

Certifying Localizable Quantum Properties with Constant Sample Complexity

Zhenyu Du¹, Jinchang Liu², Elias X. Huber³, Zi-Wen Liu^{4,*} and Xiongfeng Ma^{1,†}

¹*Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China*

²*Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China*

³*Yenching Academy, Peking University, Beijing 100871, China*

⁴*Yau Mathematical Sciences Center, Tsinghua University, Beijing 100084, China*



(Received 1 October 2025; revised 23 July 2026; accepted 16 September 2026; published 27 October 2026)

Characterizing increasingly complex quantum systems is a central task in quantum information science, yet experimental costs often scale prohibitively with system size. Certifying key properties using simple local measurements is highly desirable but challenging. In this work, we introduce a highly general certification framework based on a physical phenomenon that we call localizable quantumness: for generic many-body states, essential quantum properties are robustly preserved within the projected ensembles on small subsystems after performing local projective measurements on the rest of the system. Leveraging this insight, we develop protocols to certify global properties—including multipartite entanglement, circuit complexity, and quantum magic—by witnessing them on a small, accessible subsystem. Remarkably, randomizing the local measurement bases extends this capability to certify state fidelity. Relying solely on local Pauli measurements, these protocols achieve constant sample complexity and robustness for almost all quantum states, including a wide range of physically relevant states. For certifying the fidelity of n -qubit states, this $\mathcal{O}(1)$ scaling dramatically improves upon state-of-the-art protocols requiring $\mathcal{O}(n^4)$ samples. Our unified framework provides both a practical toolkit for large-scale quantum certification and a novel lens into complex many-body systems.

DOI: [10.1103/PhysRevX.16.041027](https://doi.org/10.1103/PhysRevX.16.041027)

Subject Areas: Quantum Physics, Quantum Information

I. INTRODUCTION

The rapid advancement of quantum technologies is enabling control over increasingly large and complex quantum systems, paving the way for next-generation quantum computers and simulators. This progress, however, brings a central challenge: how can we efficiently characterize these devices at scale? While characterizing an unknown quantum system is generally hard [1,2], in practical experiments one usually has good knowledge of the state-preparation procedure [3–6]. *Quantum certification*—verifying a quantum system by comparing with prior knowledge of its state—provides a powerful approach [7–9]. This approach not only carries fundamental importance in quantum information science [10], but also underpins a broad range of applications, from probing novel

quantum phenomena [11,12] and device benchmarking [13–17] to quantum cryptography [18–20].

A central challenge in certification is to reduce measurement requirements and resource costs [21–28]. As the system size grows, the exponential cost of standard characterization techniques like full state tomography becomes prohibitive. Another straightforward approach—projecting an experimental system onto the ideal state—is impractical, as it requires measurement capabilities comparable to the state preparation itself. These challenges create an imperative need for scalable and experimentally feasible methods to certify quantum states and their essential properties.

This need has motivated a shift toward certification protocols that leverage simple local measurements, which are readily available on most quantum platforms [25–29]. The central difficulty, however, is that many crucial quantum properties, such as multipartite entanglement, are inherently global. Prior attempts to certify these global quantumness with local measurements face crucial limitations: protocols are often designed case by case for specific states or properties [4,25,26], require demanding adaptive measurement schemes that are challenging for near-term devices [28,29], or guarantee soundness only for pure states [25,30–32], severely limiting their applicability in realistic, noisy systems. Furthermore, existing nonadaptive protocols for certifying state fidelity or generic

*Contact author: zwliu0@tsinghua.edu.cn

†Contact author: xma@tsinghua.edu.cn

Published by the American Physical Society under the terms of the [Creative Commons Attribution 4.0 International license](https://creativecommons.org/licenses/by/4.0/). Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

TABLE I. Summary of the quantum properties certified by our framework, together with the corresponding sample complexities and the representative state classes for which these sample complexity guarantees are proven or numerically demonstrated.

Property	Sample complexity	Representative states
(Measurement-assisted) circuit complexity d in D spatial dimensions	$\exp(\mathcal{O}(d^D))$	Deep-thermalized states (Proposition 1) Random brickwork-circuit states (Proposition 1)
Bipartite entanglement	$\mathcal{O}(1)$	Deep-thermalized states (Proposition 1) Random brickwork-circuit states (Proposition 1) Practical Hamiltonian ground states ^a (Sec. V C)
Fully inseparable entanglement	$\mathcal{O}(\log n)$	Haar-random states (Sec. V B; Lemma 10) Random stabilizer states ^a (Sec. V B)
Quantum magic	$\mathcal{O}(1)$	Haar-random states (Sec. VI; Lemma 11) Magic-injection-and-scrambling circuits ^a (Sec. VI)
State fidelity	$\mathcal{O}(1)$	Random graph states (Theorem 4) Haar-random states (Theorem 5) Random brickwork-circuit states ^a (Sec. VII C)

^aNumerics.

properties typically suffer from sample complexity that grows with system size and a diminishing robustness [27]. This prompts a critical question: *is there a general physical principle for robustly and efficiently certifying global quantum properties with simple local measurements?*

In this work, we address this question in the affirmative by introducing and formalizing a fundamental phenomenon we term localizable quantumness. Inspired by localizable entanglement [33,34], we show that the underlying physical principle is far more general. For generic many-body states, essential quantum properties including entanglement, circuit complexity, and magic are robustly encoded throughout the system. Consequently, local projective measurements on a large complement do not destroy these properties but rather concentrate them into the remaining small, accessible subsystem. The measurement-induced projected ensemble on the subsystem thereby carries a distinctive feature that serves as a local signature of the global quantum property.

Leveraging this phenomenon, we develop a unified and highly efficient certification framework that applies broadly to diverse properties (see Table I for the properties considered in detail). Our protocol first localizes the global property into a small subsystem via projective measurements on the large complement system and then witnesses the localized property on the small subsystem. The significant reduction in system size allows us to efficiently certify the quantumness of the subsystem, thereby substantially reducing experimental overhead and enabling the certification of entanglement, circuit complexity, and quantum magic for generic states using only local Pauli measurements. We prove that the method achieves (i) constant sample complexity, (ii) constant-level robustness against deviations from the target states, and (iii) soundness for mixed states, thereby overcoming key limitations of previous approaches and achieving substantial improvement in sample complexity [12,30–32,35]. Our framework

also improves the sample complexity from $\mathcal{O}(n)$ to $\mathcal{O}(\log n)$ for certifying complex properties such as fully inseparable entanglement [26,36]. We further demonstrate its efficiency across various Hamiltonian systems and large-scale magic-injection circuits.

Furthermore, extending this framework by measuring the large complement system in random Pauli bases demonstrates remarkable power in certifying global state fidelity. Using random matrix theory, we prove its constant sample complexity and constant robustness for certifying almost all quantum states. We also establish these guarantees for random graph states via an error localization mechanism: Pauli errors acting on generic stabilizer states can be localized to small subsystems via local measurements. This $\mathcal{O}(1)$ scaling substantially improves upon the state-of-the-art nonadaptive local measurement protocol requiring $\mathcal{O}(n^4)$ samples [27]. Taken together, our unified framework delivers optimal constant-sample-complexity scaling for both property and state certification tasks across generic many-body systems.

Our paper is organized as follows. In Sec. II, we present the key ideas underlying our protocols and provide an overview of the main results. Section III introduces the mathematical framework, formalizes the certification protocol, and analyzes its performance. Sections IV–VI apply our methods to certifying circuit complexity, entanglement, and magic, respectively. Section VII develops the random-basis-enhanced protocol for fidelity certification. Finally, Sec. VIII concludes with broader implications and future directions.

II. OVERVIEW OF METHODS AND RESULTS

This work presents a unified and practical framework for quantum certification based solely on local Pauli measurements. In certification tasks, one typically has reliable prior

knowledge of the quantum system. Specifically, a pure target state ψ_{AB} is known (for example, from a noiseless quantum circuit description), and the goal is to certify whether the experimentally realized mixed state ρ_{AB} possesses certain desired properties. We partition the system into a small subsystem A and its large complement B . Performing computational basis measurements on B generates a measurement-induced ensemble on A , commonly referred to as a *projected ensemble*. Specifically, the experimental state yields $\mathcal{E}_\rho = \{p_\rho(z), \rho_z\}$ on A , while the target state generates $\mathcal{E}_\psi = \{p_\psi(z), \psi_z\}$, as illustrated in Fig. 1(a). While such ensembles have recently attracted substantial attention for probing complex dynamics and deep thermalization [17,37–41], we reveal a powerful new capability: these projected ensembles can serve as robust local signatures of the original global quantum properties. By locally comparing ρ_z and ψ_z on the small subsystem A , our approach efficiently certifies the global quantum properties of ρ . We demonstrate that a broad class of quantum properties can be certified in this way with constant sample complexity. This yields highly efficient certification protocols for complex quantum structures, such as nontrivial measurement-equivalent quantum phases and fully inseparable entanglement.

Our certification framework relies on two key ingredients: (i) establishing that many quantum properties are localizable, meaning they concentrate into the small subsystem A once the complement B is measured, and (ii) converting this observation into an efficient certification protocol by introducing and measuring a quantity we term the conditional fidelity (see Algorithm 1). Together, these ingredients yield our main Result 1, which guarantees that any such property can be certified both efficiently and

robustly. We now outline these two ingredients, with details provided in Sec. III.

The central concept of our approach is *localizable quantumness*. For a broad class of physically relevant many-body states, essential quantum properties of the global system remain robustly encoded in small subsystems even after local projective measurements on the complement. Concretely, if the global target state ψ possesses a localizable quantum property P (see Table I for examples), then the projected ensemble $\mathcal{E}_\psi$ necessarily differs from $\mathcal{E}_\rho$ for any state ρ that lacks P , as shown in Fig. 1(b). This difference represents a local signature of the global property, thereby transforming the otherwise challenging task of global certification into a tractable local problem: certifying the properties of the projected ensemble $\mathcal{E}_\rho$.

To harness localizable quantumness, we avoid the intractable task of directly evaluating projected-ensemble-averaged nonlinear quantities, such as localizable entanglement [33,34]. Instead, we compare the projected ensemble of the experimental state with that of the target. To this end, we introduce the notion of *conditional fidelity*, which evaluates the local fidelity between each projected state ρ_z and its corresponding ψ_z , conditioned on the measurement outcome z on B . A naive strategy—estimating each fidelity $\text{tr}(\psi_z \rho_z)$ —is inefficient, because we have only single-copy access to ρ_z without postselection. In contrast, we estimate the ensemble-averaged local fidelity $\sum_z p_\rho(z) \text{tr}(\psi_z \rho_z)$ via randomized local Pauli measurements on the small subsystem A . This is achieved using the postselection-free local shadow primitive introduced in Ref. [42] and also employed in the shadow-overlap protocol [27]. By estimating the conditional fidelity, we can certify whether the property P is present or the state lies in the free set $\mathcal{F}_P$ (states lacking P), thereby turning the localizable quantumness into a robust witness of global quantum properties. In summary, we establish the following.

Result 1 (Certifying localizable quantumness, informal).

For any property P with associated free set $\mathcal{F}_P$, if the target state ψ exhibits localizable quantumness on a small subsystem A , then the protocol achieves:

- (1) using nonadaptive local measurements;
- (2) soundness: all (possibly mixed) $\rho \in \mathcal{F}_P$ are rejected with high probability;
- (3) completeness (robustness): any ρ within a constant trace distance of ψ is accepted with high probability; and
- (4) constant sample complexity: the number of required copies is $\mathcal{O}(1)$ for constant subsystem size $|A| = \mathcal{O}(1)$.

The requirement of localizable quantumness is highly general [12,17,25,33,34,37,38,43]. As summarized in Table I, we establish both analytically and numerically that this phenomenon is indeed a universal feature across a wide range of quantum many-body systems.

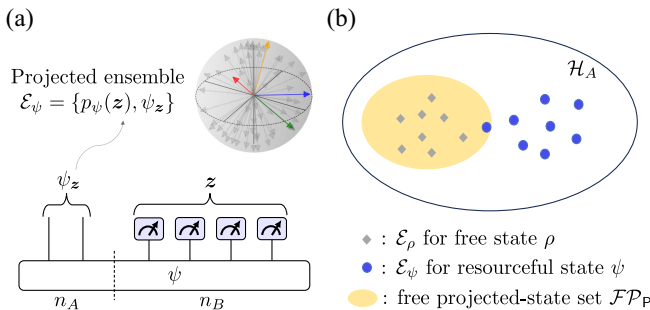


FIG. 1. Localizable quantumness within projected states. (a) Projected ensemble: the target state is partitioned into subsystems A and B . Measuring B in the computational basis yields an outcome z and a corresponding projected state ψ_z on A with probability $p_\psi(z)$, thereby defining the projected ensemble $\mathcal{E}_\psi$. (b) Localizable quantumness: if the target state exhibits localizable quantumness, then its projected ensemble $\mathcal{E}_\psi$ differs significantly from the projected ensemble of any free state ρ . For instance, most projected states lie outside the free projected-state set $\mathcal{F}_P$. This difference can be utilized to certify the quantumness of the target state by examining the small subsystem A .

Built upon this ubiquitous physical phenomenon, our certification framework achieves powerful performance guarantees. First, the guarantee of soundness for mixed states marks a significant advance over previous approaches, which often applied only to pure states when certifying complex quantum properties [30–32,35]. Second, the constant robustness also represents an important advantage over protocols whose robustness diminishes with system size [27,28], ensuring practical certification in realistic noisy settings. Finally, the guarantee of constant sample complexity yields substantial improvements over prior methods, as detailed below. Combined with the use of only local Pauli measurements, this ensures experimental efficiency and scalability. Taken together, these features establish a versatile and powerful framework for certifying diverse quantum properties.

A. Complexity certification

A highlight of our results is the first explicit construction of complexity witnesses. In Sec. IV, we show that circuit complexity, i.e., the minimal circuit depth required to prepare a state, can be certified to exceed a constant threshold with constant sample complexity and robustness. The key idea is to certify reliable signatures of circuit complexity, such as high entanglement, on a carefully chosen small subsystem. This approach also extends to certifying *measurement-assisted* circuit complexity, which can be exponentially smaller than standard state complexity and is, therefore, more challenging to certify [44,45]. Our framework, thus, opens a new pathway for probing intricate structures in many-body quantum systems. As two important examples, it enables efficient certification of long-range entanglement [46,47] and nontrivial measurement-equivalent quantum phases [48].

Corollary 1 (Certifying quantum circuit complexity, informal). If the target state exhibits high localizable entanglement on a specific small subsystem, then constant (measurement-assisted) quantum circuit complexity can be certified with constant sample complexity while achieving constant robustness. This enables certification of long-range entanglement and nontrivial measurement-equivalent quantum phases with $\omega(1)$ sample complexity. [In this work, “ $\omega(1)$ sample complexity” means $\mathcal{O}(f(n))$ samples for any function $f(n) = \omega(1)$.]

Concretely, these performance guarantees are established for deep-thermalized states [17,37–41] and physically relevant random brickwork-circuit states (see Table I).

B. Entanglement certification

In Sec. V, we show that our method enables highly efficient certification of entanglement. For bipartite entanglement, we show that localizable entanglement on a small subsystem suffices to certify entanglement across exponentially many bipartitions with constant sample complexity. More strikingly, we establish a highly efficient method for

certifying *fully inseparable entanglement*, namely, entanglement across all possible bipartitions [36], using only logarithmic sample complexity. Fully inseparable entanglement is a crucial resource for quantum error correction [26] and for the activation of genuine multipartite entanglement [49], making our certification protocol especially valuable.

Corollary 2 (Certifying fully inseparable entanglement, informal). If the target state exhibits localizable entanglement on certain small subsystems, then fully inseparable entanglement can be certified with $\mathcal{O}(\log n)$ sample complexity while achieving constant robustness.

Beyond establishing the performance of this entanglement certification method for deep-thermalized states and random brickwork-circuit states, we also numerically demonstrate its efficiency across random stabilizer states and various Hamiltonian systems (see Table I).

C. Magic certification

We further apply our framework to quantum magic (or nonstabilizerness) certification in Sec. VI, with the free set consisting of convex mixtures of all stabilizer states. Since local Pauli measurements are free operations in the magic resource theory and preserve stabilizerness, the presence of localizable quantum magic after measuring a large complement in the computational basis directly certifies the magic of the target state.

Corollary 3 (Certifying quantum magic, informal). If the target state exhibits localizable magic on a small subsystem, then quantum magic can be certified with $\mathcal{O}(1)$ sample complexity while achieving constant robustness.

These performance guarantees are established for typical Haar-random states. Furthermore, because magic is a fundamental resource for fault-tolerant quantum computing [50], we numerically demonstrate the scalability of our approach on magic-injection circuits for systems up to 512 qubits. To the best of our knowledge, this is the first protocol to certify quantum magic using only single-copy local measurements while achieving soundness for mixed states. Consequently, our framework offers the potential for exponential improvements in sample complexity for relevant experiments, such as detecting magic phase transitions [12] and benchmarking near-term fault-tolerant demonstrations.

D. Fidelity certification

Finally, we show that global state fidelity is also robustly encoded within small subsystems in Sec. VII. Specifically, we propose a fidelity certification protocol that compares local fidelities on a small subsystem after measuring the large complement in local Pauli bases. Our protocol achieves constant sample complexity and robustness for almost all quantum states, including random graph states. Since every stabilizer state is local-Clifford equivalent to a graph state, this yields the first proof that generic stabilizer states can be efficiently certified using solely local random

Pauli measurements. This constant scaling dramatically improves upon state-of-the-art nonadaptive methods, whose costs grow polynomially with system size and whose robustness against state imperfection diminishes [27,28], as well as over adaptive local-measurement approaches that require challenging classical feedback and long-lived quantum memory to store states between measurement rounds [28,29,51] (see Sec. VII for a detailed comparison).

Result 2 (Certifying state fidelity, informal). Conditional fidelity robustly certifies the global fidelity of typical pure target states. Specifically, the protocol provably achieves constant sample complexity and constant robustness for almost all quantum states (Theorem 5) and for random graph states (Theorem 4).

III. MATHEMATICAL FRAMEWORK AND PROTOCOL

Having outlined the key ideas and results of our work, we now present the certification framework and protocol in detail. We begin by formalizing the notion of localizable quantumness, which serves as the foundation of our approach. Building on this, we show how to construct property witnesses through conditional fidelity. Then, we present the complete protocol scheme, together with an analysis of its performance guarantees.

A. Localizable quantumness and conditional fidelity

We partition the n -qubit system into a small subsystem A (with n_A qubits) and its complement B (with n_B qubits, so that $n_A + n_B = n$). In the computational basis of B , the target state can be written as

$$|\psi\rangle = \sum_{z \in \{0,1\}^{n_B}} \sqrt{p_\psi(z)} |\psi_z\rangle_A \otimes |z\rangle_B, \quad (1)$$

which induces the projected ensemble $\mathcal{E}_\psi := \{p_\psi(z), \psi_z\}$ [see Fig. 1(a)]. For a (possibly mixed) experimental state ρ , computational-basis measurements on B yields outcome z with a projected state on A :

$$\rho_z := \frac{\text{tr}_B[(I_A \otimes |z\rangle\langle z|_B)\rho]}{p_\rho(z)} \quad (2)$$

with probability $p_\rho(z) := \text{tr}[(I_A \otimes |z\rangle\langle z|_B)\rho]$.

To quantify the strength of localizable quantumness for a property P , we first specify its associated free set $\mathcal{F}_P \subseteq \mathcal{D}(\mathcal{H}_{AB})$, consisting of all states that do not possess P (e.g., the separable states when P is entanglement). Local projective measurements on subsystem B maps each $\rho \in \mathcal{F}_P$ to a family of projected states on A , thereby inducing the free projected-state set

$$\mathcal{FP}_P := \{\rho_z : \rho \in \mathcal{F}_P, p_\rho(z) \neq 0\}. \quad (3)$$

For the target state ψ , we then define the maximal fidelity at each outcome z by

$$\text{Fid}_P(\psi_z) := \sup_{\sigma \in \mathcal{FP}_P} \text{tr}(\sigma \psi_z). \quad (4)$$

Small values of $\text{Fid}_P(\psi_z)$ indicates strong localizable quantumness—i.e., ψ_z remains far from all property-free projected states on A [Fig. 1(b)]. Averaging over outcomes yields our localizable-quantumness metric

$$\text{LQP}(\psi) := \sum_{z \in \{0,1\}^{n_B}} p_\psi(z) [1 - \text{Fid}_P(\psi_z)]. \quad (5)$$

This quantity plays a central role in our certification protocols, serving as the gap that separates the target state from all property-free states (Lemma 1). Unlike localizable entanglement [33], we do not optimize over measurement bases on B , as fixing a simple local measurement scheme minimizes experimental requirements.

We also consider random-basis measurements on B : independently for each qubit, randomly choose a Pauli measurement basis $X/Y/Z$. Equivalently, the single-qubit positive operator-valued measure (POVM) on B is

$$\left\{ \frac{1}{3} |0\rangle\langle 0|, \frac{1}{3} |1\rangle\langle 1|, \frac{1}{3} |+\rangle\langle +|, \frac{1}{3} |-\rangle\langle -|, \frac{1}{3} | +i\rangle\langle +i|, \frac{1}{3} | -i\rangle\langle -i| \right\}. \quad (6)$$

Let $\mathbf{x} \in \{0, 1, +, -, +i, -i\}^{n_B}$ (abbreviated as $\mathbf{X}^{n_B}$) denote the outcome string. The projected state on A and its probability are, respectively,

$$|\psi_{\mathbf{x}}\rangle = \frac{(I_A \otimes \langle \mathbf{x} |_B) |\psi\rangle}{\sqrt{3^{n_B} \tilde{p}_\psi(\mathbf{x})}}, \quad \tilde{p}_\psi(\mathbf{x}) = 3^{-n_B} \text{tr}[(I_A \otimes |\mathbf{x}\rangle\langle \mathbf{x}|_B) \psi]. \quad (7)$$

The random-basis metric of localizable quantumness is then

$$\widetilde{\text{LQP}}(\psi) := \sum_{\mathbf{x} \in \mathbf{X}^{n_B}} \tilde{p}_\psi(\mathbf{x}) [1 - \text{Fid}_P(\psi_{\mathbf{x}})]. \quad (8)$$

This variant preserves minimal experimental requirements while enabling extensive data reuse and flexible postprocessing from a single measurement dataset. These advantages will be leveraged in our entanglement certification scheme. In what follows, we present the protocol under computational-basis measurements on B , and the extension to the random-basis setting is straightforward.

