqrt{N}} \sum_{t\in[N]} |\chi_{c_1^t}\rangle \otimes \cdots \otimes |\chi_{c_n^t}\rangle$$

Define $|\psi_C\rangle$ to be the quantum state in the direction of v_C, and let $|\psi_{c^t}\rangle \coloneqq |\chi_{c_1^t}\rangle \otimes \cdots \otimes |\chi_{c_n^t}\rangle$.

Lemma 19. Let $N = \lfloor 2^{10^{-10}n} \rfloor$ and choose $C \coloneqq (c^1 \dots c^N) \in \{0, 1, 2, 3\}^n$ i.i.d. With probability at least 0.9,

$$1 - 2^{-0.1n} \le \|v_C\|^2 \le 1 + 2^{-0.1n}.$$

Proof. Standard coding theory. □

Therefore, v_C is extremely close to being a quantum state $|\psi_C\rangle$. In the next section, we will show that it is also likely that $|\psi_C\rangle\langle\psi_C|$ is indistinguishable from the mixed state

$$\rho_C := \frac{1}{N}\sum_s |\psi_{c^s}\rangle\langle\psi_{c^s}|.$$

3.2 The cross term operators

We will show that the advantage of distinguishing between $|\psi_C\rangle\langle\psi_C|$ and the mixed state ρ_C is related to sum of the absolute values on the diagonal of the operator $\frac{1}{N}\sum_{s\neq t}|\psi_{c^s}\rangle\langle\psi_{c^t}|$, maximized over the set of product bases for $(\mathbb{C}^2)^{\otimes n}$. More formally we have:

Lemma 20. Let $|\varphi_x\rangle$ with $x \in \{0,1\}^n$ form an orthonormal basis for $(\mathbb{C}^2)^{\otimes n}$. Suppose that C of size $N = 2^{10^{-10}n}$ satisfies the normalization condition of Lemma 19. Then for large enough n,

$$d_{\mathrm{TV}}(\mathcal{D}_1, \mathcal{D}_2) \leq \frac{1}{N}\sum_x \left|\sum_{s\neq t}\langle\varphi_x|\psi_{c^s}\rangle\langle\psi_{c^t}|\varphi_x\rangle\right| + 2^{-0.001n}.$$

Proof. We directly compute

$$2d_{\mathrm{TV}}(\mathcal{D}_1, \mathcal{D}_2) = \sum_x \left|\langle\varphi_x|\psi_C\rangle\langle\psi_C|\varphi_x\rangle - \langle\varphi_x|\rho_C|\varphi_x\rangle\right| = \sum_x \left|\langle\varphi_x|(|\psi_C\rangle\langle\psi_C| - \rho_C)|\varphi_x\rangle\right|.$$

By Lemma 19, we can approximate the matrix in the middle up to spectral norm:

$$|\psi_C\rangle\langle\psi_C| - \rho_C \underset{N/2^{0.001n}}{\approx} v_C v_C^\dagger - \rho_C = \frac{1}{N}\sum_{s,t}|\psi_{c^s}\rangle\langle\psi_{c^t}| - \frac{1}{N}\sum_s |\psi_{c^s}\rangle\langle\psi_{c^s}| = \frac{1}{N}\sum_{s\neq t}|\psi_{c^s}\rangle\langle\psi_{c^t}|.$$

Using the bound on N we conclude the result when n is large enough. □

Finally, to show that indeed a random C will give a hard to distinguish state, we show the following:

Lemma 21. Let $C := (c^1 \dots c^N) \in \{0,1,2,3\}^n$ i.i.d. where $N := \lfloor 2^{10^{-10}n} \rfloor$. Then if n is large enough, with probability at least 0.9 we have for all product bases $|\varphi_x\rangle = |\varphi^1_{x_1}\rangle \otimes \cdots \otimes |\varphi^n_{x_n}\rangle$ with $x \in \{0,1\}^n$ that

$$\sum_{x\in\{0,1\}^n}\left|\sum_{s\neq t\in[N]}\langle\varphi_x|\psi_{c^s}\rangle\langle\psi_{c^t}|\varphi_x\rangle\right| \leq 5.$$

Proof. Since the $|\varphi_x\rangle$ form a product basis, we can use the following expansion:

$$\begin{aligned}
&\sum_{x\in\{0,1\}^n}\left|\sum_{s\neq t}\langle\varphi_x|\psi_{c^s}\rangle\langle\psi_{c^t}|\varphi_x\rangle\right| \leq \sum_{x\in\{0,1\}^n}\sum_{s\neq t}\left|\langle\varphi_x|\psi_{c^s}\rangle\langle\psi_{c^t}|\varphi_x\rangle\right| \\
&\leq \sum_{s\neq t}\sum_{x\in\{0,1\}^n}\prod_i\left|\langle\varphi^i_{x_i}|\chi_{c^s_i}\rangle\langle\chi_{c^t_i}|\varphi^i_{x_i}\rangle\right| = \sum_{s\neq t}\prod_i\left(\left|\langle\varphi^i_0|\chi_{c^s_i}\rangle\langle\chi_{c^t_i}|\varphi^i_0\rangle\right| + \left|\langle\varphi^i_1|\chi_{c^s_i}\rangle\langle\chi_{c^t_i}|\varphi^i_1\rangle\right|\right).
\end{aligned}$$

Notice that the term inside the right-hand side expression is always at most 1 and sometimes less than 1. Our goal will be to show that or all product bases φ, for most pairs (s,t), the product will be close to 0.