We certify the target property P by comparing the projected ensemble of the experimental state ρ with that of the target ψ . Formally, we define the observable

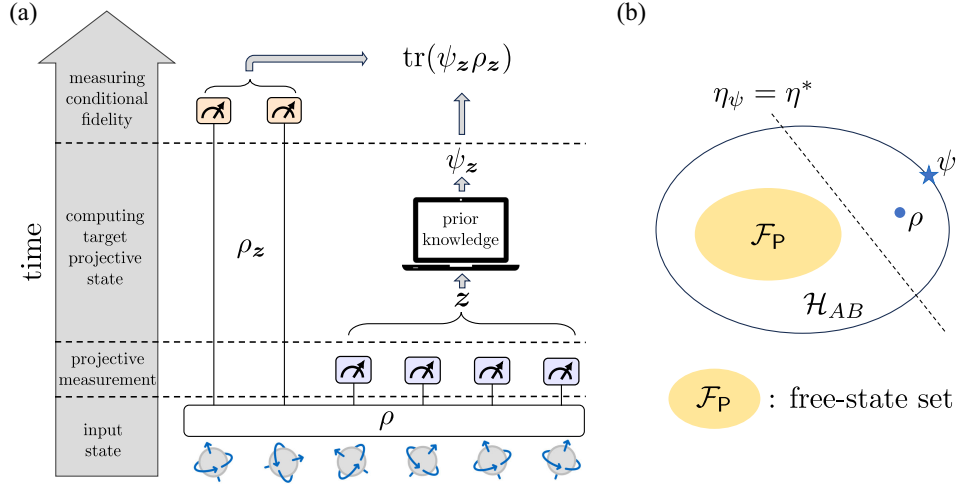


FIG. 2. Certifying quantum properties via conditional fidelity. (a) Work flow of Algorithm 1. Computational-basis measurements (shown in blue) are performed on a subsystem of ρ , yielding an outcome z and the corresponding projected state ρ_z . Randomized Pauli measurements (shown in orange) are then applied to ρ_z . Leveraging prior knowledge of ψ_z , we postprocess the measurement data to obtain estimators of $\text{tr}(\psi_z \rho_z)$. (b) Decision rule and robustness. By selecting an appropriate threshold η^* and estimating the conditional fidelity η_ψ from the measurement data, states ρ that are close to ψ are accepted, while property-free states are rejected.

$$\begin{aligned}
 O_P(\psi) &:= \sum_z [\psi_z - \text{Fid}_P(\psi_z)I] \otimes |z\rangle\langle z| \\
 \eta_\psi(\rho) &:= \text{tr}[O_P(\psi)\rho] \\
 &= \sum_z p_\rho(z) [\text{tr}(\psi_z \rho_z) - \text{Fid}_P(\psi_z)]. \quad (9)
 \end{aligned}$$

We refer to such an ensemble-averaged quantity as a conditional fidelity, since it averages local fidelities conditioned on measurement outcomes of B . Each local fidelity is shifted by the constant $\text{Fid}_P(\psi_z)$, ensuring that the operator $\psi_z - \text{Fid}_P(\psi_z)I$ acts as a valid property witness, taking positive expectation only for projected states lying outside the free set $\mathcal{FP}_P$.

Lemma 1 ($\eta_\psi(\rho)$ is a valid witness). The conditional fidelity η_ψ satisfies

- (1) soundness: if $\rho \in \mathcal{F}_P$, then $\eta_\psi(\rho) \leq 0$; and
 - (2) completeness: for the target ψ , $\eta_\psi(\psi) = \text{LQ}_P(\psi)$.
- Consequently, the gap $\text{LQ}_P(\psi)$ separates ψ from all property-free states, making η_ψ a valid witness for P .

Proof. If $\rho \in \mathcal{F}_P$, then for every z with $p_\rho(z) > 0$ we have $\rho_z \in \mathcal{FP}_P$. The definition of maximal fidelity implies $\text{tr}(\psi_z \rho_z) - \text{Fid}_P(\psi_z) \leq 0$. Averaging over outcomes yields $\eta_\psi(\rho) \leq 0$. For the target state ψ ,

$$\text{tr}[O_P(\psi)\psi] = \sum_z p_\psi(z) [1 - \text{Fid}_P(\psi_z)], \quad (10)$$

which equals $\text{LQ}_P(\psi)$ by definition. $\blacksquare$

By continuity, η_ψ also certifies P for any state ρ sufficiently close to ψ [Fig. 2(b)]. Moreover, replacing $\text{Fid}_P(\psi_z)$ in $O_P(\psi)$ with suitable upper bounds $f(\psi_z)$ also suffices for certification. This slightly reduce the gap in

Lemma 1 to

$$\Delta = \sum_z p_\psi(z) [1 - f(\psi_z)], \quad (11)$$

but, in practice, such bounds are often easier to compute and readily available.

B. Protocol scheme and performance

We now turn the above construction into a practical, experimentally implementable protocol and analyze its performance (see Appendix A for proofs). Algorithm 1 details our protocol scheme, which proceeds in three

ALGORITHM 1. Protocol for certifying quantum properties.

Input: Quantum state ρ ; classical description of a target state ψ ; failure probability $\delta \in (0, 1)$.

Output: accept or reject.

Precomputation:

1. Find a partition $A \cup B$.

Experiment:

2. Measure subsystem B of ρ in the computational basis, obtaining an outcome z .
3. Measure subsystem A of ρ_z in a random Pauli basis, obtaining an outcome x .
4. Repeat steps 2 and 3 for T rounds, obtaining $\{(z_i, x_i)\}_{i=1}^T$.

Postprocessing:

5. Compute the estimator ω_i of $\text{tr}(\psi_{z_i} \rho_{z_i})$ for $1 \leq i \leq T$ using local classical shadow, and compute the median-of-means estimator ω using $\{\omega_i - \text{Fid}(\psi_{z_i})\}_{i=1}^T$.
6. Set $\eta^* = \text{LQ}(\psi)/3$. If $\omega \leq \eta^*$, output reject; otherwise, output accept.

stages: (i) Choose a partition $A \cup B$ such that the subsystem A exhibits large localizable quantumness. (ii) Perform measurements on ρ and record the measurement outcomes. (iii) Using the measurement record together with prior knowledge of ψ , compute the estimator of $\eta_\psi(\rho)$ and decide whether ρ possesses the target property.

In the protocol, we need to evaluate $\text{LQ}_P(\psi)$ for the chosen partition and $\text{Fid}_P(\psi_z)$ for the sampled projected states. Rather than exhaustively enumerating the full projected ensemble $\mathcal{E}_\psi$, one can reliably estimate $\text{LQ}_P(\psi)$ by sampling only a small subset of projected states. As discussed, it is not necessary to compute $\text{Fid}_P(\psi_z)$ exactly; replacing it with suitable upper bounds $f(\psi_z)$ suffices. This substitution reduces the gap from $\text{LQ}_P(\psi)$ to a smaller value Δ [Eq. (11)], and we may adjust the threshold to $\eta^* = \Delta/3$ accordingly. In all applications considered here, subsystem A is of constant size, which makes the computation of $\text{Fid}_P(\psi_z)$ or its upper bound efficient. Throughout this section, we therefore treat the partition $A \cup B$ together with the values of $\text{LQ}_P(\psi)$ and $\text{Fid}_P(\psi_z)$ as given, deferring their explicit construction to the discussion of specific applications.

In each experimental round i , we first measure subsystem B in the computational basis $\{|z\rangle\}_{z \in \{0,1\}^{n_B}}$, obtaining a bit string z_i drawn from $p_\rho(z)$. Conditional on this outcome, we then measure each qubit of A in an independently and uniformly chosen random single-qubit Pauli basis using the POVM of Eq. (6), recording the outcome $\mathbf{x}_i \in X^{n_A}$. Repeating for T rounds yields the dataset $\{(z_i, \mathbf{x}_i)\}_{i=1}^T$.

In the postprocessing step, we use the collected data to evaluate $\eta_\psi(\rho)$. The informationally complete POVM on subsystem A enables an unbiased estimator $\omega_i := \text{tr}\{\psi_{z_i}[\otimes_{j \in A} (3|\mathbf{x}_{i,j}\rangle\langle\mathbf{x}_{i,j}| - I_j)]\}$ of $\text{tr}(\psi_{z_i}\rho_{z_i})$ using local classical shadow [27,42,52]. The final estimator ω is given by applying the median-of-means procedure to T estimators $\{\omega_i - \text{Fid}_P(\psi_{z_i})\}_{i=1}^T$.

Finally, we certify the property by comparing the estimator to $\eta^* = \text{LQ}_P(\psi)/3$. This decision threshold is placed between the maximal free-state value (≤ 0) and the ideal value $\text{LQ}_P(\psi)$, leaving margins of $\text{LQ}_P(\psi)/3$ above 0 and $2\text{LQ}_P(\psi)/3$ below $\text{LQ}_P(\psi)$. These margins absorb statistical fluctuations and experimental noise. Our protocol is summarized in Fig. 2. We have the following performance guarantee.

Theorem 1 (Performance of Algorithm 1, formal version of Result 1). Given a property P , a target state ψ , and a bipartition $A \cup B$, Algorithm 1 satisfies

- (1) (soundness): if the input state $\rho \in \mathcal{F}_P$, the protocol outputs **reject** with probability at least $1 - \delta$; and
- (2) (completeness): if ρ satisfies $d_{\text{tr}}(\psi, \rho) \leq \varepsilon$ with $\varepsilon = \text{LQ}_P(\psi)/6$, the protocol outputs **accept** with probability at least $1 - \delta$.

Moreover, the protocol performs local Pauli measurements on ρ with sample complexity

$$T = \frac{243 \ln(\delta^{-1}) \sigma^2}{\text{LQ}_P^2(\psi)}, \quad (12)$$

where $\sigma^2 = 4^{n_A} + 1$.

When $n_A = \mathcal{O}(1)$, $\text{LQ}_P(\psi) = \Omega(1)$, the sample complexity is $T = \mathcal{O}(1)$, while achieving $\varepsilon = \Omega(1)$ robustness.

Therefore, strong localizable quantumness $\text{LQ}_P(\psi)$ on a small subsystem guarantees sample-efficient certification, validating Result 1. This condition holds for a broad class of states, which is established in subsequent sections.

An important benefit of our protocol is its constant robustness against state deviation. Specifically, our scheme accepts any input state ρ within $\varepsilon = \Omega(1)$ trace distance of the target state ψ . Compared to certification methods that require the experimental state to be ε -close to the target with $\varepsilon \sim 1/\text{poly}(n)$ [27,28], the constant robustness of our method significantly relaxes experimental requirements. Given the high gate fidelities achieved by current platforms [53,54], this robustness effectively enlarges the certifiable circuit volume by a substantial factor. Furthermore, in the early fault-tolerant regime with quantum error correction techniques, our protocol serves as a practical tool for certifying logical preparation procedures, such as magic injection and cultivation.

Moreover, our protocol reliably rejects any mixed state in $\mathcal{F}_P$, offering an advantage over previous protocols that detect properties only for pure input states, such as those for circuit complexity [31,32] and magic [30]. The decision boundary η^* can also be tuned closer to the property-free value 0 to further enhance robustness. Meanwhile, this also increases the sample complexity, as higher precision is required to estimate $\eta_\psi(\rho)$. Therefore, η^* can be tuned to balance robustness and sample complexity.

C. Remarks on computational efficiency

While our protocol is experimentally efficient, its practical application also relies on the computational cost of classical processing. In our protocol, this cost is dominated by obtaining classical descriptions of the projected states ψ_z . Although, in general, computing ψ_z may require exponential time, for a broad class of physically relevant states, this computation is tractable. Tensor-network representations enable efficient classical computation for a wide class of large quantum systems [55–59]. Examples include states produced by one-dimensional logarithmic-depth circuits [60], the surface-code ground state [61], and other long-range-entangled states [62]. Neural-network quantum states [63–65] also capture highly entangled states while permitting efficient evaluation of ψ_z . In many scenarios, such as magic-state injection protocols [50],

the projected states are known exactly by construction. Furthermore, for small subsystem sizes n_A , computing the projected state is feasible under the amplitude query model by querying individual amplitudes of ψ_z , consistent with the framework established in Ref. [27]. Hence, our certification scheme is both sample efficient and computationally tractable for a broad range of states.

Our protocol also requires estimating the maximal fidelity $\text{Fid}_P(\psi_z)$, or a suitable upper bound, on the subsystem A . This value can be computed in time $2^{\mathcal{O}(n_A)}$ for entanglement and circuit complexity via singular value decomposition or in time $2^{\mathcal{O}(n_A^2)}$ for quantum magic using the methods from Ref. [66]. Since our protocol requires only a small subsystem size n_A , this computational procedure remains efficient.

Crucially, our framework decouples the quantum experiment from the classical computation by using nonadaptive local measurements. During the quantum stage, no prior knowledge of state preparation is required, so data collection is highly efficient. Consequently, the same dataset can be analyzed offline for exponentially many different properties or even different target states [27,52], which can yield exponential improvements in sample complexity over previous protocols, as exemplified in Sec. V. Given that quantum resources are currently far expensive than classical ones, this decoupling is a significant practical advantage.

IV. CERTIFYING QUANTUM CIRCUIT COMPLEXITY

Having established our certification framework, we now illustrate its power and versatility by applying it to four central tasks in quantum information: certifying quantum circuit complexity, entanglement, magic, and state fidelity.

We begin with circuit complexity. It quantifies the minimal resources required to prepare a quantum state and plays a fundamental role connecting quantum computation [67,68], quantum learning [31,32,69], many-body physics [37,41,43,46,47,70], and black-hole physics [71–73]. Certifying that a prepared state has high complexity is, therefore, crucial both for probing novel structures of quantum matter and for benchmarking experimental platforms.

A. Certifying unitary circuit complexity

We first consider the standard notion of circuit complexity for unitary circuit architectures. Formally, for a given circuit architecture specified by a graph $G = (V, E)$ where vertices represent qubits and edges indicate the qubit pairs on which native two-qubit gates may act, we define the circuit complexity of a quantum state as the minimum circuit depth required to prepare it within G . For a pure target state ψ , the circuit complexity is given by

$$C_G(\psi) := \min \left\{ d : |\psi\rangle = \prod_{i=1}^d \left(\bigotimes_j V_{i,j} \right) |0\rangle^{\otimes n} \right\}, \quad (13)$$

where $V_{i,j}$ is a two-qubit gate in the i th layer with $\text{supp}(V_{i,j}) \in E$ or a single-qubit gate and the gates in the same layer act on disjoint qubits. For a mixed state ρ , we adopt the convex-roof extension. Any ρ can be written as $\rho = \sum_k p_k \psi_k$ with $p_k \geq 0$ and $\sum_k p_k = 1$. One may prepare ρ by sampling k with probability p_k and then preparing ψ_k using a circuit of depth $C_G(\psi_k)$. The quantum circuit complexity of ρ can, therefore, be no larger than the largest depth needed among the ψ_k . Formally,

$$C_G(\rho) := \min \left\{ d : \rho = \sum_i p_i \psi_i, \text{ with } p_i \geq 0, \sum_i p_i = 1, \right. \\ \left. \text{and } C_G(\psi_i) \leq d \text{ for all } i \right\}. \quad (14)$$

We apply our framework to certify that the complexity of a state exceeds a certain depth d on a D -dimensional lattice. While learning-based protocols exist [31,32,35], they are often restricted to pure states and require a sample complexity that grows with system size, limiting their usage in realistic noisy settings. In contrast, our approach overcomes these limitations and exponentially improves sample complexity, achieving constant sample complexity for certifying constant-depth complexity [$d = \mathcal{O}(1)$] and remaining sound for mixed states.

Our approach is based on a key physical insight: in a low-depth circuit, information can propagate only a limited distance. This light-cone effect dictates that local measurements on the periphery of a system cannot substantially alter the entanglement structure deep within its center. Consequently, low-complexity states yield projected states with limited entanglement.

Formally, we focus here on an $m \times m$ two-dimensional case ($D = 2$, with circuit complexity denoted C_2). Our method readily extends to higher dimensions. Let A be the set of qubits in a $2w \times 2w$ square and B its complement, as illustrated in Fig. 3(a), where the width w is chosen slightly larger than the threshold depth d . The key observation is that, for a circuit of depth d , the entanglement between the left and right halves of region A [L and R , respectively, in Fig. 3(a)] is bounded. This is because only gates near the boundary between L and R can generate entanglement across this cut, and a shallow circuit contains few such gates. We formalize this as the following lemma. Detailed proofs are given in Appendix B.

Lemma 2 (Entanglement in states of low unitary circuit complexity). Let $|\phi\rangle$ be an $(m \times m)$ -qubit pure state with circuit depth $C_2(\phi) \leq d$. Consider the partition $A \cup B$ with $A = L \cup R$, as depicted in Fig. 3. Then, for every measurement outcome $z \in \{0, 1\}^{n_B}$,

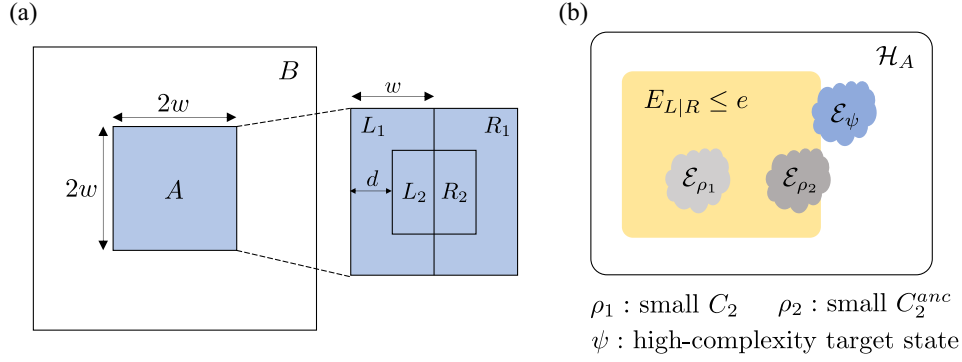


FIG. 3. Projected ensembles for certifying circuit complexity d . (a) Partitioning of a two-dimensional lattice: the full $m \times m$ lattice is divided into subsystems A and B , where A is a $2w \times 2w$ square. Subsystem A is further split into L and R , with $L = L_1 \cup L_2$ and $R = R_1 \cup R_2$. The regions L_1 and R_1 comprise all qubits whose distance to B is at most d . (b) Entanglement in the projected ensemble certifies complexity. The free projected-state set $\mathcal{FP}_P$ consists of states with entanglement across $L|R$ below a threshold e . If a state ρ_1 has small unitary circuit complexity C_2 , all of its projected states lie in $\mathcal{FP}_P$. If a state ρ_2 has small measurement-assisted complexity C_2^{anc} , a large fraction of its projected states lie in $\mathcal{FP}_P$. Our protocol efficiently certifies the complexity of a high-complexity target ψ whose projected states are far from $\mathcal{FP}_P$.

$$E_{L|R}(\phi_z) \leq 8wd, \quad (15)$$

where $E_{L|R}(\xi_{LR}) := S(\xi_L) = -\text{tr}(\xi_L \log \xi_L)$ is the entanglement entropy of the state ξ_{LR} across the bipartition $L|R$.

In essence, Lemma 2 characterizes the projected free set $\mathcal{FP}_P$ for the property P of “circuit complexity $C_2 > d$ ”: it contains only projected states with low entanglement across $L|R$. Conversely, if the projected states of the target are highly entangled, they must lie far from $\mathcal{FP}_P$. Therefore, the high entanglement entropy of the projected ensemble provides a clear signature of circuit complexity, as illustrated in Fig. 3(b), enabling efficient certification of circuit complexity.

Theorem 2 (Certifying 2D quantum circuit complexity). Let ψ be the target state and consider the bipartition $A \cup B$ shown in Fig. 3, with $w = \eta d$ for some $\eta > 4$. Suppose projected ensemble of ψ on A satisfies

$$\Pr_{z \sim p_\psi(z)} [E_{L|R}(\psi_z) \geq c|L| + 1] \geq p = \Omega(1), \quad (16)$$

for a constant $c = 4\eta^{-1} + \Omega(1)$. Then Algorithm 1 certifies that the circuit complexity of ψ exceeds d with constant failure probability, using $T = \exp(\mathcal{O}(\eta^2 d^2))$ copies of ψ and achieving robustness $\varepsilon = \Omega(1)$.

Therefore, for constant circuit complexity $d = \mathcal{O}(1)$, our protocol achieves constant sample complexity and robustness. This constant-depth regime is particularly important: in finite spatial dimensions, depths $d = \omega(1)$ are associated with long-range entanglement in many-body systems [46,47,74]. Consequently, our protocol provides a sample-efficient method for certifying long-range entanglement by certifying depths just beyond the constant regime using $\omega(1)$ samples. Moreover, the protocol

requires only polynomially many samples up to depths $d = \mathcal{O}[(\log n)^{1/2}]$ (or, more generally, $d = \mathcal{O}[(\log n)^{1/D}]$ in spatial dimension D).

B. Certifying measurement-assisted circuit complexity

We now turn to a stronger notion—measurement-assisted circuit complexity [43,48]. Measurement-assisted circuits permit midcircuit single-qubit measurements with classical feedforward and have attracted significant recent interest because they can provide exponential depth shortcuts for preparing important many-body states, including topologically ordered phases [44,45,62,75,76]. The recently introduced spacetime quantum circuit complexity also unifies notions of circuit width, depth, and measurements and reveals a novel complexity concentration phenomenon in measurement-assisted circuits [43].

Here, we focus on the definition of measurement-assisted circuit complexity as the minimum number of measurement layers required to prepare a target state *deterministically*. This definition underpins the hierarchy of topological order and the notion of nontrivial measurement-equivalent quantum phases [48]. Formally, fix an architecture $\mathbf{G} = (V, E)$ on $n = |V|$ qubits, a depth- d measurement-assisted circuit consists of d rounds. In round $i \in [d]$, conditioned on the previous measurement record $m_{<i} = (m_1, \dots, m_{i-1})$, one applies parallel two-qubit gates $\{V_{i,\ell}^{m_{<i}}\}_\ell$ on pairwise disjoint edges of E (and arbitrary single-qubit gates if desired), followed by single-qubit projective measurements $\{P_{i,q}^{m_{<i}}(b)\}_{b \in \{0,1\}}$ on a subset of qubits q , yielding outcomes $m_{i,q} \in \{0,1\}$. Gates and measurements within the same round act on disjoint qubits, and future operations may depend on the cumulative measurement record $m_{<i}$. Let $m = (m_1, \dots, m_d)$ denote

the full outcome record. The unnormalized postmeasurement state is

$$|\tilde{\phi}_m\rangle = \left[\prod_{i=1}^d \left(\prod_q P_{i,q}^{m_{<i}}(m_{i,q}) \right) \left(\prod_{\ell} V_{i,\ell}^{m_{<i}} \right) \right] |0\rangle^{\otimes n}, \quad (17)$$

with branch probability $p_m = \|\tilde{\phi}_m\|_2^2$ and normalized state $|\phi_m\rangle = |\tilde{\phi}_m\rangle / \sqrt{p_m}$. The measurement-assisted circuit complexity of a pure state ψ is

$$C_G^{\text{anc}}(\psi) := \min\{d: \exists \text{ depth-}d \text{ measurement-assisted circuit such that, } \forall m \text{ with } p_m > 0, |\phi_m\rangle = |\psi\rangle\}. \quad (18)$$

For mixed states, we use the convex-roof extension the same as in Eq. (14).

Low-depth measurement-assisted circuits are also expected to generate limited entanglement across appropriately chosen cuts. Nonetheless, incorporating the effects of measurements is subtle. For example, depending on the partition, measurements can induce significant entanglement in postmeasurement states even when the underlying unitary depth is shallow [77]. We address this by choosing the specific bipartition in Fig. 3 and leveraging the fact that entanglement entropy is a monotone that is nonincreasing on average under local measurements [78]. The next lemma quantifies the average entanglement remaining on A after measuring its complement B .

Lemma 3 (*Entanglement in states of measurement-assisted circuit complexity*). Let $|\phi\rangle$ be an $(m \times m)$ -qubit pure state with measurement-assisted circuit complexity $C_2^{\text{anc}}(\phi) \leq d$. Consider the partition $A \cup B$ with $A = L \cup R$ as depicted in Fig. 3. Then,

$$\mathbb{E}_{z \sim p_\phi(z)} [E_{L|R}(\phi_z)] \leq 12wd. \quad (19)$$

Therefore, although certain projected states ϕ_z may exhibit high entanglement, the average entanglement remains small. As a result, most projected states lie in a low-entanglement set [Fig. 3(b)]. Nonetheless, this crucial distinction makes the conditional fidelity witness in Lemma 1 less effective. To address this, we adopt a linear witness of the form

$$\tilde{O} := \sum_z [t + (1-t)\Theta_t(\text{Fid}(\psi_z))]| \psi_z \rangle \langle \psi_z |_A \otimes |z\rangle \langle z|_B, \quad (20)$$

where $t \in (0, 1)$ and $\Theta_t(x) = \mathbf{1}[x \leq t]$ is a threshold function. The precise construction of $\tilde{O}$, along with the set defining the maximal fidelity $\text{Fid}(\psi_z)$, is provided in Appendix B, together with the full proofs. Using this construction, we establish the following.

Theorem 3 (*Certifying 2D measurement-assisted circuit complexity*). Let ψ be the target state and consider the

bipartition $A \cup B$ shown in Fig. 3, with $w = \eta d$ for some $\eta > 6$. Suppose the projected ensemble of ψ on A satisfies

$$\Pr_{z \sim p_\psi(z)} [E_{L|R}(\psi_z) \geq c|L| + 1] \geq p = \Omega(1), \quad (21)$$

for a constant $c = [6 + \Omega(1)]p^{-1}\eta^{-1}$. Then, estimating $\text{tr}(\tilde{O}\rho)$ above a threshold η^* certifies that the measurement-assisted circuit complexity of ψ exceeds d with constant failure probability δ using $\exp(\mathcal{O}(\eta^2 d^2))$ copies of ψ and achieving robustness $\varepsilon = \Omega(1)$.

In the regime $d = \mathcal{O}(1)$, our protocol again uses only $\mathcal{O}(1)$ sample complexity. This enables, in particular, the certification of nontrivial measurement-equivalent quantum phases [those with $C_2^{\text{anc}} = \omega(1)$] [48] using only $\omega(1)$ samples. Although the hidden constant could be large, to our knowledge, these are the first protocols to achieve system-size-independent sample-complexity scaling for certifying unitary and measurement-assisted circuit complexity.

C. Performance on generic quantum states

We now show that our approach applies to generic quantum states and a wide range of physically relevant states. The detailed proofs are given in Appendix C.

An important class of states is those drawn Haar randomly, which could demonstrate the average-case performance of our protocol over the full Hilbert space. For Haar-random states, the projected states on subsystem A are highly entangled. This can be established via the concept of deep thermalization [17,37]: higher moments of the measurement-induced projected ensemble within a subsystem are close to their thermal values (i.e., to those of the Haar ensemble), so the ensemble forms an (approximate) state design. The high entanglement inherent in second-order state designs [79] suffices to satisfy the requirement in Theorems 2 and 3, enabling sample-efficient certification of complexity for these deep-thermalized states.

Proposition 1 (*Certifying circuit complexity of deep-thermalized states*). Let ψ be an n -qubit state whose projected ensemble $\mathcal{E}_\psi$ on a specific $\Theta(d^2)$ -qubit system A (see Fig. 3) forms an ϵ -approximate 2-design with $\epsilon = \mathcal{O}(2^{-n_A/2})$. Then, our protocols can certify that ψ has complexity C_2 (or C_2^{anc}) larger than d with a sample complexity of $\exp(\mathcal{O}(d^2))$ while achieving constant robustness.

Using deep thermalization results for Haar-random states [37], we establish the average-case performance of our protocol for Haar-random states. Moreover, deep thermalization has been observed in many chaotic physical quantum systems [39–41], so our protocol also applies to these physically relevant states.

To further assess practical performance, we consider more experimentally relevant ensembles: states generated by brickwork quantum circuits, where each layer consists of two-qubit gates arranged in a staggered pattern. Such

architectures serve as canonical ensembles for studying the generic behavior of physical quantum states [77,80–82]. We prove in Appendix C that, for finite D -dimensional circuits, as long as the circuit depth d' is slightly larger than the complexity d we aim to certify—specifically, $d' \geq kd$ for some global constant k —these depth- d' circuits yield highly entangled projected states, which are, therefore, far from $\mathcal{FP}_P$. This provides a sample-efficient method for certifying the complexity of shallow-brickwork-circuit states. We summarize the result below, which generalizes to any finite D -dimensional circuit.

Proposition 2 (Certifying circuit complexity of random brickwork-circuit states). There exists a constant k such that, for a state ψ drawn from random $2D$ brickwork circuits with depth $d' \geq kd$, with probability at least 0.99, our protocols can certify that ψ has complexity C_2 (or C_2^{anc}) larger than d with a sample complexity of $\exp(\mathcal{O}(d^2))$ while achieving constant robustness.

Taken together, these two propositions establish the sample efficiency of our protocol for both generic quantum states and experimentally realizable states on near-term quantum platforms.

V. CERTIFYING QUANTUM ENTANGLEMENT

Entanglement is a fundamental feature of quantum mechanics, and certifying it has long been a central yet challenging task in quantum physics [10,18,83–85]. While fidelity-based witnesses are a powerful and widely used tool [4,84,86], they suffer from a major practical limitation: measuring fidelity typically requires global measurements, which are often experimentally prohibitive. Here, we demonstrate that our certification framework provides a highly efficient solution for certifying both bipartite and fully inseparable multipartite entanglement. By relying solely on local measurements, our approach substantially reduces the implementation complexity required to witness entanglement.

We begin by showing that entanglement across exponentially many bipartitions can be certified with constant sample complexity. We then tackle the more demanding task of certifying fully inseparable entanglement. Remarkably, we demonstrate an exponential improvement over prior methods, reducing the required sample complexity from linear to logarithmic in the system size for generic quantum states.

A. Bipartite entanglement

We first consider certifying entanglement across a bipartition $A|B$. In general, certifying bipartite entanglement is a daunting task [2,87,88]. Entanglement witnesses provide a powerful route: every entangled state admits a witness, which is very useful in experiments [84]. Nevertheless, designing witnesses using simple local measurements is highly nontrivial [26,89].

Our framework circumvents this obstacle by reducing global certification to a local entanglement witnessing task on a small subsystem. Let $A_1 \subset A$ and $B_1 \subset B$ be two small, disjoint subsystems. The key insight is that, if a state ρ is separable across $A|B$, then any state on A_1B_1 obtained by performing local measurements on the complement $R := [n] \setminus (A_1 \cup B_1)$ must also be separable. (Note the difference in notation adopted in this section: the system R corresponds to B in Algorithm 1 and A_1B_1 corresponds to A .) Therefore, for the property P of “entanglement across $A|B$,” the free projected-state set $\mathcal{FP}_P$ on A_1B_1 is precisely the set of separable states on A_1B_1 . We define the localizable entanglement between A_1 and B_1 as

$$\text{LE}_\psi(A_1, B_1) := \text{LQ}_{\text{Ent}(A,B)}(\psi), \quad (22)$$

making explicit its dependence on the chosen subsystems. By Theorem 1, if the target state $|\psi\rangle$ robustly preserves this resource—namely, if $\text{LE}_\psi(A_1, B_1) = \Omega(1)$ —then our protocol for certifying the bipartite entanglement is efficient.

Proposition 3 (Certifying bipartite entanglement). Consider two disjoint subsystems $A_1, B_1 \subseteq [n]$ of constant size, $n_{A_1}, n_{B_1} = \mathcal{O}(1)$. If the target state ψ satisfies

$$\text{LE}_\psi(A_1, B_1) = \Omega(1), \quad (23)$$

then Algorithm 1 certifies that ψ is entangled across any bipartition $A|B$ (with $A_1 \subseteq A, B_1 \subseteq B$) with $\mathcal{O}(\ln \delta^{-1})$ sample complexity while achieving constant robustness.

This condition of constant localizable entanglement is satisfied by broad classes of states. In particular, Propositions 1 and 2 establish this behavior for deep-thermalized states and random brickwork-circuit states, respectively, with $n_{A_1}, n_{B_1} = \mathcal{O}(1)$. Furthermore, Lemma 10 proves that, for Haar-random states, two-qubit subsystems ($A_1 = \{1\}$ and $B_1 = \{2\}$) already satisfy $\text{LE}_\psi(1, 2) = \Omega(1)$ with overwhelming probability.

Notably, if the protocol outputs **accept**, then we simultaneously certify entanglement of ρ across all bipartitions that separate A_1 and B_1 . Indeed, if ρ were separable across some bipartition $A|B$ with $A_1 \subseteq A$ and $B_1 \subseteq B$, then local measurements on R cannot create entanglement between A_1 and B_1 . Consequently, every projected state ρ_z on $A_1 \cup B_1$ would be separable, and the certification would output **reject**.

We remark that prior definitions of localizable entanglement [26,33,34] optimize over local measurement bases, whereas here we do not. Avoiding this optimization eliminates substantial classical optimizations and removes stringent device requirements such as adaptive local measurements, yielding a simple, nonadaptive protocol. The price to pay is that our fixed-basis approach may fail to certify certain families of states for which basis optimization is required—for example, the n -qubit Greenberger-Horne-Zeilinger state $(|0^n\rangle + |1^n\rangle)/\sqrt{2}$. Nevertheless, the

results above demonstrate that this fixed-basis localizable entanglement remains constant across generic and broadly applicable physical state ensembles.

It is also instructive to discuss the relationship between our witness and standard entanglement measures. The quantity Fid_P corresponds to the maximum singular value ($p_{\max}$) of the Schmidt decomposition of projected states ψ_z , which relates to the min-entropy of $(\psi_z)_{A_1}$ ($-\log p_{\max}$) rather than the standard entanglement entropy $S(\psi_z)$. While these two entropies can diverge for large systems, Proposition 3 targets small subsystems where $n_A = \mathcal{O}(1)$. In this regime, the difference between the two entropies is bounded by a constant factor, ensuring comparable performance in characterizing the entanglement of the projected states. On the other hand, the relation between $\widetilde{\text{LE}}_\psi(A_1, B_1)$ and the global entanglement entropy $S(\psi)$ may be weak, as global states with disparate entanglement entropy behaviors can exhibit similar localizable entanglement. Nonetheless, the entanglement entropy is notoriously difficult to measure experimentally [90]. In contrast, fidelity-based metrics hold significant operational relevance [91] and are frequently employed in experimental certification [4,84]. By measuring conditional fidelity solely with local measurements, our method significantly reduces the implementation complexity required for certification tasks based on global quantities.

Beyond its experimental simplicity, we now show that our framework also enables substantial reductions in sample complexity for certifying more complex entanglement structures.

B. Fully inseparable entanglement

We now address the more stringent task of certifying fully inseparable entanglement, where a state is entangled across every possible bipartition [36]. This structure is a key resource for quantum networks: it is the necessary and sufficient form of entanglement for activating genuine multipartite entanglement [25,49]. It also provides a meaningful benchmark for noisy devices aiming to implement quantum error correction [26]. Consequently, certifying fully inseparable entanglement offers a stringent test of entangling power and a stepping stone toward quantum networks and fault-tolerant quantum computing.

At first glance, certifying fully inseparable entanglement appears challenging, as one must rule out separability across exponentially many bipartitions. Nonetheless, Proposition 3 provides a path forward. It suffices to certify localizable entanglement between qubits i and $i+1$ for each $i \in [n-1]$. Indeed, if ρ were separable across some bipartition $A|B$, then there exists $i \in A$ satisfying $i+1 \in B$, and, therefore, the test on the pair $\{i, i+1\}$ would fail. A straightforward implementation that runs our protocol separately for every i would require $n-1$ distinct

experiments, yielding total sample complexity at least linear in n , similar to existing methods [26].

Here, we exponentially improve this scaling by decoupling the measurement scheme from the choice of pairs and reusing a single dataset across all tests, with the spirit underlying classical shadows [52]. Concretely, rather than measuring the complement of a specific pair in the computational basis, we perform single-qubit random Pauli measurements on all qubits. Data collection is, thus, independent of which pair will be tested in postprocessing. To leverage this dataset, we use the random-basis analog of Eq. (22):

$$\widetilde{\text{LE}}_\psi(A_1, B_1) := \widetilde{\text{LQ}}_{\text{Ent}(A_1|B_1)}(\psi). \quad (24)$$

Algorithm 1 extends directly to this random-basis setting: measure the complement R of $A_1 B_1$ in a random Pauli basis instead of the Z basis, and then estimate $\text{tr}(\psi_x \rho_x)$ and $\text{Fid}_P(\psi_x)$ on $A_1 \cup B_1$. Replacing the condition in Eq. (23) of Proposition 3 by $\widetilde{\text{LE}}_\psi(A_1, B_1) = \Omega(1)$ yields the same performance guarantees by using the random-basis variant of Algorithm 1.

Now, we show our modified protocol reduces the sample complexity from linear to logarithmic in n (proofs in Appendix D). Concretely, we collect a single dataset from T rounds of random Pauli measurements on ρ and reuse the same dataset to certify localizable entanglement for the $(n-1)$ pairs $A_1 = \{i\}, B_1 = \{i+1\}$ for $1 \leq i \leq n-1$. If all tests output **accept**, we certify fully inseparable entanglement. This protocol also extends to any set of $n-1$ pairs that connects the n -vertex graph.

Proposition 4 (Certifying fully inseparable entanglement with logarithmic sample complexity). Let ψ be a quantum state satisfying

$$\widetilde{\text{LE}}_\psi(i, i+1) = \Omega(1) \quad (25)$$

for all $1 \leq i \leq n-1$. Then, the fully inseparable entanglement of ψ can be certified with failure probability δ using $T = \mathcal{O}(\log n + \log \delta^{-1})$ samples, while achieving constant robustness.

For generic states, such as Haar-random states, the condition $\widetilde{\text{LE}}_\psi(i, i+1) = \Omega(1)$ holds simultaneously for all i with high probability (Appendix D, Lemma 10). To further demonstrate localizable entanglement in a physical setting, we evaluate its distribution across all nearest-neighbor pairs for random stabilizer states ψ up to hundreds of qubits, as presented in Fig. 4 (details provided in Appendix D). Here, i_p denotes the site index where $\widetilde{\text{LE}}_\psi(i_p, i_p+1)$ corresponds to the p th quantile of the distribution ($0 < p < 1$). We observe that the deviation between the maximum $\widetilde{\text{LE}}_\psi(i_0, i_0+1)$ and the minimum $\widetilde{\text{LE}}_\psi(i_1, i_1+1)$ is small, with the minimum concentrating consistently around 0.2. Furthermore, the variation across

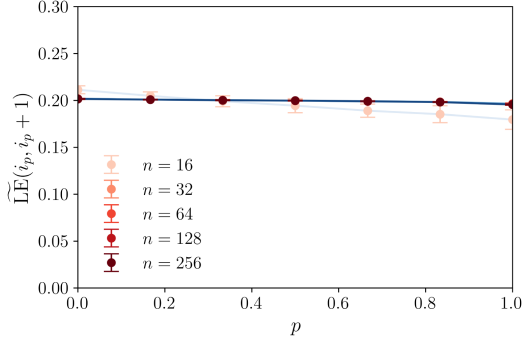


FIG. 4. Localizable entanglement $\widetilde{LE}_\psi(i_p, i_p + 1)$ for random stabilizer states ψ . Here, i_p denotes the site index corresponding to the p th quantile of the localizable entanglement across all sites. Error bars denote the standard deviation across the sampled states, which are negligible for large system sizes.

distinct random stabilizer states is negligible. These results further validate that our protocol provides a sample-efficient method for certifying this strong form of multipartite entanglement in generic quantum states.

C. Case study: Ground states of Hamiltonian systems

Building on the general result that the random-basis localizable entanglement $\widetilde{LE}_\psi$ can remain constant for generic many-body states, we now investigate this metric for ground states of concrete Hamiltonian models, thereby demonstrating the practical efficiency of our protocol.

We begin with the spin- $\frac{1}{2}$ XXZ chain, a paradigmatic and exactly solvable model of quantum magnetism with a rich phase diagram [92]. The XXZ chain has played an important role in entanglement theory [34,93,94] and serves as a key experimental benchmark on multiple platforms, including trapped ions [95] and optical cavities [96]. The Hamiltonian is

$$H_{XXZ} = - \sum_{i=1}^n [\sigma_x^i \sigma_x^{i+1} + \sigma_y^i \sigma_y^{i+1} + \Delta \sigma_z^i \sigma_z^{i+1}], \quad (26)$$

where Δ is the anisotropy, with periodic boundary condition $\sigma_\alpha^{n+1} \equiv \sigma_\alpha^1$. For a translational-invariant nondegenerate Hamiltonian, its unique ground state is also translational invariant, so $\widetilde{LE}_\psi(i, i + 1)$ is identical for all i . We numerically evaluate $\widetilde{LE}_\psi(1, 2)$ of the ground state ψ for system sizes up to $n = 64$ using the density matrix renormalization group (DMRG) algorithm [97]. Details of the numeric experiments are provided in Appendix D.

The results are shown in Fig. 5(a). We observe that $\widetilde{LE}_\psi(1, 2)$ remains nonvanishing throughout the critical regime $|\Delta| < 1$, with only mild finite-size drift as n increases. Notably, $\widetilde{LE}_\psi(1, 2)$ reaches maximal at the isotropic point $\Delta = -1$, at which the XXZ chain undergoes

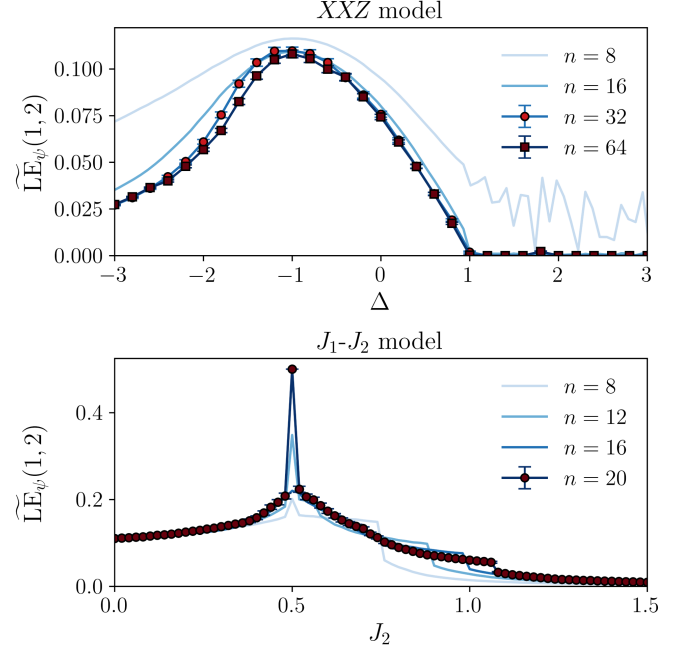


FIG. 5. Localizable entanglement $\widetilde{LE}_\psi(1, 2)$ in the ground states of Hamiltonian systems. Across broad parameter regimes, the localizable entanglement remains finite, enabling sample-efficient certification of entanglement. In addition, its behavior signifies key parameter points of the system.

a Kosterlitz-Thouless transition from gapped Néel anti-ferromagnet ($\Delta < -1$) to critical Luttinger liquid ($|\Delta| < 1$) [92]. Moreover, it vanishes at another phase transition point $\Delta = 1$ where the ground state becomes a product state for $\Delta > 1$. Therefore, the behavior of $\widetilde{LE}_\psi(1, 2)$ is able to indicate various phase transitions.