For any state one qubit basis φ', denote by $b(\varphi')$ the element in $\{1,2,3\}$ such that the inequality in Claim 17 holds (any such b if there are multiple). Say a pair (s,t), is *bad* for a product basis φ if for at least $10^{-5}n$ indices $i \in [n]$, it holds that $\{c_i^s, c_i^t\} = \{0, b(\varphi^i)\}$. Note that if the pair (s,t) is bad, then

$$\prod_i \left(\left| \langle \varphi_0^i | \chi_{c_i^s} \rangle \langle \chi_{c_i^t} | \varphi_0^i \rangle \right| + \left| \langle \varphi_1^i | \chi_{c_i^s} \rangle \langle \chi_{c_i^t} | \varphi_1^i \rangle \right| \right) \leq 2^{-10^{-6}n}$$

Consider any quintuple of distinct pairs whose elements are in $[N]$ denoted by $\{s_1,t_1\} \ldots \{s_5,t_5\}$. We will show that with probability at least $2^{-10^{-5}n}$, at least one pair is bad.

Once we have shown this, taking a union bound over all of the at most N^{10} quintuples of pairs, the probability that in every quintuple, at least one pair is bad is at least

$$1 - 2^{-10^{-5}n} \cdot N^{10} \geq 1 - 2^{-10^{-6}n}.$$

When this event holds, at most four pairs (s,t) are not bad and so

$$\sum_{s \neq t} \prod_i \left(\left| \langle \varphi_0^i | \chi_{c_i^s} \rangle \langle \chi_{c_i^t} | \varphi_0^i \rangle \right| + \left| \langle \varphi_1^i | \chi_{c_i^s} \rangle \langle \chi_{c_i^t} | \varphi_1^i \rangle \right| \right) \leq 4 + N^2 \cdot 2^{-10^{-7}n} \leq 5.$$

as desired.

Thus, it suffices to show that with probability at least $2^{-10^{-5}n}$, at least one pair is bad. The graph on $[N]$ that this pairs form either has a vertex of degree 3 or consists of disjoint cycles and edges. This means that for a fixed index $i \in [n]$, there is a labeling $(x_{s_1}, x_{t_1}, \ldots, x_{s_5}, x_{t_5}) \in \{0,1,2,3\}^{10}$ such that if $c_i^{s_1} = x_{s_1}, \ldots, c_i^{t_5} = x_{t_5}$ then

$$\{\{c_i^{s_1}, c_i^{t_1}\}, \ldots, \{c_i^{s_5}, c_i^{s_5}\}\} = \{\{0,1\},\{0,2\},\{0,3\}\}$$

If this occurs, then for any choice of φ^i, at least one pair $\{s_k,t_k\}$ will satisfy $\{c_i^{s_k}, c_i^{t_k}\} = \{0, b(\varphi^i)\}$. Moreover, the probability of this labeling occurring among the three chosen pairs is at least 4^{-6}.

Now let $w(\{s_1,t_1\}, \ldots \{s_5,t_5\})$ be the number of indices i on which this happened. By a Chernoff bound, we have

$$\mathbf{Pr}\left[w(\{s_1,t_1\}, \ldots \{s_5,t_5\}) \leq 4^{-6}n \right] \leq 2^{-10^{-5}n}.$$

When this happens, at least one pair satisfies $\{c_i^{s_k}, c_i^{t_k}\} = \{0, b(\varphi^i)\}$, and so there must be some pair $\{s_k,t_k\}$ where the condition holds for at least $4^{-6}n/5 > 10^{-5}n$ indices. Thus, at least one of the five pairs is bad. □

3.3 The Lower Bound

We complete this section by proving our lower bound:

Proof of Theorem 2. Let C be the collection of size $N = 2^{10^{-10}n}$ which exists by Lemma 21. Any nonadaptive algorithm is one that measures a given state in a product basis and makes decisions based on these measurement outcomes. By Lemmas 20 and 21, the states $|\psi_C\rangle\langle\psi_C|$ and ρ_C yield outcome distributions that have TV distance $\leq 2^{-\Omega(n)}$ in any product basis. By a standard coupling argument, this shows that if $\mathfrak{D}_1$ and $\mathfrak{D}_2$ are the distributions corresponding to measuring $2^{o(n)}$ copies of $|\psi_C\rangle\langle\psi_C|$ and ρ_C, respectively, in a sequence of potentially adaptive product bases, then $d_{\mathrm{TV}}(\mathfrak{D}_1, \mathfrak{D}_2) \leq o(1)$.

On the other hand, a similar calculation as that in the proof of Lemma 19 we have that $\langle \psi_C | \rho_C | \psi_C \rangle \leq 2^{-\Omega(n)}$, so this yields a lower bound for certifying $|\psi_C\rangle$. □

Acknowledgments

We thank Mihir Singhal for helpful discussions, Omar Alrabiah for checking calculations, Mingyu Sun for pointing out errors in an earlier version of the paper, and Sisi Zhou for the reference [ZZJ20]. We also thank ChatGPT and Gemini 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.

[ZZJ20] Sisi Zhou, Chang-Ling Zou, and Liang Jiang. Saturating the quantum Cramér–Rao bound using LOCC. *Quantum Science and Technology*, 5(2):025005, 2020.