We next consider the spin- $\frac{1}{2}$ J_1 - J_2 Heisenberg chain, a paradigmatic frustrated extension of the nearest-neighbor model with next-nearest-neighbor couplings. Although not exactly solvable, in general, its key parameter points are well established: a fluid-dimer transition occurs at $J_2/J_1 \simeq 0.2411$ [98]; the exactly solvable Majumdar-Ghosh point $J_2/J_1 = \frac{1}{2}$ [99]; and, within the same phase, a Lifshitz point near $J_2/J_1 \approx 0.52$ [100]. The model captures the physics of zigzag-chain materials [101] and has been implemented on programmable superconducting platforms [102].

Concretely, with periodic boundary conditions, the Hamiltonian is

$$H_{J_1 J_2} = J_1 \sum_{i=1}^n \boldsymbol{\sigma}^i \cdot \boldsymbol{\sigma}^{i+1} + J_2 \sum_{i=1}^n \boldsymbol{\sigma}^i \cdot \boldsymbol{\sigma}^{i+2}, \quad (27)$$

where $\boldsymbol{\sigma}^i = (\sigma_x^i, \sigma_y^i, \sigma_z^i)$ and $\sigma_\alpha^{n+k} \equiv \sigma_\alpha^k$. Here, we set $J_1 = 1$ and consider an antiferromagnetic interaction $J_2 > 0$. For the ground state ψ , we evaluate the random-basis localizable entanglement $\widetilde{LE}_\psi(1, 2)$. The results are shown in Fig. 5(b).

At the Majumdar-Ghosh point $J_2/J_1 = \frac{1}{2}$, fluctuations in $\widetilde{\text{LE}}_\psi(1, 2)$ are from the twofold degeneracy of the ground space: in one ground state, sites 1 and 2 are maximally entangled, whereas in the other they are unentangled. Therefore, $\widetilde{\text{LE}}_\psi(1, 2)$ depends on the superposition coefficients of the two ground states. As J_2 increases from 0, $\widetilde{\text{LE}}_\psi(1, 2)$ grows and peaks near the Lifshitz point $J_2 \approx 0.52$ and then decreases for larger J_2 . Therefore, the Lifshitz point is signaled by the discontinuity in the first derivative of $\widetilde{\text{LE}}_\psi(1, 2)$. By contrast, we do not observe a clear signature near the phase transition $J_2/J_1 \simeq 0.2411$, and understanding which types of parameters can be captured by localizable entanglement is an interesting question [34].

One can find wide parameter regimes where $\widetilde{\text{LE}}_\psi(1, 2)$ is robustly bounded away from zero across both models. For nondegenerate Hamiltonians, translation invariance then implies $\widetilde{\text{LE}}_\psi(i, i+1) = \widetilde{\text{LE}}_\psi(1, 2) = \Omega(1)$ for all nearest-neighbor pairs. By Proposition 4, this yields logarithmic sample complexity and constant robustness for certifying fully inseparable entanglement in those Hamiltonian systems.

VI. CERTIFYING QUANTUM MAGIC

Here, we further demonstrate the power of our framework by applying it to certify quantum magic (or non-stabilizerness), a critical resource for fault-tolerant quantum computing [103–106]. Its characterization has recently received significant attention [30, 107–112]. Nonetheless, robust certification of this critical resource remains challenging. Existing protocols often lack soundness for mixed-state inputs or require demanding measurements [30, 109, 110]. We overcome these limitations and present the first protocol that certifies quantum magic using very few local measurements and achieves soundness for mixed states. Furthermore, it uses only constant sample complexity and achieves constant robustness.

A pure n -qubit stabilizer state can be written as $|\psi\rangle = C|0\rangle^{\otimes n}$, where C is a Clifford circuit acting on the initial all-zero state [113]. The set of free states—namely, the stabilizer set—is defined as the convex hull of stabilizer states:

$$\begin{aligned} \text{STAB}_n &:= \{\rho : \rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|, \\ &\text{with } p_i \geq 0, \sum_i p_i = 1, \\ &\text{and } |\psi_i\rangle = C_i|0\rangle^{\otimes n}, C_i \text{ Clifford}\}. \end{aligned} \quad (28)$$

A key feature of the stabilizer set is its closure under Pauli measurements [113]. Consequently, the free-projected set $\mathcal{FP}_P$ is simply the set of stabilizer states on A , denoted STAB_A . The maximal fidelity $\text{Fid}_P(\phi)$ then becomes the well-known stabilizer fidelity [104, 106]:

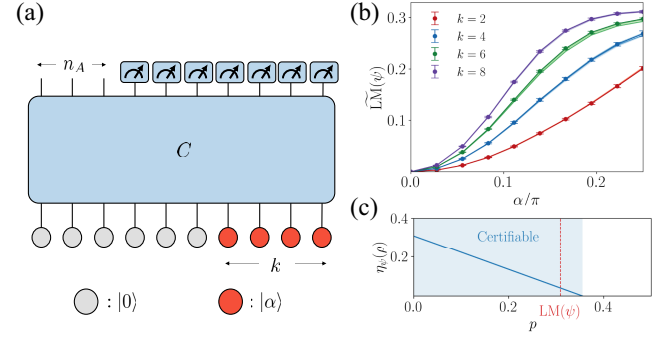


FIG. 6. Magic certification and its performance. (a) The system is initialized in the state $|0\rangle^{\otimes n-k} \otimes |\alpha\rangle^{\otimes k}$. A global random Clifford unitary C is then applied to scramble the injected magic. Finally, single-qubit Pauli measurements are performed on the complementary system, yielding projected states on the small n_A -qubit subsystem. (b) Localizable magic $\widetilde{\text{LM}}(\psi)$ with system size $n \in \{32, 64, 128, 256, 512\}$ for a fixed subsystem size $n_A = 3$ and varying numbers of injected magic state $k \in \{2, 4, 6, 8\}$. Darker colors correspond to larger system sizes. Each data point represents the average over five random Clifford realizations (each estimated using 1000 projected state samples), with error bars denoting the standard deviation across realizations. (c) The relation between global depolarizing noise strength p and $\eta_\psi(\rho)$ for $\rho = (1-p)\psi + pI/d$ with the same state ψ . The value of $\eta_\psi(\rho)$ remains in the certifiable regime for $p \gtrsim \text{LM}(\psi)$, demonstrating the strong robustness of our protocol.

$$\text{Fid}_P(\psi_z) = \max_{|\phi\rangle \in \text{STAB}_A} \langle \phi | \psi_z | \phi \rangle. \quad (29)$$

Let $\text{LM}(\psi) := \text{LQ}_{\text{Magic}}(\psi)$ denote the localizable magic of the target. By Theorem 1, if $n_A = \mathcal{O}(1)$ and $\text{LM}(\psi) = \Omega(1)$, then our protocol has constant sample complexity and robustness. We prove that this condition holds for typical Haar-random states with $n_A = 1$ in Appendix E. This condition is also expected for generic physical states: their projected ensemble on A is typically random states [37], which possess abundant quantum magic and require many layers of non-Clifford gates to prepare [114, 115]. Hence, our certification protocol is both efficient and robust for generic states.

However, in many practical scenarios, quantum magic is a scarce and costly resource. A crucial scenario involves the injection of magic into Clifford circuits [12, 50]. In near-term demonstration of fault-tolerant architectures, the quantum circuits are likely to be dominated by Clifford operations, with a limited number of logical T gates implemented via magic state distillation or cultivation [116]. To demonstrate the efficiency of our certification protocol for this practical setting, we consider and examine a magic-injection-and-scrambling model [Fig. 6(a)]. We initialize the system in a product state comprising $n - k$ single-qubit stabilizer states $|0\rangle$ and k magic states $|\alpha\rangle = 1/\sqrt{2}(|0\rangle + e^{i\alpha}|1\rangle)$, where $\alpha \in [0, \pi/4]$ and k

controls the amount of injected magic (with $\alpha = \pi/4$ yielding maximal magic). A random n -qubit Clifford unitary C is then applied to scramble the injected magic across the system. The resulting target state is given by

$$|\psi\rangle = C(|0\rangle^{\otimes n-k} \otimes |\alpha\rangle^{\otimes k}). \quad (30)$$

Following local Pauli measurements on the n_B -qubit subsystem B , the resulting projected states ψ_z are defined on the complementary subsystem A , which consists of $n_A = n - n_B$ qubits.

We first numerically evaluate the localizable magic $\widetilde{\text{LM}}(\psi)$ for a fixed subsystem size $n_A = 3$, varying the magic injection angle α , magic state count k , and the total system size n [Fig. 6(b)]. These simulations utilize established classical algorithms for T -doped Clifford circuits and stabilizer fidelity estimation [66,104]. The data reveal several key features. First, $\widetilde{\text{LM}}(\psi)$ increases with k , demonstrating that global magic is effectively concentrated into the subsystem A , an insight that underlies protocols like magic-state injection. Second, and most importantly for our purposes, $\widetilde{\text{LM}}(\psi)$ quickly exceeds a constant threshold as α increases. This implies that, for a fixed random Pauli basis, the localizable magic $\widetilde{\text{LM}}(\psi)$ exceeds a constant with high probability. According to Theorem 1, this directly shows that our protocol certifies magic in these states with constant sample complexity and robustness. It is also interesting that $\widetilde{\text{LM}}$ increases monotonically with α , suggesting that the projected-ensemble-averaged magic faithfully reflects, to a significant extent, the total magic of the full state. Such a magic concentration phenomenon has likewise been observed in Refs. [12,117]. We remark that $\widetilde{\text{LM}}(\psi)$ is not a magic monotone, as it can change under the addition of ancillary $|0\rangle$ qubits and Clifford rotations. Nevertheless, it serves as a practical indicator of the global magic contained in the state.

To further demonstrate robustness, we simulate our protocol on a state subject to global depolarizing noise, $\rho = (1-p)\psi + pI/d$, a good model for present-day experiments [118]. Moreover, coherent errors can be converted into effective depolarizing noise via randomized compiling [119,120]. Figure 6(c) plots $\eta_\psi(\rho)$ versus the noise strength p for a 512-qubit state generated with $\alpha = \pi/4$. As shown, the conditional fidelity $\eta(\rho)$ remains well above zero even for substantial noise levels $p \approx 0.35$. This behavior can also be derived analytically:

$$\begin{aligned} \eta_\psi(\rho) &= (1-p)\text{LM}(\psi) + p d^{-1} \left[\sum_z (1 - d_A \text{Fid}_P(\psi_z)) \right] \\ &= (1-p)\text{LM}(\psi) + p \left[d_A^{-1} - d_B^{-1} \sum_z \text{Fid}_P(\psi_z) \right]. \end{aligned} \quad (31)$$

By adjusting the decision boundary to require $\eta^* < \eta_\psi(\rho)$, our protocol could certify the magic in ρ whenever $\eta_\psi(\rho) > 0$, which holds provided

$$p < \frac{\text{LM}(\psi)}{d_B^{-1} \sum_z \text{Fid}_P(\psi_z) + \text{LM}(\psi) - d_A^{-1}} \approx \frac{\text{LM}(\psi)}{1 - d_A^{-1}}, \quad (32)$$

consistent with the numerical simulation. Here, the approximation uses the empirical observation $\text{LM}(\psi) \approx 1 - d_B^{-1} \sum_z \text{Fid}_P(\psi_z)$. This level of robustness is much better than a direct application of Theorem 1, showing that robustness can be improved in realistic noise scenarios. Moreover, the monotonic decrease of $\eta_\psi(\rho)$ with increasing noise strength directly highlights the utility of our protocol for benchmarking noisy quantum devices.

VII. CERTIFYING QUANTUM STATE FIDELITY USING RANDOM-BASIS-ENHANCED CONDITIONAL FIDELITY

We now address a particularly strong certification task: certifying the global state fidelity $\langle \psi | \rho | \psi \rangle$. Recent protocols achieve this using only local measurements [27–29,51], but they face severe trade-offs between experimental simplicity and certification power. Adaptive protocols can, in principle, certify arbitrary states [28]. For Haar-random states, recent adaptive local-measurement protocols have achieved a sample complexity of $\mathcal{O}[(\log n)^2]$ and a robustness of $\Omega(1/\log n)$ [51]. However, employing adaptive protocol requires challenging classical feedback and long-lived quantum memory to store the state between measurement rounds [28,29,51]. Reference [51] also demonstrated that constant scaling is achievable, but doing so required nonlocal measurements across $\mathcal{O}(\log n)$ qubits.

By contrast, protocols that employ nonadaptive local measurement schemes are far more compatible with near-term hardware. However, state-of-the-art nonadaptive methods for generic states, such as the shadow-overlap protocol, exhibit $\mathcal{O}(n^4)$ sample complexity and $\Omega(n^{-2})$ noise robustness, and this sample complexity can improve to $\mathcal{O}(n^2)$ only by using adaptive measurements [27]. Consequently, whether constant robustness and sample complexity can be achieved for generic states using solely nonadaptive local measurements has remained a central open challenge in the field.

Here, we show that our enhanced conditional fidelity protocol settles this problem. Relying solely on nonadaptive single-qubit Pauli measurements, it achieves $\mathcal{O}(1)$ sample complexity and $\Omega(1)$ robustness for certifying generic states, including both Haar-random states and physically relevant random graph states. By achieving essentially optimal scaling guarantees, our protocol provides a definitive resolution to this open challenge in quantum certification.

A. Random-basis-enhanced conditional fidelity

Our previous conditional fidelity mainly focuses on measuring subsystem B in a single, fixed basis (e.g., the computational basis), which is insufficient for fidelity certification: the product state $|\psi_{0^{n_B}}\rangle_A \otimes |0^{n_B}\rangle_B$ achieves unit conditional fidelity even though its global fidelity with $|\psi\rangle$ could be exponentially small in n_B . The core issue is that a fixed measurement basis on B fails to capture the rich correlations across the $A|B$ partition, which are revealed only in other bases (e.g., the relative phases among the projected states).

Our solution is to measure subsystem B in randomly chosen single-qubit Pauli bases. The intuition is that random basis choices produce projected states on subsystem A that are closely correlated with one another, so the conditional fidelity captures the global fidelity structure and becomes a sensitive witness of the overall state fidelity. To formalize this idea, we define the following observable:

$$O_\psi = 3^{-n_B} \sum_{x \in X^{n_B}, \bar{p}(x) \neq 0} |\psi_x\rangle\langle\psi_x|_A \otimes |x\rangle\langle x|_B. \quad (33)$$

By construction, $\text{tr}(O_\psi \psi) = 1$. The ability to certify fidelity is determined by the spectral gap

$$\Delta(O_\psi) := 1 - \max_{\phi \perp \psi} \text{tr}(O_\psi \phi), \quad (34)$$

as shown in the following.

Proposition 5 (Certifying state fidelity with local Pauli measurements). Let ψ be the target state with $\Delta(O_\psi) > 0$, and fix parameters $0 < c < 1/2$, $0 < F < 1$, and $\delta > 0$. Then, using local Pauli measurements on

$$T = \frac{27 \ln(\delta^{-1})(4^{n_A} + 1)}{c^2 \Delta^2 (1 - F)^2} \quad (35)$$

samples of ρ suffices to

- (1) output **reject** with probability at least $1 - \delta$ when $\text{tr}(\rho \psi) \leq F$; and
- (2) output **accept** with probability at least $1 - \delta$ when $\text{tr}(\rho \psi) \geq 1 - (1 - 2c)\Delta(1 - F)$.

Therefore, a larger spectral gap Δ directly improves both sample complexity and robustness. While the gap can vanish for certain target states (e.g., product states across $A|B$), we now show that it is typically bounded below by a constant for generic families of states of interest.

B. Provable constant gap for random graph states

We first prove that our protocol achieves a constant gap for random graph states, providing a natural and robust benchmark for evaluating its performance. Graph states form a canonical and widely used subclass of stabilizer states, serving as standard resources in quantum computation and quantum networks [75,121,122]. Moreover,

every stabilizer state is local-Clifford equivalent to a graph state [113,122], making graph states a representative family for studying generic phenomena for stabilizer states.

Specifically, let $G = (V, E)$ be a simple undirected graph on n vertices $V = \{1, \dots, n\}$ with symmetric adjacency matrix $A \in \mathbb{F}_2^{n \times n}$ with zero diagonal entries. The associated n -qubit graph state $|G\rangle$ is given by $|G\rangle = (\prod_{i < j} CZ_{i,j}^{A_{i,j}})|+\rangle^{\otimes n}$. We consider the random graph state ensemble obtained by sampling A uniformly from the set of all symmetric, zero-diagonal matrices. Our main theorem for this ensemble is the following.

Theorem 4 (Constant gap for random graph states). Let $|\psi\rangle$ be drawn uniformly from n -qubit graph states, and let $n_A = 1$. Then, with probability $1 - \exp[-\Omega(n)]$, $\Delta(O_\psi) = \Omega(1)$.

Proof sketch. For a target stabilizer state ψ , the observable O_ψ has eigenstates in the form $E|\psi\rangle$, where E is a Pauli error. Consequently, bounding the second-largest eigenvalue of O_ψ reduces to showing that every Pauli error on ψ can be localized on system A via the random measurements on B and, therefore, be detected by the conditional fidelity. We further reduce this problem to a random linear-algebra problem induced by the random adjacency matrix A , and prove this is indeed the case. The detailed proof is given in Appendix F. ■

Our result of random graph states directly implies the same constant-gap behavior for the corresponding ensemble of random stabilizer states via local Clifford rotations, as these rotations preserve randomized Pauli measurements up to relabeling. While efficient local certification protocols have been previously established for graph states [22,123,124], these methods require target-specific measurements of the corresponding stabilizer operators. To our knowledge, this is the first proof that state-independent local random Pauli measurements suffice to certify generic stabilizer states with constant sample complexity and robustness. Because our approach does not require prior knowledge of the target state before measurement data collection, a single dataset of local Pauli measurements can be reused to certify many target stabilizer states simultaneously.

We remark that prior analyses of nonadaptive local certification have mainly focused on Haar-random target states [27]. Our Theorem 4 already gives a constant-gap guarantee for a physically motivated and efficiently preparable non-Haar ensemble. This shows that constant-gap behavior is not restricted to highly random ensembles but can arise in physically relevant states.

C. Provable constant gap for almost all states

We now establish the performance guarantees for generic pure states. We focus first on Haar-random states, which benchmark the average-case performance of our protocol across the entire Hilbert space. While we show in

Appendix F that the spectral gap $\Delta(O_\psi)$ is strictly positive almost surely, efficient certification demands a much stronger condition. Specifically, an exponentially small positive gap would still yield poor robustness and prohibitive sample complexity. Our main fidelity theorem overcomes this by proving that, for all but an exponentially small fraction of states, the spectral gap is strictly lower bounded by a constant.

Theorem 5 (Constant gap for almost all states). Let $|\psi\rangle$ be drawn Haar randomly from the n -qubit Hilbert space $\mathcal{H}_d$ with $d = 2^n$ and $n_A \geq 1$. Then, with probability $1 - \exp[-\Omega(n)]$, $\Delta(O_\psi) = \Omega(1)$.

Proof sketch. It suffices to consider $n_A = 1$, since, for any one-qubit subsystem $A_1 \subseteq A$, one has $O_{\psi,A} \leq O_{\psi,A_1}$ and, hence, $\Delta(O_{\psi,A}) \geq \Delta(O_{\psi,A_1})$. Let the target state $|\psi\rangle$ and an orthogonal input pure state $|\phi\rangle$ be decomposed as $|\psi\rangle = |0\rangle|u\rangle + |1\rangle|v\rangle$ and $|\phi\rangle = |0\rangle|a\rangle + |1\rangle|b\rangle$, where the first qubit corresponds to subsystem A . For each random Pauli measurement outcome $\mathbf{x}$ on subsystem B , we denote the projected amplitudes as $u_{\mathbf{x}} = \langle \mathbf{x}|u\rangle$, and define $v_{\mathbf{x}}$, $a_{\mathbf{x}}$, and $b_{\mathbf{x}}$ analogously. The spectral gap can then be expressed as

$$\langle \phi|(I - O_\psi)|\phi\rangle = \sum_{\mathbf{x} \in \mathcal{X}^{n_B}} 3^{-n_B} \frac{|u_{\mathbf{x}}b_{\mathbf{x}} - v_{\mathbf{x}}a_{\mathbf{x}}|^2}{|u_{\mathbf{x}}|^2 + |v_{\mathbf{x}}|^2}. \quad (36)$$

By introducing two positive semidefinite operators, H_0 and H_1 [defined in Eq. (F83)], we apply the Cauchy-Schwarz inequality to lower bound Eq. (36) by the ratio $\langle \phi|H_0|\phi\rangle^2 / \langle \phi|H_1|\phi\rangle$. Using Gaussian random matrix concentration inequalities and the Wick integration formula for Gaussian random variables, we prove that, with probability $1 - \exp[-\Omega(n)]$, the following conditions hold simultaneously:

$$\begin{aligned} \ker(H_0) &= \text{span}\{|\psi\rangle\}, \\ \lambda_{\min}^+(H_0) &= \Omega(2^{-n}), \\ \|H_1\| &= \mathcal{O}(2^{-2n}). \end{aligned} \quad (37)$$

The dimensional scaling factors exactly cancel in this ratio, yielding a constant lower bound of $\Omega(1)$. The complete proof is provided in Appendix F. ■

Combining Theorem 5 and Proposition 5 establishes that, for any chosen parameter $c < 1/2$, a given fidelity F can be certified using $\mathcal{O}(1)$ samples for all but a $2^{-\Omega(n)}$ fraction of pure states. Moreover, this approach tolerates an infidelity of $(1 - 2c)\Delta(1 - F) = \Omega(1)$. This performance substantially improves upon previous protocols requiring $\mathcal{O}(n^4)$ samples and $\Omega(n^{-2})$ robustness [27].

To test whether this behavior persists for more experimentally accessible targets, we evaluated the practical performance of our protocol using numerical simulations on physically relevant, non-Haar states. We sampled

$N_s = 50$ states $\{\psi_j\}_{j=1}^{N_s}$ generated by local quantum circuits of depth $10n$. The depth is chosen so that the states are far from Haar-random states, whose preparation requires exponentially deep circuits. To estimate the spectral gap of O_ψ for these states, we draw $N_M = 100$ random local Pauli bases $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_{N_M} \in \{X, Y, Z\}^{n_B}$ and define the truncated observable

$$\begin{aligned} O_\psi^{(i)} &= \frac{1}{i} \sum_{j=1}^i \sum_{\mathbf{z}: \bar{\mathbf{p}}[\mathbf{x}(\mathbf{b}_j, \mathbf{z})] \neq 0} |\psi_{\mathbf{x}(\mathbf{b}_j, \mathbf{z})}\rangle \langle \psi_{\mathbf{x}(\mathbf{b}_j, \mathbf{z})}|_A \otimes |\mathbf{x}(\mathbf{b}_j, \mathbf{z})\rangle \\ &\quad \times \langle \mathbf{x}(\mathbf{b}_j, \mathbf{z})|_B, \end{aligned} \quad (38)$$

where $1 \leq i \leq N_M$ and $\mathbf{x}(\mathbf{b}_j, \mathbf{z}) \in \mathcal{X}^{n_B}$ denotes the basis state corresponding to measurement outcome $\mathbf{z}$ in basis $\mathbf{b}_j$. The previously defined O_ψ is recovered in the limit $i \rightarrow \infty$. For $n_A = 1$, we compute the averaged spectral gap

$$\bar{\Delta}_i = \frac{1}{N_s} \sum_{j=1}^{N_s} \Delta(O_{\psi_j}^{(i)}) \quad (39)$$

over the sampled random states and plot the results in Fig. 7(a). As i increases, $\bar{\Delta}_i$ grows, indicating that the average gap $\bar{\Delta}_\infty = \Delta(O_\psi)$ exceeds $\bar{\Delta}_{N_M}$; thus, $\bar{\Delta}_{N_M}$ gives a good empirical lower bound of $\Delta(O_\psi)$.

As shown in Fig. 7(a), the averaged gap rapidly increases and approaches a stable value as more local basis patterns are included. Furthermore, Fig. 7(b) shows that the finite-basis gap remains bounded away from zero over the accessible system sizes, in sharp contrast with the decreasing shadow-overlap gap [27]. These data clearly indicate that the constant-gap phenomenon established in Theorem 5 is not restricted to Haar-random states but extends robustly to physically generated states. While enlarging n_A can further increase the spectral gap, thereby improving robustness, it also increases estimator variance as $\mathcal{O}(4^{n_A})$, yielding a trade-off in sample complexity. The ability to maintain a large constant gap shows that our protocol is highly practical for certifying and benchmarking intermediate-scale components of near-term devices, using significantly fewer quantum resources while tolerating larger device imperfections.

VIII. DISCUSSION AND OUTLOOK

In this work, we introduced the physical principle of localizable quantumness and developed a conditional fidelity certification framework, establishing a powerful approach for certifying central quantum properties. By relying only on state-independent, nonadaptive local Pauli measurements, our protocols guarantee mixed-input soundness while yielding substantial improvements in both robustness and sample complexity. Crucially, we resolved the open challenge regarding state fidelity certification by proving that a strictly constant spectral gap, $\Delta(O_\psi) = \Omega(1)$, and, hence, robust certification with constant sample

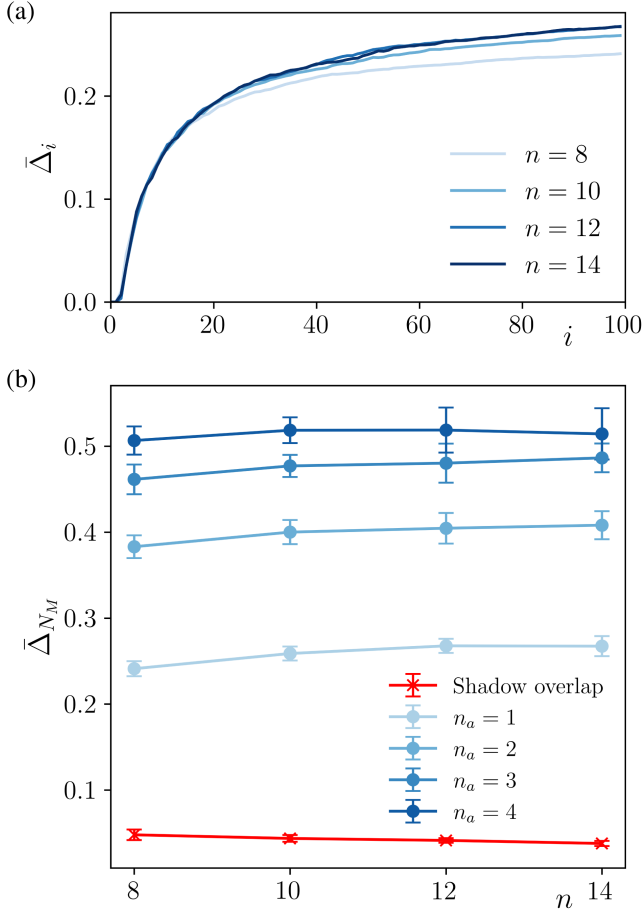


FIG. 7. Spectral gaps of conditional-fidelity observables. (a) The average spectral gap $\bar{\Delta}_i := (1/N_s) \sum_{j=1}^{N_s} \Delta(O_{\psi_j}^{(i)})$ for $1 \leq i \leq N_M = 100$ random bases increases with i , indicating that the limit O_ψ (as $i \rightarrow \infty$) has a larger average gap than $\bar{\Delta}_{N_M}$. (b) $\bar{\Delta}_{N_M}$ versus n (error bars show the standard deviation across states). Here, $\bar{\Delta}_{N_M}$ serves as a proxy for $\bar{\Delta}_\infty$, suggesting that the average spectral gap of O_ψ remains $\Omega(1)$ as n grows. Moreover, $\bar{\Delta}_{N_M}$ increases with n_A , enhancing the protocol's robustness. For comparison, the shadow-overlap protocol exhibits a smaller spectral gap that decays with n .

complexity, is achievable for generic quantum states via local measurements. Consequently, our unified framework achieves optimal, constant-sample-complexity scaling for certifying a broad range of many-body properties. While our current circuit-complexity witnesses primarily target relatively shallow circuits, measurements are known to concentrate exponentially large circuit complexity into small subsystems [43]. Harnessing this complexity concentration phenomenon to design sample-efficient witnesses for highly complex, deep circuits represents a compelling direction for future research.

Localizable quantumness offers a unifying lens on several previously established effects. For example, complexity concentration [43], localizable entanglement [33,34], magic concentration [12,117,125], and magic-state

injection [50] can all be viewed as special cases in which a global resource localizes into a small subsystem after local projective measurements on the complement. This highlights the broader significance of projected-ensemble properties such as LQ_P and their potential applications and impact on resource theories and many-body physics. In condensed matter physics, it is especially compelling to study order parameters and phases through the lens of localizable quantumness [126]. Another exciting direction is to develop a theory of localizable magic, paralleling localizable entanglement [33], as a tool to probe quantum many-body magic.

Extending localizable quantumness to mixed states and developing protocols that certify mixed-state properties, especially mixed-state entanglement and magic, represent especially promising directions. Recent work also shows that, with tolerable additional overhead, one can obtain good bounds on nonlinear quantities of the projected ensemble, enabling powerful certifications such as emergent quantum state designs [42]. It is therefore compelling to investigate whether nonlinear projected-ensemble quantities can certify stronger quantum properties or yield sharper, more powerful property-detection criteria.

More broadly, our approach complements and extends existing paradigms for certification and estimation such as direct fidelity estimation [21] and randomized measurements [52,127] by showing that simple local measurements can certify global properties with favorable scaling. A particularly promising avenue for future work is to tailor our method to other physical platforms, leveraging native, low-overhead measurements to certify key properties—for example, nonclassicality in bosonic systems [128] and non-Gaussianity in fermionic systems [129,130].

Parts of the numerical results were obtained using the ITensor [131] and Qiskit [132] software packages.

ACKNOWLEDGMENTS

We are grateful to Zhenhuan Liu and Muzhou Ma for insightful discussions in the early stages of this project. We thank Shuo Yang for helpful suggestions on the numerical experiments. This work is supported by the National Natural Science Foundation of China (Grant No. 12575023), the Quantum Science and Technology-National Science and Technology Major Project (Grants No. 2021ZD0300804 and No. 2021ZD0300702), the CCF-QuantumCtek Superconducting Quantum Computing Special Cooperation Program (Grant No. CCF-QC2025005), and the Turing AI Institute of Nanjing. Z.-W.L. is supported in part by NSFC under Grant No. 12475023, Dushi Program, and a startup funding from YMSC.

DATA AVAILABILITY

The data that support the findings of this article are openly available [133].

APPENDIX A: ADDITIONAL ANALYSIS ON THE PERFORMANCE OF ALGORITHM 1

In this appendix, we analyze the performance of Algorithm 1. We first collect the statistical tools used throughout our work, including local shadow tomography, standard concentration inequalities, and the median-of-means estimator. We then establish the performance guarantee based on those tools.

$$\left\{ \frac{1}{3} |+\rangle\langle+|, \frac{1}{3} |-\rangle\langle-|, \frac{1}{3} |+\rangle\langle+i|, \frac{1}{3} |+\rangle\langle-i|, \frac{1}{3} |0\rangle\langle 0|, \frac{1}{3} |1\rangle\langle 1| \right\}. \quad (\text{A1})$$

Suppose the POVM yields measurement outcomes $\mathbf{x} \in \mathbf{X}^k$. The classical shadow estimator for $\text{tr}(O\rho)$ is given by

$$\omega = \text{tr} \left\{ O \left[\bigotimes_{i \in [k]} (3|\mathbf{x}_i\rangle\langle\mathbf{x}_i| - I_i) \right] \right\}. \quad (\text{A2})$$

This estimator is unbiased:

$$\mathbb{E}[\omega] = \text{tr}(O\rho), \quad (\text{A3})$$

and its variance is bounded by

$$\text{Var}[\omega] \leq 4^k \|O\|_2^2. \quad (\text{A4})$$

Crucially, ω uses only a single copy of ρ , which is essential for estimating ensemble-averaged local fidelities in our protocol.

Lemma 4. Let $\mathbf{z} \sim p$ and ω be a random variable such that $\mathbb{E}[\omega|\mathbf{z}] = o_{\mathbf{z}} \geq 0$ and $\text{Var}[\omega|\mathbf{z}] \leq \sigma^2$ for all $\mathbf{z}$. Then, $\mathbb{E}[\omega] = \sum_{\mathbf{z}} p(\mathbf{z}) o_{\mathbf{z}}$ and $\text{Var}[\omega] \leq \sigma^2 + \max_{\mathbf{z}} |o_{\mathbf{z}}|^2$.

Proof. The proof is from the laws of total expectation and variance:

$$\begin{aligned} \mathbb{E}\omega &= \mathbb{E}_{\mathbf{z}} \mathbb{E}[\omega|\mathbf{z}] \\ &= \sum_{\mathbf{z}} p(\mathbf{z}) o_{\mathbf{z}}, \\ \text{Var}[\omega] &= \mathbb{E}_{\mathbf{z}} \text{Var}[\omega|\mathbf{z}] + \text{Var}_{\mathbf{z}} \mathbb{E}[\omega|\mathbf{z}] \\ &\leq \mathbb{E}_{\mathbf{z}} \sigma^2 + \text{Var}_{\mathbf{z}} o_{\mathbf{z}} \\ &\leq \sigma^2 + \max_{\mathbf{z}} |o_{\mathbf{z}}|^2. \end{aligned} \quad (\text{A5})$$

This enables unbiased estimation of projected-ensemble-averaged linear quantities [42]. Combining the lemma with the variance bound in Eq. (A4) yields the following guarantee for estimating conditional fidelities.

Corollary 4 (Variance of conditional fidelity). Let an n -qubit state ρ be partitioned as $A \cup B$, and measure B in the computational basis to obtain $\mathbf{z}$ with probability $p_{\rho}(\mathbf{z})$ and postmeasurement state $\rho_{\mathbf{z}}$ on A . Construct ω by

1. Local classical shadow

We briefly review the local classical shadow protocol [52]. For a given k -qubit input state ρ , the protocol performs random single-qubit Pauli measurements in the X , Y , or Z basis independently on each qubit. This is equivalent to applying a POVM composed of six elements:

applying local classical shadows on $\rho_{\mathbf{z}}$ to estimate $\text{tr}(\psi_{\mathbf{z}} \rho_{\mathbf{z}})$. Then, $\mathbb{E}[\omega] = \sum_{\mathbf{z}} p_{\rho}(\mathbf{z}) \text{tr}(\psi_{\mathbf{z}} \rho_{\mathbf{z}})$ and $\text{Var}[\omega] \leq 4^{n_A} + 1$.

2. Median-of-means estimator

The median-of-means estimator is a standard statistical method that uses medians to suppress the contribution of outlier estimators, which has the benefit of exponentially suppressing the failure probability. We first introduce Hoeffding's inequality, which is useful for bounded-value estimators.

Proposition 6 (Hoeffding's inequality, Theorem 8 in Ref. [8]). Let $\{\omega_i\}_{i=1}^T$ be i.i.d. random variables with $a_i \leq \omega_i \leq b_i$, and define $S_T := \sum_{i=1}^T \omega_i$. For any $t > 0$,

$$\Pr[S_T - \mathbb{E}[S_T] \geq t] \leq \exp \left[-\frac{2t^2}{\sum_{i=1}^T (b_i - a_i)^2} \right]. \quad (\text{A6})$$

Then, we introduce the median-of-means estimator.

Proposition 7 (Median-of-means estimator). Let $T = BK$ and $\{\omega_i\}_{i=1}^T$ be i.i.d. random variables with mean μ and variance σ^2 . For each block $l \in \{1, \dots, K\}$ define the empirical mean

$$o_l := \frac{1}{B} \sum_{i=(l-1)B+1}^{lB} \omega_i, \quad (\text{A7})$$

and let $\omega = \text{median}\{o_1, o_2, \dots, o_K\}$. Fix $\delta \in (0, 1)$ and $\varepsilon > 0$. By choosing $B = (6\sigma^2/\varepsilon^2)$ and $K = \frac{9}{2} \ln(\delta^{-1})$, we have that

$$\Pr[|\omega - \mu| \geq \varepsilon] \leq \delta. \quad (\text{A8})$$

Equivalently, with probability at least $1 - \delta$,

$$|\omega - \mu| < \sigma \sqrt{\frac{27 \ln(\delta^{-1})}{T}}. \quad (\text{A9})$$

Proof. For each block mean o_l , we have $\mathbb{E}[o_l] = \mu$ and $\text{Var}[o_l] = \sigma^2/B = \varepsilon^2/6$. By Chebyshev's inequality,

$$\Pr[|o_l - \mu| \geq \varepsilon] \leq \frac{\text{Var}[o_l]}{\varepsilon^2} = \frac{1}{6}. \quad (\text{A10})$$

Define the indicator $\tilde{o}_l := \mathbf{1}[|o_l - \mu| \geq \varepsilon]$, and then $\mathbb{E}[\tilde{o}_l] \leq 1/6$ and $0 \leq \tilde{o}_l \leq 1$. Applying Proposition 6 to $\sum_{l=1}^K \tilde{o}_l$, we have that

$$\begin{aligned} \Pr[|\omega - \mu| \geq \varepsilon] &\leq \Pr\left[\sum_{i=1}^K \tilde{o}_i \geq \frac{K}{2}\right] \\ &\leq \Pr\left[\sum_{i=1}^K \tilde{o}_i - \mathbb{E}\left[\sum_{i=1}^K \tilde{o}_i\right] \geq \frac{K}{3}\right] \\ &\leq \exp\left[-\frac{2(\frac{K}{3})^2}{K}\right] = \delta, \end{aligned} \quad (\text{A11})$$

completing the proof. $\blacksquare$

3. Proof of Theorem 1

a. Soundness

For any property-free state $\rho \in \mathcal{F}_P$, we have $\eta_\psi(\rho) \leq 0$ by Lemma 1. Moreover, $\mathbb{E}[\omega_i - \text{Fid}_P(\psi_{z_i})] = \eta_\psi(\rho)$. Applying the median-of-means estimator (Proposition 7) to T independent estimates $\{\omega_i - \text{Fid}_P(\psi_{z_i})\}_{i=1}^T$ yields a final estimator ω satisfying

$$|\omega - \eta_\psi(\rho)| < \sigma \sqrt{\frac{27 \ln(\delta^{-1})}{T}} \quad (\text{A12})$$

with probability at least $1 - \delta$, where $\sigma^2 = 4^{n_A} + 1$ by Corollary 4. With the choice of T in Eq. (12), we obtain, with probability at least $1 - \delta$,

$$\omega < \eta_\psi(\rho) + \text{LQ}_P(\psi)/3 \leq \eta^*, \quad (\text{A13})$$

So the protocol outputs **reject**.

b. Completeness

Since the experimental state ρ is ε -close to the ideal state ψ in trace distance, expectation values of bounded observables are also close, ensuring that $\eta_\psi(\rho)$ is close to the ideal value. Specifically, for a given ρ satisfying $d_{\text{tr}}(\rho, \psi) \leq \varepsilon$, we have that

$$\begin{aligned} \eta_\psi(\rho) &= \text{tr}[O_P(\psi)\psi] + \text{tr}[O_P(\psi)(\rho - \psi)] \\ &\geq \text{LQ}_P(\psi) - \|O_P(\psi)\|_\infty \|\rho - \psi\|_1 \\ &\geq \text{LQ}_P(\psi) - 2d_{\text{tr}}(\rho, \psi) \\ &\geq \frac{2}{3} \text{LQ}_P(\psi). \end{aligned} \quad (\text{A14})$$

Choosing T as in Eq. (12) ensures

$$\omega > \eta_\psi(\rho) - \frac{\text{LQ}_P(\psi)}{3} \geq \eta^* \quad (\text{A15})$$

with probability at least $1 - \delta$. $\blacksquare$

APPENDIX B: ADDITIONAL PROOFS ON COMPLEXITY CERTIFICATION

1. Proof of Lemma 2: Entanglement of low-complexity states

Proof. Because $C_2(\phi) \leq d$, the state $|\phi\rangle$ can be prepared from $|0\rangle^{\otimes n}$ by a two-dimensional depth- d circuit

$$U = \prod_{i=1}^d \left(\bigotimes_j V_{i,j} \right), \quad (\text{B1})$$

where the gates $\{V_{i,j}\}_j$ in the i th layer act on disjoint pairs of nearest-neighbor qubits or on single qubits. Define the backward light cone of the subsystem B layer by layer:

$$\begin{aligned} \mathcal{L}_{B,d+1} &= B, \\ \mathcal{L}_{B,i} &= \mathcal{L}_{B,i+1} \\ &\cup [\cup \{\text{supp}(V_{i,j}) | \text{supp}(V_{i,j}) \cap \mathcal{L}_{B,i+1} \neq \emptyset\}]. \end{aligned} \quad (\text{B2})$$

Thus, $\mathcal{L}_{B,1}$ contains all qubits that can interact with B through at most d layers. By construction of L_1 and R_1 (see Fig. 3),

$$(\mathcal{L}_{B,1} \cap L) \subseteq L_1, \quad (\mathcal{L}_{B,1} \cap R) \subseteq R_1. \quad (\text{B3})$$

The unitary V is defined as the product of all gates whose supports lie outside the backward light cone of B :

$$V = \prod_{i=1}^d \left(\bigotimes_{\text{supp}(V_{i,j}) \not\subseteq \mathcal{L}_{B,i}} V_{i,j} \right). \quad (\text{B4})$$

The remaining two-qubit gates define the unitary

$$W = \prod_{i=1}^d \left(\bigotimes_{\text{supp}(V_{i,j}) \subseteq \mathcal{L}_{B,i}} V_{i,j} \right). \quad (\text{B5})$$

By construction, $U = VW$, and V acts only on subsystem A . Consequently, V commutes with the operator $\langle z|_B \otimes I_A$ for every measurement outcome $z \in \{0, 1\}^{n_B}$. The unnormalized projected state can, therefore, be written as

$$\begin{aligned} |\tilde{\phi}_z\rangle &= (\langle z|_B \otimes I_A) |\phi\rangle \\ &= (\langle z|_B \otimes I_A) VW|0\rangle_{AB} \\ &= V(\langle z|_B \otimes I_A) W|0\rangle_{AB}. \end{aligned} \quad (\text{B6})$$

Equation (B3) implies that W acts nontrivially only on BL_1R_1 . Consequently,

$$\begin{aligned} V(\langle z|_B \otimes I_A)W|0\rangle_{AB} &= V[(\langle z|_B|\phi_1\rangle_{BL_1R_1})|0\rangle_{L_2R_2}] \\ &= V(|\tilde{\phi}\rangle_{L_1R_1}|0\rangle_{L_2R_2}). \end{aligned} \quad (\text{B7})$$

Normalizing this state, we obtain

$$|\phi_z\rangle = V(|\varphi\rangle_{L_1R_1} \otimes |0\rangle_{L_2R_2}). \quad (\text{B8})$$

The circuit V has depth d , and in each layer at most $2w$ two-qubit gates can cross the cut $L|R$, so at most $2wd$ such gates appear in total. Each gate increases the bipartite entanglement entropy by at most 2 (Lemma 4 in Ref. [134]). Hence,

$$\begin{aligned} E_{L|R}(\phi_z) &\leq E_{L|R}(|\varphi\rangle_{L_1R_1} \otimes |0\rangle_{L_2R_2}) + 4wd \\ &= E_{L_1|R_1}(\varphi_{L_1R_1}) + 4wd \\ &\leq 8wd, \end{aligned} \quad (\text{B9})$$

where we used $E_{L_1|R_1}(\varphi_{L_1R_1}) \leq |L_1| \leq 4wd$. This completes the proof. ■

2. Proof of Theorem 2: Certifying unitary circuit complexity

We first establish the following lemma, which gives an upper bound on the maximal fidelity of highly entangled projected states.

Lemma 5. Let ϕ be a pure state on subsystem A with bipartite entanglement $E_{L|R}(\phi) = e > 8wd + 1$. Then,

$$\text{Fid}_P(\phi) \leq 1 - \left(\frac{e-1}{4w^2} - \frac{2d}{w} \right)^2. \quad (\text{B10})$$

Proof. For any pure state $\varphi \in \mathcal{FP}_P$,

$$\begin{aligned} E_{L|R}(\phi) - E_{L|R}(\varphi) &\leq |E_{L|R}(\phi) - E_{L|R}(\varphi)| \\ &\leq 2d_{\text{tr}}(\phi_L, \varphi_L)|L| + 1, \end{aligned} \quad (\text{B11})$$

where the last step uses Fannes' inequality (Theorem 11.6 in Ref. [135]). Because trace distance is nonincreasing under partial trace, $d_{\text{tr}}(\phi_L, \varphi_L) \leq d_{\text{tr}}(\phi, \varphi)$. With $|L| = 2w^2$ and $E_{L|R}(\varphi) \leq 8wd$ as given in Lemma 2, we obtain

$$d_{\text{tr}}(\phi, \varphi) \geq \frac{e - 8wd - 1}{4w^2} = \frac{e-1}{4w^2} - \frac{2d}{w}. \quad (\text{B12})$$

Finally,

$$\text{tr}(\phi\varphi) = 1 - d_{\text{tr}}^2(\phi, \varphi) \leq 1 - \left(\frac{e-1}{4w^2} - \frac{2d}{w} \right)^2, \quad (\text{B13})$$

which completes the proof. ■

Then we prove the following theorem.

Theorem 6. Let ψ be the target state and consider the bipartition $A \cup B$ shown in Fig. 3, with $w = \eta d$ for some $\eta > 4$. Assume projected ensemble of ψ on A satisfies

$$\Pr_{z \sim p_\psi(z)} [E_{L|R}(\psi_z) \geq c|L| + 1] \geq p > 0, \quad (\text{B14})$$

for a constant $c > 4\eta^{-1}$. Then, Algorithm 1 certifies that the circuit complexity of ψ exceeds d with constant failure probability δ , using

$$T = \mathcal{O}\left(\frac{2^{\mathcal{O}(\eta^2 d^2)}}{(c - 4\eta^{-1})^4 p^2} \ln(\delta^{-1})\right) \quad (\text{B15})$$

copies of ψ and achieving robustness $\varepsilon = \Omega((c - 4\eta^{-1})^2 p)$.

Proof of Theorem 2. Lemma 5 and Eq. (B14) give

$$\Pr_{z \sim p_\psi(z)} \left[\text{Fid}_P(\psi_z) \leq 1 - \frac{1}{4}(c - 4\eta^{-1})^2 \right] \geq p > 0, \quad (\text{B16})$$

which implies $\text{LQ}_P(\psi) \geq \frac{1}{4}(c - 4\eta^{-1})^2 p$. Substituting this into Theorem 1 with variance $\sigma^2 = 4\eta^A + 1 = 2^{\mathcal{O}(\eta^2 d^2)}$ produces the stated sample complexity and robustness. ■

Theorem 2 follows immediately by substituting $c - 4\eta^{-1} = \Omega(1)$ and $p = \Omega(1)$ into the preceding theorem.

3. Proof of Lemma 3: Entanglement in states of low measurement-assisted circuit complexity

Proof. We analyze the preparation of $|\phi\rangle$, considering more and more layers while tracking the expected bipartite entanglement entropy $\mathbb{E}_m[E_{L|(R \cup B)}(\phi_m)]$, where m denotes the outcomes of midcircuit measurements in the considered layers and ϕ_m denotes the state after performing the considered layers given the measurement outcomes m . In each layer of unitary gates, at most $6w$ two-qubit gates can cross the cut $L|(R \cup B)$. Each such gate can increase the bipartite entanglement entropy by at most 2 (Lemma 4 in Ref. [134]). Therefore, the increase in entanglement entropy across the cut per layer is at most $12w$. For measurement rounds, local projective measurements cannot increase entanglement entropy on average [78]. Therefore, after a measurement layer, the expected entanglement entropy across the cut does not increase. After d layers in total, combining the above two observations yields

$$E_{L|(R \cup B)}(\phi) = \mathbb{E}_m[E_{L|(R \cup B)}(\phi_m)] \leq 12wd. \quad (\text{B17})$$

Finally, applying again the monotonicity of entanglement entropy under local measurements when measuring B , we obtain

$$\mathbb{E}_{z \sim p_\phi(z)}[E_{L|R}(\phi_z)] \leq E_{L|(R \cup B)}(\phi) \leq 12wd. \quad (\text{B18})$$

4. Proof of Theorem 3: Certifying measurement-assisted circuit complexity

We begin by analyzing the performance of the linear witness $\tilde{O}$ given in Eq. (20). Define the set

$$\mathcal{FP}_P^p := \left\{ \phi : E_{L|R}(\phi) \leq \frac{12wd}{1-p} \right\}. \quad (\text{B19})$$

We call a set $\mathcal{S}$ a p -likely free projected-state set with respect to property **P** if, for every pure **P**-free state $\psi \in \mathcal{F}_P$,

$$\Pr_{\psi_z \sim \mathcal{E}(\psi)}[\psi_z \in \mathcal{S}] \geq p. \quad (\text{B20})$$

The set $\mathcal{FP}_P^p$ is a p -likely free projected-state set for the property **P** of “measurement-assisted circuit complexity $C_2^{\text{anc}} > d$.” This follows from Lemma 3 together with Markov’s inequality.

We define the maximal fidelity of a state against this p -likely free set as

$$\text{Fid}_{\mathcal{FP}_P^p}(\psi_z) := \max_{\rho \in \mathcal{FP}_P^p} \text{tr}(\rho \psi_z), \quad (\text{B21})$$

and its cumulative distribution function

$$F_{\mathcal{FP}_P^p}(\psi, t) := \Pr_{\psi_z \sim \mathcal{E}(\psi)}[\text{Fid}_{\mathcal{FP}_P^p}(\psi_z) \leq t]. \quad (\text{B22})$$

With these definitions, the linear witness is formally defined as

$$\tilde{O}(\psi, t, p) := \sum_z [t + (1-t)\Theta_t(\text{Fid}_{\mathcal{FP}_P^p}(\psi_z))] |\psi_z\rangle\langle\psi_z|_A \otimes |z\rangle\langle z|_B. \quad (\text{B23})$$

Lemma 6 (Performance of witness $\tilde{O}(\psi, t, p)$). For any threshold $t \in (0, 1)$: (i) (Soundness)—If $\rho \in \mathcal{F}_P$, then $\text{tr}(\tilde{O}(\psi, t, p)\rho) \leq t + (1-p)(1-t)$. (ii) (Completeness)—For the target ψ , $\text{tr}(\tilde{O}(\psi, t, p)\psi) = t + (1-t)F_{\mathcal{FP}_P^p}(\psi, t)$. When the gap

$$\Delta(\psi, t, p) := (1-t)[F_{\mathcal{FP}_P^p}(\psi, t) - (1-p)] > 0, \quad (\text{B24})$$

the witness $\tilde{O}(\psi, t, p)$ separates ψ from $\mathcal{F}$, certifying that ψ has measurement-assisted circuit complexity greater than d .

Proof. By definition, any free state $\rho \in \mathcal{F}_P$ satisfies

$$\begin{aligned} \text{tr}(\tilde{O}(\psi, t, p)\rho) &= \sum_{z: \text{Fid}_{\mathcal{FP}_P^p}(\psi_z) \leq t} p_\rho(z) \text{tr}(\psi_z \rho_z) + t \sum_{z: \text{Fid}_{\mathcal{FP}_P^p}(\psi_z) > t} p_\rho(z) \text{tr}(\psi_z \rho_z) \\ &\leq \sum_{z: \text{Fid}_{\mathcal{FP}_P^p}(\psi_z) \leq t} p_\rho(z) [t + (1-t) \cdot \mathbf{1}[\rho_z \notin \mathcal{FP}_P^p]] + t \sum_{z: \text{Fid}_{\mathcal{FP}_P^p}(\psi_z) > t} p_\rho(z) \\ &\leq t + (1-p)(1-t). \end{aligned} \quad (\text{B25})$$

For the target state ψ ,

$$\begin{aligned} \text{tr}(\tilde{O}(\psi, t, p)\psi) &= \sum_z p_\psi(z) [t + (1-t)\Theta_t(\text{Fid}_{\mathcal{FP}_P^p}(\psi_z))] \\ &= t + (1-t)F_{\mathcal{FP}_P^p}(\psi, t). \end{aligned} \quad (\text{B26})$$

■

Then, we establish the lower bound of the witness gap for high-complexity states.

Lemma 7. Let ψ be the target state and consider the bipartition $A \cup B$ shown in Fig. 3, with $w = \eta d$ for some $\eta > 6$. Suppose the projected ensemble of ψ on A satisfies

$$\Pr_{z \sim p_\psi(z)}[E_{L|R}(\psi_z) \geq c|L| + 1] \geq p > 0, \quad (\text{B27})$$

for a constant $c > 6p^{-1}\eta^{-1}$. Then, setting

$$t = 1 - \frac{1}{4} \left[c - \frac{6}{\eta(1-p')} \right]^2, \quad p' = 1 - \frac{p + 6\eta^{-1}c^{-1}}{2}, \quad (\text{B28})$$

the witness gap satisfies

$$\Delta(\psi, t, p') \geq \frac{c(\eta c p - 6)^3}{8\eta(\eta c p + 6)^2}. \quad (\text{B29})$$

Proof. Let $p' \in (0, 1)$ to be determined with $c > 6/[\eta(1-p')]$. First, by an argument parallel to that of Lemma 5, for any state ϕ satisfying $e := E_{L|R}(\phi) > c|L| + 1$, we obtain

$$\text{Fid}_{\mathcal{F}\mathcal{P}_P^{p'}}(\phi) \leq 1 - \left(\frac{e-1}{4w^2} - \frac{3d}{(1-p')w} \right)^2. \quad (\text{B30})$$

Substituting the entanglement bound $e \geq c|L| + 1$ then yields

$$\Pr_{z \sim p_\psi(z)} [\text{Fid}_{\mathcal{F}\mathcal{P}_P^{p'}}(\psi_z) \leq 1 - \frac{1}{4} [c - 6\eta^{-1}/(1-p')]^2] \geq p > 0. \quad (\text{B31})$$

Hence, for $t = 1 - \frac{1}{4} [c - 6\eta^{-1}/(1-p')]^2$,

$$F_{\mathcal{F}\mathcal{P}_P^{p'}}(\psi, t) = \Pr_{z \sim p_\psi(z)} [\text{Fid}_{\mathcal{F}\mathcal{P}_P^{p'}}(\psi_z) \leq t] \geq p > 0. \quad (\text{B32})$$

By Lemma 6, the gap is, therefore,

$$\begin{aligned} \Delta(\psi, t, p') &= (1-t)[F_{\mathcal{F}\mathcal{P}_P^{p'}}(\psi, t) - (1-p')] \\ &\geq \frac{1}{4} [c - 6\eta^{-1}/(1-p')]^2 [p - (1-p')]. \end{aligned} \quad (\text{B33})$$

When $\eta c p > 6$, choosing $p' = 1 - (p + 6\eta^{-1}c^{-1})/2$ gives

$$\Delta(\psi, t, p') \geq \frac{c(\eta c p - 6)^3}{8\eta(\eta c p + 6)^2}. \quad (\text{B34})$$

Proof of Theorem 3. Choose t, p' as specified in Lemma 7, and define $O := \tilde{O}(\psi, t, p'), a := t + (1-p') \times (1-t) \geq \sup_{\rho \in \mathcal{F}} \text{tr}(\tilde{O}\rho)$, and $b := \text{tr}(\tilde{O}\psi)$ according to Lemma 6. From Lemma 7, we know that the gap $\Delta := \Delta(\psi, t, p') = b - a = \Omega(1)$. Set the decision threshold to $\eta^* := a + (\Delta/3)$.

Soundness. For any $\rho \in \mathcal{F}$, we have $\text{tr}(\tilde{O}\rho) \leq a$. Estimating this quantity to an additive error $\varepsilon = \Delta/3$ ensures $\omega < \text{tr}(\tilde{O}\rho) + \varepsilon \leq \eta^*$, so all property-free states are rejected with high probability.

Completeness. For any state ρ satisfying $d_{\text{tr}}(\rho, \psi) \leq \varepsilon$,

$$\text{tr}(\tilde{O}\rho) - \varepsilon \geq \text{tr}(\tilde{O}\psi) - \|\tilde{O}\|_{\infty} \|(\rho - \psi)_+\|_1 - \varepsilon = \eta^*. \quad (\text{B35})$$

Here, for a Hermitian operator $M = M_+ - M_-$, M_+ is its positive part. The inequality follows because $\tilde{O}$ is positive semidefinite. Therefore, the estimator satisfies

$$\omega > \text{tr}(\tilde{O}\rho) - \varepsilon \geq \eta^*. \quad (\text{B36})$$

So ρ is accepted with high probability.

By Proposition 7, the sample complexity required to achieve additive error ε is given by

$$T = \mathcal{O}\left(\frac{\sigma^2 \ln(\delta^{-1})}{\varepsilon^2}\right) = \mathcal{O}(4^{n_A}) = \exp(\mathcal{O}(\eta^2 d^2)), \quad (\text{B37})$$

where $\sigma^2 \leq 4^{n_A} + 1$. For the two-dimensional setting with $n_A = \mathcal{O}(\eta^2 d^2)$ and constant failure probability, this gives $T = \exp(\mathcal{O}(\eta^2 d^2))$, which completes the proof. ■

APPENDIX C: PERFORMANCE ANALYSIS OF COMPLEXITY CERTIFICATION FOR GENERIC STATES

In this section, we prove the performance of our complexity certification schemes for generic quantum states, including Haar-random states and brickwork-circuit states.

1. Deep-thermalized and Haar-random states

We first establish the performance guarantees for deep-thermalized states. We begin by introducing the basic definitions of quantum state designs and their associated entanglement properties. We then use these tools to establish the desired performance guarantees.

a. Entanglement in quantum state designs

Quantum state designs are defined as approximations to the Haar random distribution [80]. In this context, we denote by $\text{Haar}(n)$ the Haar random distribution over n -qubit pure states. Given a state ensemble $\mathcal{E} = \{p_\psi, \psi\}$, we define its k th moment as

$$\rho_{\mathcal{E}}^{(k)} = \mathbb{E}_{\psi \sim \mathcal{E}} [(|\psi\rangle\langle\psi|)^{\otimes k}]. \quad (\text{C1})$$

Following Ref. [37], we define an ε -approximate k -design as follows.

Definition 1 (ε -approximate k -design). An n -qubit state ensemble $\mathcal{E}$ is an ε -approximate k -design if

$$\|\rho_{\mathcal{E}}^{(k)} - \rho_{\text{Haar}(n)}^{(k)}\|_1 \leq \epsilon. \quad (\text{C2})$$

where $\|\cdot\|_1$ denotes the trace norm.

Note that an ϵ -approximate k_1 -design is also an ϵ -approximate k_2 -design for any $k_2 \leq k_1$. There is also an alternate definition of approximate state designs, using the name “frame operator” (FO).

Definition 2 [λ -FO-approximate k -design (*Definition 10 in Ref. [79]*)]. An n -qubit state ensemble $\mathcal{E}$ is a λ -FO-approximate k -design if

$$\|\rho_{\mathcal{E}}^{(k)} - \rho_{\text{Haar}(n)}^{(k)}\|_1 \leq \lambda D_k^{-1}, \quad (\text{C3})$$

where $D_k = \binom{k+N-1}{k}$ and $N = 2^n$.

It follows that the ensemble $\mathcal{E}$ is an ϵ -approximate k -design if and only if it is a λ -FO-approximate k -design with $\lambda = \epsilon D_k$.

Intuitively, states in a state design exhibit high entanglement, a fact that is rigorously established in Ref. [79]. To show this, we consider the generalized Rényi entropy. In the following, all logarithms are taken to base 2.

Definition 3. The quantum Rényi entropy of a density matrix ρ is defined as

$$S^{(\alpha)}(\rho) = \frac{1}{1-\alpha} \log \text{tr}[\rho^\alpha]. \quad (\text{C4})$$

Taking the limit as $\alpha \rightarrow 1$, the Rényi entropy converges to the von Neumann entropy:

$$S(\rho) := \lim_{\alpha \rightarrow 1} S^{(\alpha)}(\rho) = -\text{tr}[\rho \log \rho]. \quad (\text{C5})$$

By Jensen’s inequality,

$$\sum_{i=1}^D p_i \log p_i \leq \log \sum_{i=1}^D p_i^2, \quad (\text{C6})$$

it follows that $S(\rho) \geq S^{(2)}(\rho)$.

Here, we fix the system to be LR , where both L and R consist of m qubits, with a total of $2m$ qubits. We now present the following result.

Lemma 8 (Purity in a state design). Let $\mathcal{E}$ be an ϵ -approximate 2-design on system LR . For sufficiently large m , it holds that

$$\mathbb{E}_{\psi \sim \mathcal{E}} \text{tr}(\psi_L^2) \leq \frac{d_A + d_B}{d_A d_B + 1} + \epsilon \leq 2^{-m+1} + \epsilon. \quad (\text{C7})$$

Proof. The ensemble $\mathcal{E}$ is also a λ -FO-approximate 2-design with $\lambda = \epsilon D_2$. From Theorem 26 in Ref. [79], we have

$$\mathbb{E}_{\psi \sim \mathcal{E}} \text{tr}(\psi_L^2) \leq \mathbb{E}_{\psi \sim \text{Haar}(2m)} \text{tr}(\psi_L^2) + \frac{\lambda}{D_2} = \frac{d_A + d_B}{d_A d_B + 1} + \epsilon \leq 2^{-m+1} + \epsilon, \quad (\text{C8})$$

where we use $\mathbb{E}_{\psi \sim \text{Haar}(2m)} \text{tr}(\psi_L^2) = \frac{d_A + d_B}{d_A d_B + 1}$ [Eq. (4.11) in Ref. [79]]. ■

b. Proof of Proposition 1: Deep-thermalized states

Proof. Since $E_{L|R}(\phi) = S(\phi_L) \geq S^{(2)}(\phi_L)$, we can bound $\Pr_{\phi \sim \mathcal{E}_\psi} [E_{L|R}(\phi) \geq c|L| + 1]$ as follows:

$$\Pr_{\phi \sim \mathcal{E}_\psi} [E_{L|R}(\phi) \geq c|L| + 1] \geq \Pr_{\phi \sim \mathcal{E}_\psi} [S^{(2)}(\phi_L) \geq c|L| + 1] = \Pr_{\phi \sim \mathcal{E}_\psi} [-\log \text{tr}(\phi_L^2) \geq c|L| + 1] = \Pr_{\phi \sim \mathcal{E}_\psi} [\text{tr}(\phi_L^2) \leq 2^{-(c|L|+1)}]. \quad (\text{C9})$$

By Markov’s inequality,

$$\Pr_{\phi \sim \mathcal{E}_\psi} [\text{tr}(\phi_L^2) > 2^{-(c|L|+1)}] \leq \frac{\mathbb{E}_{\phi \sim \mathcal{E}_\psi} [\text{tr}(\phi_L^2)]}{2^{-(c|L|+1)}} = 2^{c|L|+1} \mathbb{E}_{\phi \sim \mathcal{E}_\psi} [\text{tr}(\phi_L^2)]. \quad (\text{C10})$$

Hence,

$$\begin{aligned} \Pr_{\phi \sim \mathcal{E}_\psi} [E_{L|R}(\phi) \geq c|L| + 1] &\geq \Pr_{\phi \sim \mathcal{E}_\psi} [\text{tr}(\phi_L^2) \leq 2^{-(c|L|+1)}] \\ &= 1 - \Pr_{\phi \sim \mathcal{E}_\psi} [\text{tr}(\phi_L^2) > 2^{-(c|L|+1)}] \\ &\geq 1 - 2^{c|L|+1} \mathbb{E}_{\phi \sim \mathcal{E}_\psi} [\text{tr}(\phi_L^2)]. \end{aligned} \quad (\text{C11})$$

Lemma 8 shows that

$$\mathbb{E}_{\phi \sim \mathcal{E}_\psi}[\text{tr}(\phi_L^2)] \leq 2^{-|L|+1} + \epsilon = \mathcal{O}(2^{-|L|}). \quad (\text{C12})$$

Choosing, for example, $\eta = 5$ and $c = \frac{9}{10}$, we have

$$\begin{aligned} \Pr_{\phi \sim \mathcal{E}_\psi} [E_{L|R}(\phi) \geq c|L| + 1] &\geq 1 - 2^{c|L|+1} [2^{-|L|+1} + \epsilon] \\ &= 1 - \mathcal{O}(2^{-(1-c)|L|}) = \Omega(1). \end{aligned} \quad (\text{C13})$$

Therefore, the sample complexity in Theorem 2 is $\exp(\mathcal{O}(d^2))$.

Moreover, for example, when choosing $\eta = 7$ and $c = \frac{9}{10}$, we still have $\Pr_{\phi \sim \mathcal{E}_\psi} [E_{L|R}(\phi) \geq c|L| + 1] \geq 1 - o(1)$. In this case, the gap given by Eq. (B29) is $\Omega(1)$, and, hence, the observable $\tilde{O}(\psi, t, p')$ can be used to certify the measurement-assisted circuit complexity with $\mathcal{O}(1)$ sample complexity. ■

c. Haar-random states

For Haar-random states, we use the following result on deep thermalization.

Fact 1 [Haar-random states deeply thermalize (Theorem 1 in Ref. [37])]. Let $|\psi\rangle$ be chosen Haar randomly from the set of n -qubit pure states. Then, the ensemble $\mathcal{E}_\psi$ forms an ϵ -approximate k -design with probability at least $1 - \delta$, provided that

$$|B| = \Omega\left(k|A| + \log\left(\frac{1}{\epsilon}\right) + \log\log\left(\frac{1}{\delta}\right)\right). \quad (\text{C14})$$

For complexity certification task, by choosing $k = 2$ and $\epsilon = \Theta(2^{-n_A/2})$, we see that n -qubit Haar-random states with $n = \Omega(|A|) = \Omega(d^2)$ satisfy the requirement in Proposition 1 with probability at least $1 - \delta$, and, thus, their circuit complexity can be sample-efficiently certified.

2. Brickwork-circuit states

We now establish the performance guarantee for brickwork-circuit states. In a D -dimensional brickwork circuit, qubits are labeled by D -dimensional coordinate vectors in $[L]^D$, where L is the edge length. Within every $2D$ consecutive layers, the $(2i-1)$ th and $2i$ th layers, for $1 \leq i \leq D$, each act on adjacent qubits that differ only in their i th coordinate. Specifically, in the i th coordinate, these two layers, respectively, couple qubits with coordinates $(2x_i, 2x_i + 1)$ and $(2x_i - 1, 2x_i)$.

We first show that the projected states of shallow-depth brickwork-circuit states are highly entangled. Building on this, we then derive the corresponding performance guarantee for such states.

a. Entanglement in projected states

Here, we establish the entanglement growth result for general finite dimension D . We begin by using the result on entanglement growth for a two-qubit random unitary.

Fact 2 [Entanglement growth under random unitary (Appendix B in Ref. [81]).] Let $|\phi_t\rangle_{1234}$ be a pure state, and define $|\phi_{t+1}\rangle_{1234} = U_{23}|\phi_t\rangle_{1234}$, where U_{23} is a two-qubit unitary sampled from the Haar measure. Assume subsystems 2 and 3 each have dimension 2. Then, over the Haar-random choice of U_{23} ,

$$\mathbb{E}_{U_{23}} \text{tr}(\rho_{t+1,12}^2) = \frac{2}{5} (\text{tr}(\rho_{t,1}^2) + \text{tr}(\rho_{t,123}^2)). \quad (\text{C15})$$

Then, we establish the entanglement growth of the projected ensemble for random brickwork-circuit states. We denote $\mathcal{E}$ as the random state ensemble $\{p(\psi), \psi\}$. The projected ensemble is defined as $\mathcal{E}_A := \{p(\psi)p_\psi(\mathbf{z}), \psi_z\}$, where A is a region of size $(2w)^D$ in the lattice (for the 2D case, see Fig. 3). We have the following result.

Lemma 9 (High entanglement in D -dimensional random brickwork-circuit states). Let $\mathcal{E}$ be the ensemble of output states from a random D -dimensional depth- d' circuit. Let s be an integer with $w \geq 4s$. Then,

$$\mathbb{E}_{\psi \sim \mathcal{E}_A} [\text{tr}(\psi_L^2)] \leq (4/5)^{(2w-4s)^{D-1} \min(s, \lfloor d'/2D \rfloor)}. \quad (\text{C16})$$

Proof. Recall the definition of the backward light cone of the subsystem B :

$$\begin{aligned} \mathcal{L}_{B,d'+1} &= B, \\ \mathcal{L}_{B,i} &= \mathcal{L}_{B,i+1} \\ &\cup [\cup \{\text{supp}(V_{i,j}) | \text{supp}(V_{i,j}) \cap \mathcal{L}_{B,i+1} \neq \emptyset\}]. \end{aligned} \quad (\text{C17})$$

The whole D -dimensional circuit unitary U can be partitioned into two parts VW , where V is defined as the product of all two-qubit gates in the last $2Ds'$ layers [with $s' = \min(s, \lfloor d'/2D \rfloor)$] whose supports lie entirely outside the backward light cone of B :

$$V = \prod_{i=d'-2Ds'+1}^{d'} \left(\bigotimes_{\text{supp}(V_{i,j}) \not\subseteq \mathcal{L}_{B,i}} V_{i,j} \right), \quad (\text{C18})$$

and W is defined as the product of the remaining unitaries. Similar to Eq. (B8), one can show that, given W and measurement outcome $\mathbf{z}$, there exists a state $|\phi_z\rangle$ such that

$$|\psi_z\rangle = V|\phi_z\rangle. \quad (\text{C19})$$

We now show that, when W and $\mathbf{z}$ are fixed, under the randomness of V , which consists of Haar-random two-qubit unitaries,

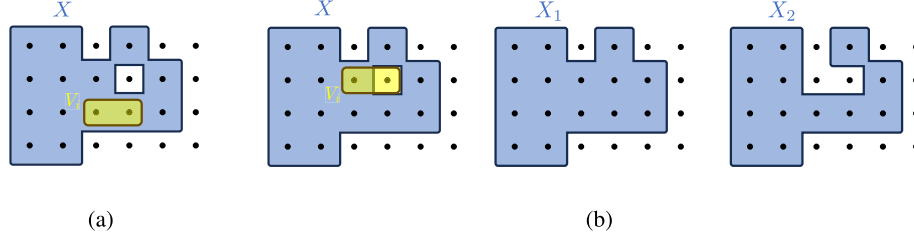


FIG. 8. Illustration of “expanding terms” in the proof of Lemma 9. (a) When V_i acts on two qubits both inside X or both outside X : $c\mathbb{E}_{V_{i-1}, \dots, V_1}[\text{tr}(\psi_X^{(i)2})] = c\mathbb{E}_{V_{i-1}, \dots, V_1}[\text{tr}(\psi_X^{(i-1)2})]$. (b) When V_i acts on one qubit in X and the other outside X : $c\mathbb{E}_{V_{i-1}, \dots, V_1}[\text{tr}(\psi_X^{(i)2})] = \frac{2}{3}c(\mathbb{E}_{V_{i-1}, \dots, V_1}[\text{tr}(\psi_{X_1}^{(i-1)2})] + \mathbb{E}_{V_{i-1}, \dots, V_1}[\text{tr}(\psi_{X_2}^{(i-1)2})])$.

$$\mathbb{E}_V[\text{tr}(\psi_L^2)] \leq (4/5)^{(2w-4s)^{D-1} \min(s, \lfloor d'/2D \rfloor)}, \quad (\text{C20})$$

where $|\psi\rangle$ denotes $|\psi_z\rangle$ with a slight abuse of notation. The idea is to iteratively expand the term using Fact 2. We write V as the product of unitaries $V = V_m \dots V_1$, ordered by layer from V_1 (in layer $d' - 2Ds' + 1$) to V_m (in layer d'), where each V_i is drawn independently from the Haar measure. Let $|\psi^{(i)}\rangle = V_i \dots V_1 |\phi_z\rangle$, so that

$$\begin{aligned} |\psi^{(0)}\rangle &= |\phi_z\rangle, & |\psi^{(i)}\rangle &= V_i |\psi^{(i-1)}\rangle, \\ |\psi\rangle &= V_m \dots V_1 |\phi_z\rangle = |\psi^{(m)}\rangle. \end{aligned} \quad (\text{C21})$$

We start with $\mathbb{E}_V[\text{tr}(\psi_L^2)] = \mathbb{E}_{V_m, \dots, V_1}[\text{tr}(\psi_L^{(m)2})]$. At each step, we pick a term of the form $c\mathbb{E}_{V_{i-1}, \dots, V_1}[\text{tr}(\psi_X^{(i)2})]$ for some coefficient $c > 0$, subset X , and $i > 0$, and “decrease i ” by integrating out V_i using Fact 2. This process acts as follows (illustrated in Fig. 8).

- (i) If V_i acts on two qubits both inside X or both outside X , then

$$\begin{aligned} c\mathbb{E}_{V_{i-1}, \dots, V_1}[\text{tr}(\psi_X^{(i)2})] &= c\mathbb{E}_{V_i} \mathbb{E}_{V_{i-1}, \dots, V_1} \\ &\quad \times [\text{tr}((V_i \psi^{(i-1)} V_i^\dagger)_X^2)] \\ &= c\mathbb{E}_{V_{i-1}, \dots, V_1}[\text{tr}(\psi_X^{(i-1)2})], \end{aligned} \quad (\text{C22})$$

and we replace the term accordingly.

- (ii) Otherwise, V_i acts on one qubit $x \in X$ and one qubit $x' \notin X$. By Fact 2, we replace this term by

$$\begin{aligned} \frac{2}{3}c(\mathbb{E}_{V_{i-1}, \dots, V_1}[\text{tr}(\psi_{X \cup \{x'\}}^{(i-1)2})] \\ + \mathbb{E}_{V_{i-1}, \dots, V_1}[\text{tr}(\psi_{X \setminus \{x\}}^{(i-1)2})]), \end{aligned} \quad (\text{C23})$$

where the two resulting terms still have the desired form, but the sum of coefficients becomes $\frac{4}{3}c$. In this case, we say “the coefficient decreases.”

Now, we expand $\mathbb{E}_V[\text{tr}(\psi_L^2)] = \mathbb{E}_{V_m, \dots, V_1}[\text{tr}(\psi_L^{(m)2})]$ and decrease the coefficient round by round. In each round, we enumerate every current term and reduce its index i until its coefficient decreases. If this process continues for r rounds before reaching $i = 0$, then the sum of the coefficients becomes $(\frac{4}{3})^r$. Moreover, since $\text{tr}(\psi_X^{(i)2}) \leq 1$, the averaged purity is bounded by $(\frac{4}{3})^r$. We show that there are at least $(2w - 4s)^{D-1} s'$ rounds.

Let i_l ($0 \leq l \leq 2Ds'$) be the index such that $V_{i_l+1}, \dots, V_m$ are the unitaries in the last l layers, i.e., layers $d' - l + 1$ to d' . By definition, we have $i_0 = m$ and $i_{2Ds'} = 0$. The unitaries can be grouped by their layer as

$$\begin{aligned} V &= V_m \dots V_1 = (V_{i_0} V_{i_0-1} \dots V_{i_1+1}) (V_{i_1} V_{i_1-1} \dots V_{i_2+1}) \\ &\quad \dots (V_{i_{2Ds'-1}} V_{i_{2Ds'-1}-1} \dots V_{i_{2Ds'}+1}), \end{aligned} \quad (\text{C24})$$

where $V_{i_l}, V_{i_l-1}, \dots, V_{i_{l+1}+1}$ are the unitaries in layer $d' - l$. We have the following claim.

Claim 1. When i is decreased to i_{2Dg} for $0 \leq g < s'$, the partition set X of each term satisfies $L_{-2g} \subseteq X \subseteq L_{+2g}$, where $L_{\pm t}$ is defined in Fig. 9.

Proof. We proceed by induction. The claim holds trivially for $g = 0$. Consider a term with $i = i_l$ and $L_{-l} \subseteq X \subseteq L_{+l}$, and suppose i is then decreased to i_{l+1} , meaning we examine all the unitaries in layer $d' - l + 1$. Let X' be the partition set of any term after decreasing i . There exists $j \in [D]$ such that every gate in the $(d' - l + 1)$ th layer is aligned along the j th coordinate; that is, each gate acts on qubits x, x' satisfying $x'_j = x_j + 1$ and $x'_j = x_j$ for $j' \neq j$. By the “decrease i ” rule, if $j \neq 1$, then $L_{-l} \subseteq X' \subseteq L_{+l}$; otherwise, $L_{-(l+1)} \subseteq X' \subseteq L_{+(l+1)}$.

From the circuit architecture, in every $2D$ consecutive layers, there are exactly two layers where all unitaries are aligned with the first coordinate. Therefore, after each such occurrence, t increases by at most 2. This proves the claim by induction. ■

By the construction of D -dimensional brickwork circuits,

$$\mathcal{L}_{B, d'-i} \cap A_{-2s'} = \emptyset, \quad (\text{C25})$$

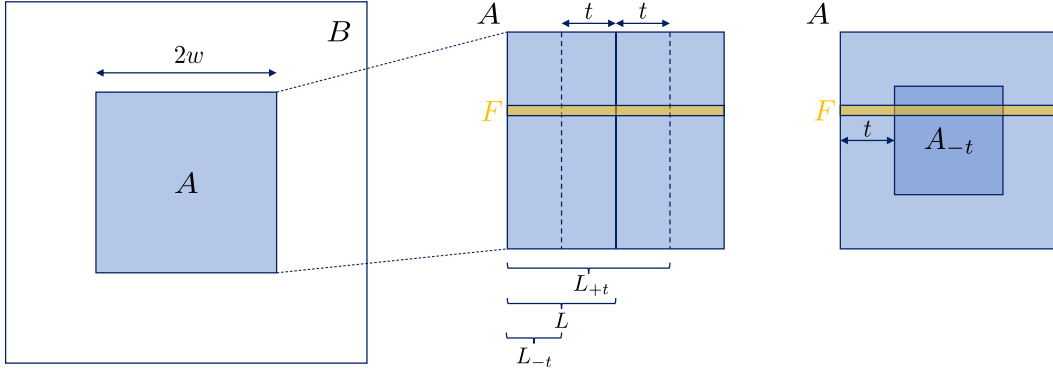


FIG. 9. Definitions used in Claims 1 and 2. Here, $L_{\pm t}$ denotes the set of coordinates in A whose first coordinate lies in $[1, w \pm t]$. A fiber F is defined as a one-dimensional line of qubits in A that differ only in their first coordinate. A_{-t} denotes the set of coordinates at least distance t from the boundary of A .

for all $0 \leq i \leq 2Ds'$, where A_{-t} is defined in Fig. 9. Hence, by the definition of V , for all adjacent qubits $x, x' \in A_{-2s'}$ and $0 \leq g < s'$, there exists some V_i acting on x, x' in a layer from $d' - 2Dg + 1$ to d' , i.e., $i_{2Dg} \geq i > i_{2D(g+1)}$. We now show that, when i of a term is decreased to i_{2Dg} for $0 \leq g < s'$, before i is decreased to $i_{2D(g+1)}$, the coefficient can be decreased at least $(2w - 4s)^{D-1}$ times. It suffices to focus on one term with partition set X . To establish this, we define a fiber F as a one-dimensional line of qubits in A that differ only in their first coordinate (Fig. 9). We have the following claim.

Claim 2. For any fiber F intersecting $A_{-2s'}$, for any term with set X , $X \cap F$ changes at least once before i decreases from i_{2Dg} to $i_{2D(g+1)}$.

Proof. By Claim 1, $L_{-2g} \subseteq X \subseteq L_{+2g}$. This implies the existence of adjacent $x, x' \in (L_{+(2g+1)} \setminus L_{-(2g+1)}) \cap F$ such that $x \in X$ and $x' \notin X$. Since $(2g + 1) < 2s' \leq w - 2s'$, both x, x' belong to $A_{-2s'}$, and, thus, there exists some $V_{i'}$ acting on x, x' with $i_{2Dg} \geq i' > i_{2D(g+1)}$. If $X \cap F$ has never changed before i decreases to i' , then for the current term with partition set X , we have $x \in X$ and $x' \notin X$. At this point, when i is decreased, $X \cap F$ changes. This proves the claim. ■

There are at least $(2w - 4s')^{D-1}$ such fibers. Moreover, whenever the coefficient decreases, exactly one qubit is either added to X or removed from X . Therefore, the coefficient decreases at least $(2w - 4s)^{D-1}$ times when i of a term is decreased to i_{2Dg} for $0 \leq g < s'$. In total, we can decrease the coefficients for at least $(2w - 4s)^{D-1}s'$ rounds. From the earlier discussion, this yields the bound in Eq. (C20). Including the randomness over W and z completes the proof of Lemma 9. ■

b. Proof of Proposition 2

Proof. Let

$$p_\psi := \Pr_{z \sim \mathcal{E}_\psi} [E_{L|R}(\psi_z) \geq c|L| + 1]. \quad (\text{C26})$$

We first compute the expectation of p_ψ over $\psi \sim \mathcal{E}$:

$$\begin{aligned} \mathbb{E}_{\psi \sim \mathcal{E}} [p_\psi] &= \mathbb{E}_{\psi \sim \mathcal{E}} \left[\Pr_{\psi_z \sim \mathcal{E}_\psi} [E_{L|R}(\psi_z) \geq c|L| + 1] \right] \\ &= \Pr_{\psi \sim \mathcal{E}, \psi_z \sim \mathcal{E}_\psi} [E_{L|R}(\psi_z) \geq c|L| + 1] \\ &= \Pr_{\psi \sim \mathcal{E}_A} [E_{L|R}(\psi) \geq c|L| + 1] \\ &\geq 1 - 2^{c|L|+1} \mathbb{E}_{\psi \sim \mathcal{E}_A} [\text{tr}(\psi_L^2)] \\ &\geq 1 - 2^{c|L|+1} (4/5)^{(2w-4s) \min(s, \lfloor d'/4 \rfloor)}. \end{aligned} \quad (\text{C27})$$

where the fourth line uses Eq. (C11) and the last inequality applies Lemma 9.

For $s = \frac{1}{4}w$, $d' \geq w = \eta d$ (where η is a constant to be determined later), a sufficiently small constant c , and a large w ,

$$\mathbb{E}_{\psi \sim \mathcal{E}} [p_\psi] \geq 1 - 2^{-\Omega(w^2)}. \quad (\text{C28})$$

Then,

$$\Pr_{\psi \sim \mathcal{E}} [p_\psi \geq 0.5] \geq 1 - 2 \cdot 2^{-\Omega(w^2)}. \quad (\text{C29})$$

By Theorem 2, when $p_\psi > 0.5$, we can certify circuit complexity d with sample complexity $\exp(\mathcal{O}(w^2)) = \exp(\mathcal{O}(d^2))$, as η is also a constant. By choosing w to be a large constant such that $1 - 2 \cdot 2^{-\Omega(w^2)} > 0.99$, we obtain the desired result.

Moreover, whenever the constant $\eta \geq 14c^{-1}$, when $p_\psi > 0.5$, $\eta p_\psi c \geq 7$. In this case, the gap given by Eq. (B29) is $\Omega(1)$ and, hence, the observable $\tilde{O}(\psi, t, p)$ can be used to certify the measurement-assisted circuit complexity with $\mathcal{O}(1)$ sample complexity. ■

APPENDIX D: ADDITIONAL ANALYSIS ON ENTANGLEMENT CERTIFICATION

1. Proof of Proposition 4

a. Soundness

If ρ is not fully inseparable, let $A|B$ be a separable bipartition. Then, there exists some $i \in A$ such that $i + 1 \in B$. Then, by Proposition 3 (random-basis variant), when testing $A_1 = \{i\}$ and $B_1 = \{i + 1\}$, the protocol outputs **reject** with probability at least $1 - \delta$. Therefore, among all tests, at least one test rejects with probability at least $1 - \delta$.

b. Completeness

If the input state ρ satisfies $d_{\text{tr}}(\rho, \psi) \leq \epsilon := \min_i \{\widetilde{\text{LE}}_\psi(i, i + 1)/6\} = \Omega(1)$ [see Theorem 1 and Eq. (25)], set the failure probability parameter to $\delta' = \delta/(n - 1)$. By Proposition 3 (random-basis variant), with $T = \mathcal{O}(\log(\delta'^{-1})) = \mathcal{O}(\log n + \log \delta^{-1})$, each individual test for a fixed $1 \leq i < n$ outputs **accept** with probability at least $1 - \delta'$. A union bound then implies that all tests (for $1 \leq i < n$) output **accept** simultaneously with probability at least $1 - \delta$. ■

2. Localizable entanglement of Haar-random states

Here, we prove that the localizable entanglement of Haar-random states is bounded below by a constant with overwhelmingly high probability, thereby validating the performance of our protocol on generic states.

Lemma 10 (Localizable entanglement of Haar-random states). Let $|\psi\rangle$ be chosen Haar randomly from the set of n -qubit pure states. Then, with probability at least $1 - \delta$ for $\delta = \exp\{-\exp[\Omega(n)]\}$, we have

$$\text{LE}_\psi(1, 2) = \Omega(1), \quad \widetilde{\text{LE}}_\psi(1, 2) = \Omega(1). \quad (\text{D1})$$

Proof. Fix $\epsilon = \frac{1}{10}$. By Fact 1, the projected ensemble $\mathcal{E}_\psi$ on qubits $\{1, 2\}$ is an ϵ -approximate 2-design with probability $1 - \delta_0$, where $\delta_0 = \exp(-\exp[\Omega(n)])$. Then, by Lemma 8,

$$\mathbb{E}_{\phi \sim \mathcal{E}_\psi}[\text{tr}(\phi_1^2)] \leq \frac{4}{5} + \epsilon = \frac{9}{10}. \quad (\text{D2})$$

Now we show, for the constant $e_0 = \frac{1}{20}$, it holds that $\text{LE}_\psi(1, 2) \geq e_0$. Denote by λ_1 and λ_2 the Schmidt coefficients of the projected state ϕ with $\lambda_1 \geq \lambda_2$. We have $\lambda_2 = 1 - \lambda_1$, $\text{tr}(\phi_1^2) = \lambda_1^2 + \lambda_2^2$, and $\text{Fid}(\phi) = \lambda_1$. Therefore,

$$\begin{aligned} \text{LE}_\psi(1, 2) &= \mathbb{E}_{\phi \sim \mathcal{E}_\psi}[1 - \lambda_1] \\ &\geq \mathbb{E}_{\phi \sim \mathcal{E}_\psi}[\lambda_1(1 - \lambda_1)] \\ &= \frac{1}{2} \mathbb{E}_{\phi \sim \mathcal{E}_\psi}[2\lambda_1(1 - \lambda_1) - 1] + \frac{1}{2} \\ &= -\frac{1}{2} \mathbb{E}_{\phi \sim \mathcal{E}_\psi}[\text{tr}(\phi_1^2)] + \frac{1}{2} \\ &\geq \frac{1}{20}. \end{aligned} \quad (\text{D3})$$

Hence $\text{LE}_\psi(1, 2) \geq e_0$ with probability at least $1 - \delta_0$.

To lower bound $\widetilde{\text{LE}}_\psi(1, 2)$, define $\text{LE}_\psi^{\mathbf{b}}$ for $\mathbf{b} \in \{X, Y, Z\}^{n_B}$ as the localizable entanglement under measurement basis $\mathbf{b}$ on B . By local unitary invariance of the Haar measure, $\text{LE}_\psi^{\mathbf{b}}(1, 2) \geq e_0$ for Haar-random ψ with probability at least $1 - \delta_0$. Let $f(\psi, \mathbf{b}) := \mathbf{1}[\text{LE}_\psi^{\mathbf{b}}(1, 2) \geq e_0]$. Then, for $\mathbf{b}$ chosen uniformly from $\{X, Y, Z\}^{n_B}$,

$$\mathbb{E}_\psi \mathbb{E}_{\mathbf{b}} f(\psi, \mathbf{b}) = \mathbb{E}_{\mathbf{b}} \mathbb{E}_\psi f(\psi, \mathbf{b}) \geq 1 - \delta_0. \quad (\text{D4})$$

By Markov's inequality,

$$\Pr_\psi[\mathbb{E}_{\mathbf{b}} f(\psi, \mathbf{b}) \leq 1 - \sqrt{\delta_0}] \leq \sqrt{\delta_0}. \quad (\text{D5})$$

Therefore, with probability at least $1 - \delta_1$ for $\delta_1 := \sqrt{\delta_0} = \exp(-\exp[\Omega(n)])$,

$$\begin{aligned} \mathbb{E}_{\mathbf{b}} f(\psi, \mathbf{b}) &> 1 - \delta_1, \\ \widetilde{\text{LE}}_\psi(1, 2) &= \mathbb{E}_{\mathbf{b}} \text{LE}_\psi^{\mathbf{b}}(1, 2) \\ &> (1 - \delta_1)e_0 \\ &= \Omega(1). \end{aligned} \quad (\text{D6})$$

Combining the bounds, we conclude that, with probability at least $1 - \delta$ for $\delta = \delta_0 + \delta_1 = \exp(-\exp[\Omega(n)])$,

$$\text{LE}_\psi(1, 2) = \Omega(1), \quad \widetilde{\text{LE}}_\psi(1, 2) = \Omega(1). \quad (\text{D7})$$

■

By a union bound, with probability at least $1 - \delta'$ for $\delta' = n\delta = \exp(-\exp[\Omega(n)])$, we have $\widetilde{\text{LE}}_\psi(i, i + 1) = \Omega(1)$ for all $i \in [n - 1]$. This establishes that our certification protocol for fully inseparable entanglement is sample-efficient for Haar-random states.

3. Details of the numerical experiments on localizable entanglement

a. Stabilizer states

In Fig. 4, we sampled $N_s = 5$ random stabilizer states for system sizes $n \in \{32, 64, 128, 256\}$ and $N_s = 10$ for $n = 16$. For each stabilizer state, we set the failure

probability to $\delta = 0.01$ and the additive error to $\varepsilon = 0.05$. To guarantee that all sites are simultaneously estimated up to an additive error ε with a global failure probability of at most δ , we applied a union bound by setting $\delta' = (\delta/nN_s)$. Accordingly, we set the parameters for the median-of-means estimator (Proposition 7) to $K = \lceil \frac{9}{2} \ln(\delta'^{-1}) \rceil \approx 60$ and $B = \lceil (6\sigma^2/\varepsilon^2) \rceil = 600$, assuming a conservative variance upper bound of $\sigma^2 = 0.25$ of Fid_P across different projected states.

A total of $T = BK$ samples $\{\mathbf{x}_i\}_{i=1}^T$ were obtained by performing random Pauli measurements on the sampled stabilizer states. Each measurement sample $\mathbf{x}_i \in \mathbf{X}^n$ is reused across all sites j to construct the projected state on the nearest-neighbor pair $(j, j+1)$. Subsequently, the localizable entanglement $\widetilde{\text{LE}}_\psi(j, j+1)$ is obtained by computing the median-of-means estimator of Fid_P of the obtained projected states on $(j, j+1)$. Note that $\sigma^2 = 0.25$ overestimates the actual variance of Fid_P . Consequently, the actual additive error is much smaller than the target ε .

b. Hamiltonian systems

In Fig. 5, we report sample means and plot error bars as the standard error of the mean, computed from $N = 1000$ independently sampled projected states. The maximal fidelity to a two-qubit product state is evaluated as λ_1 , the square of the maximal Schmidt coefficient of the two-qubit projected state. Ground states of the XXZ chain are obtained by DMRG for system sizes $n = 32$ and $n = 64$, while the $J_1 - J_2$ chain is treated by DMRG at $n = 20$. All other datasets shown in the figures are produced by exact diagonalization.

APPENDIX E: ADDITIONAL ANALYSIS ON MAGIC CERTIFICATION

In this appendix, we prove that, when the subsystem A consists of a single qubit, the localizable magic of a Haar-random state is lower bounded by a constant with overwhelmingly high probability.

Lemma 11 (Localizable magic of Haar-random states). Let A be a single-qubit subsystem and B be an n_B -qubit subsystem. If $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is a Haar-random pure state, then with probability at least $1 - \exp[-\Omega(2^{n_B})]$,

$$\min \{\text{LM}(\psi), \widetilde{\text{LM}}(\psi)\} \geq \frac{1}{24}. \quad (\text{E1})$$

Proof. Let $\mathcal{S}_1 = \{|0\rangle, |1\rangle, |+\rangle, |-\rangle, |+i\rangle, |-i\rangle\}$ be the set of single-qubit stabilizer states. For a pure single-qubit state $|\phi\rangle$, we define

$$m(\phi) := 1 - \max_{|s\rangle \in \mathcal{S}_1} |(s|\phi)|^2. \quad (\text{E2})$$

Since the free projected set STAB_1 is the convex hull of $\mathcal{S}_1$, we have $m(\phi) = 1 - \text{Fid}_P(\phi)$.

For a fixed $|s\rangle \in \mathcal{S}_1$ and a Haar-random state $|\phi\rangle \in \mathbb{C}^2$, the overlap $X_s := |(s|\phi)|^2$ is uniformly distributed on $[0, 1]$. Thus, for any $0 \leq t \leq 1/6$, a union bound gives

$$\Pr_\phi[m(\phi) \geq t] \geq 1 - \sum_{|s\rangle \in \mathcal{S}_1} \Pr_\phi[X_s > 1 - t] = 1 - 6t. \quad (\text{E3})$$

Consequently,

$$\mu_1 := \mathbb{E}_{\phi \sim \text{Haar}(n_A)}[m(\phi)] = \int_0^1 \Pr_\phi[m(\phi) \geq t] dt \geq \int_0^{1/6} (1 - 6t) dt = \frac{1}{12}. \quad (\text{E4})$$

Fix a product Pauli basis $\mathbf{b} \in \{X, Y, Z\}^{n_B}$ on B , and denote the corresponding localizable magic under basis $\mathbf{b}$ as $\text{LM}_\mathbf{b}$. Using the Gaussian representation of Haar measure, let $\{g_z\}_z$ be independent standard complex Gaussian vectors in $\mathbb{C}^2$, and set $R_z = \|g_z\|_2^2$ and $|u_z\rangle = |g_z\rangle/\|g_z\|_2$. Then,

$$|\psi\rangle = \frac{1}{\sqrt{\sum_z R_z}} \sum_z \sqrt{R_z} |u_z\rangle_A \otimes |z\rangle_B. \quad (\text{E5})$$

The directions $|u_z\rangle$ are independent Haar-random states in $\mathcal{H}_A$ and are independent of $\{R_z\}_z$. Therefore,

$$\mathbb{E}_\psi[\text{LM}_\mathbf{b}(\psi) | \{R_z\}_z] = \sum_z \frac{R_z}{\sum_{z'} R_{z'}} \mathbb{E}_{u_z} m(u_z) = \mu_1. \quad (\text{E6})$$

Thus, $\mathbb{E}_\psi[\text{LM}_\mathbf{b}(\psi)] = \mu_1$ for every basis $\mathbf{b}$. In particular,

$$\mathbb{E}_\psi[\text{LM}(\psi)] = \mathbb{E}_\psi[\widetilde{\text{LM}}(\psi)] = \mu_1, \quad \widetilde{\text{LM}}(\psi) = 3^{-n_B} \sum_{\mathbf{b} \in \{X, Y, Z\}^{n_B}} \text{LM}_\mathbf{b}(\psi). \quad (\text{E7})$$

It remains to prove concentration. For any $s = (s_z)_z \in \mathcal{S}_1^{d_B}$, where $d_B = 2^{n_B}$, set

$$P_{s,b} := \sum_z |s_z\rangle\langle s_z|_A \otimes |z\rangle\langle z|_b. \quad (\text{E8})$$

This is an orthogonal projector, and Eq. (E2) gives

$$\text{LM}_b(\psi) = 1 - \max_{s \in \mathcal{S}_1^{d_B}} \langle \psi | P_{s,b} | \psi \rangle. \quad (\text{E9})$$

For any unit vectors $|\psi\rangle, |\varphi\rangle$ and any orthogonal projector P ,

$$|\langle \psi | P | \psi \rangle - \langle \varphi | P | \varphi \rangle| \leq 2\|\psi - \varphi\|_2. \quad (\text{E10})$$

Hence, every LM_b is 2-Lipschitz on the unit sphere of $\mathbb{C}^{2d_B}$, and so is their average $\widetilde{\text{LM}}$. Then, Levy's lemma (Theorem 7.37 in Ref. [136]) implies, for a universal $c_0 > 0$ and every $\varepsilon > 0$,

$$\begin{aligned} \Pr_\psi[|\text{LM}(\psi) - \mu_1| \geq \varepsilon] &\leq 2 \exp(-c_0 d_B \varepsilon^2), \\ \Pr_\psi[|\widetilde{\text{LM}}(\psi) - \mu_1| \geq \varepsilon] &\leq 2 \exp(-c_0 d_B \varepsilon^2). \end{aligned} \quad (\text{E11})$$

Because $\mu_1 \geq 1/12$, for either quantity to be smaller than $1/24$, it must deviate by at least $1/24$ from its mean. Taking $\varepsilon = 1/24$ in Eq. (E11) and applying a union bound concludes the proof. ■

APPENDIX F: ADDITIONAL PROOFS ON FIDELITY CERTIFICATION

1. Proof of Proposition 5

Proof. Set the decision boundary as $\eta^* = 1 - (1 - c)\Delta(1 - F)$ and the estimation error as $\varepsilon = c\Delta(1 - F)$. Accounting for statistical fluctuations of the estimator ω of $\text{tr}(O_\psi\rho)$ [see Eq. (A9) and Corollary 4], the number of copies required to guarantee precision ε with failure probability at most δ is

$$T = \frac{27 \ln(\delta^{-1})(4^{n_A} + 1)}{c^2 \Delta^2 (1 - F)^2}. \quad (\text{F1})$$

When $\text{tr}(\psi\rho) \leq F$, we have

$$\text{tr}(O_\psi\rho) \leq F \cdot 1 + (1 - F)(1 - \Delta) = 1 - \Delta(1 - F). \quad (\text{F2})$$

Therefore, with probability at least $1 - \delta$, the estimator ω satisfies

$$\omega < \text{tr}(O_\psi\rho) + \varepsilon \leq \eta^*, \quad (\text{F3})$$

so the protocol outputs **reject**.

Conversely, when $\text{tr}(\psi\rho) \geq 1 - (1 - 2c)\Delta(1 - F)$, note that the spectrum of O_ψ is non-negative and has eigenvalue 1 for $|\psi\rangle$. Therefore,

$$\text{tr}(O_\psi\rho) \geq \text{tr}(\psi\rho) \geq 1 - (1 - 2c)\Delta(1 - F). \quad (\text{F4})$$

Hence, with probability at least $1 - \delta$,

$$\omega > \text{tr}(O_\psi\rho) - \varepsilon \geq \eta^*. \quad (\text{F5})$$

and the protocol will output **accept**. ■

2. Proof of Theorem 4

Let $G = (V, E)$ be a simple undirected graph on n vertices $V = \{1, \dots, n\}$ with symmetric adjacency matrix $A \in \mathbb{F}_2^{n \times n}$ with zero diagonal. The associated n -qubit graph state $|G\rangle$ is the unique $+1$ common eigenstate of the stabilizer generators

$$K_i = X_i \prod_{j \in N(i)} Z_j, \quad i \in [n], \quad (\text{F6})$$

where $N(i) = \{j : A_{ij} = 1\}$ is the neighborhood of i . Equivalently, writing an n -qubit Pauli as

$$P_j = i^{p_j} \prod_{k=1}^n X_k^{H_{k,j}^X} Z_k^{H_{k,j}^Z}, \quad (\text{F7})$$

the stabilizer of $|G\rangle$ is generated by $\{P_1, \dots, P_n\}$ with

$$H^X = I_n, \quad H^Z = A; \quad (\text{F8})$$

i.e., the j th generator has an X on qubit j and Z 's on its neighbors. A *random graph state* is obtained by sampling A uniformly at random from all symmetric matrices in $\mathbb{F}_2^{n \times n}$ with zero diagonal and setting $H^Z = A$ (with $H^X = I_n$).

Proof of Theorem 4. Operationally, measuring O_ψ can be viewed as follows: independently sample a local Pauli basis (X , Y , or Z) for each qubit in B , measure B in the resulting product basis, and then (conditioned on the outcome $\mathbf{x}$) either output 0 if $\tilde{p}_\psi(\mathbf{x}) = 0$ or project A onto $|\psi_\mathbf{x}\rangle$. For a fixed choice of local bases $\mathbf{b} \in \mathcal{B}^{n_B}$ (with $\mathcal{B} = \{\{0, 1\}, \{+, -\}, \{+i, -i\}\}$), define

$$O_{\mathbf{b}, \psi} = \sum_{\mathbf{x} \in \mathcal{B}, \tilde{p}_\psi(\mathbf{x}) \neq 0} |\psi_\mathbf{x}\rangle\langle \psi_\mathbf{x}|_A \otimes |\mathbf{x}\rangle\langle \mathbf{x}|_B, \quad (\text{F9})$$

so that

$$O_\psi = 3^{-n_B} \sum_{\mathbf{b} \in \mathcal{B}^{n_B}} O_{\mathbf{b}, \psi} = \mathbb{E}_{\mathbf{b}}[O_{\mathbf{b}, \psi}], \quad (\text{F10})$$

where $\mathbf{b}$ is uniform over $\mathcal{B}^{n_B}$.

Let $\mathcal{S} = \text{Stab}(\psi)$ be generated by $\{P_1, \dots, P_n\}$. Fix a basis choice $\mathbf{b}$, and let $\mathcal{S}_{\text{comm}, \mathbf{b}} \subseteq \mathcal{S}$ denote the subgroup of stabilizers that commute with all local Pauli measurements specified by $\mathbf{b}$ on B . Since the projectors $\{|\mathbf{x}\rangle\langle\mathbf{x}|_B\}_{\mathbf{x} \in \mathbf{b}}$ are pairwise orthogonal, we have $O_{\mathbf{b}, \psi}^2 = O_{\mathbf{b}, \psi}$, and, hence, $O_{\mathbf{b}, \psi}$ is a projector.

Moreover, $O_{\mathbf{b}, \psi}$ is exactly the projector onto the joint (+1) eigenspace of $\mathcal{S}_{\text{comm}, \mathbf{b}}$. First, for any $g \in \mathcal{S}_{\text{comm}, \mathbf{b}}$ and any outcome $\mathbf{x} \in \mathbf{b}$ with $\tilde{p}_\psi(\mathbf{x}) \neq 0$, we have

$$g(I \otimes |\mathbf{x}\rangle\langle\mathbf{x}|_B)|\psi\rangle = (I \otimes |\mathbf{x}\rangle\langle\mathbf{x}|_B)g|\psi\rangle = (I \otimes |\mathbf{x}\rangle\langle\mathbf{x}|_B)|\psi\rangle, \quad (\text{F11})$$

where we used $[g, |\mathbf{x}\rangle\langle\mathbf{x}|_B] = 0$ and $g|\psi\rangle = |\psi\rangle$. Thus, each branch state $|\psi_x\rangle_A \otimes |\mathbf{x}\rangle_B$ lies in the joint (+1) eigenspace of $\mathcal{S}_{\text{comm}, \mathbf{b}}$.

Conversely, let $|v\rangle = \sum_{\mathbf{x} \in \mathbf{b}} \widetilde{v_x}_A \otimes |\mathbf{x}\rangle_B$ satisfy $g|v\rangle = |v\rangle$ for all $g \in \mathcal{S}_{\text{comm}, \mathbf{b}}$. Since every $g \in \mathcal{S}_{\text{comm}, \mathbf{b}}$ commutes with $|\mathbf{x}\rangle\langle\mathbf{x}|_B$, each component $\widetilde{v_x}_A \otimes |\mathbf{x}\rangle_B$ is also stabilized by $\mathcal{S}_{\text{comm}, \mathbf{b}}$. In addition, it is stabilized by the measurement-outcome constraints $\{(-1)^{x_i} P_{b_i}\}_{i \in B}$, where $P_{b_i} \in \{X_i, Y_i, Z_i\}$ is the Pauli observable associated with the basis $\mathbf{b}_i$. The state stabilized by $\mathcal{S}_{\text{comm}, \mathbf{b}}$ together with these commuting single-qubit Paulis is unique. Therefore,

$$\widetilde{v_x}_A \otimes |\mathbf{x}\rangle_B \propto (I \otimes |\mathbf{x}\rangle\langle\mathbf{x}|_B)|\psi\rangle \propto |\psi_x\rangle_A \otimes |\mathbf{x}\rangle_B, \quad (\text{F12})$$

and, hence, $\langle v | O_{\mathbf{b}, \psi} | v \rangle = 1$ lies in $\text{Ran}(O_{\mathbf{b}, \psi})$. Combining above, $O_{\mathbf{b}, \psi}$ is precisely the projector onto the joint (+1) eigenspace of $\mathcal{S}_{\text{comm}, \mathbf{b}}$.

For each $x \in \mathbb{F}_2^n$, let $|\psi_x\rangle$ be the stabilizer state whose stabilizer group is generated by $\{(-1)^{x_1} P_1, \dots, (-1)^{x_n} P_n\}$. Then, $\{|\psi_x\rangle\}_{x \in \mathbb{F}_2^n}$ forms an orthonormal basis. Because $O_{\mathbf{b}, \psi}$ is the projector onto the subspace stabilized by $\mathcal{S}_{\text{comm}, \mathbf{b}}$, we have $\langle \psi_x | O_{\mathbf{b}, \psi} | \psi_x \rangle \in \{0, 1\}$ and $\langle \psi_x | O_{\mathbf{b}, \psi} | \psi_x \rangle = 1$ iff every $g \in \mathcal{S}_{\text{comm}, \mathbf{b}}$ also stabilizes $|\psi_x\rangle$. To make this condition explicit, write each generator in (H^X, H^Z) form in Eq. (F7). Any stabilizer element can be written as

$$g_z := P_1^{z_1} \dots P_n^{z_n} \propto \prod_{k=1}^n X_k^{(H^X z)_k} Z_k^{(H^Z z)_k}, \quad z \in \mathbb{F}_2^n. \quad (\text{F13})$$

Such g_z stabilizes $|\psi_x\rangle$ iff $(-1)^{z^\top x} = 1$, i.e., $z^\top x = 0$ in $\mathbb{F}_2$. For each $i \in B$, let

$$m_i^T = \begin{cases} e_i^T H^X, & \mathbf{b}_i = \{0, 1\}, \\ e_i^T H^Z, & \mathbf{b}_i = \{+, -\}, \\ e_i^T H^X + e_i^T H^Z, & \mathbf{b}_i = \{+i, -i\}, \end{cases} \quad (\text{F14})$$

where e_i denote the unit vector having 1 on the i th entry. A direct Pauli commutation check shows that g_z commutes with the local measurement on qubit i iff $m_i^T z = 0$ in $\mathbb{F}_2$. Therefore, $\langle \psi_x | O_{\mathbf{b}, \psi} | \psi_x \rangle = 1$ iff “for any $z \in \mathbb{F}_2^n$, $m_i^T z = 0$ for all $i \in B$ implies $z^\top x = 0$ ”, which is equivalent to $x \in \text{span}\{m_i | i \in B\}$.

Since $O_\psi = \mathbb{E}_{\mathbf{b}}[O_{\mathbf{b}, \psi}]$ and each $O_{\mathbf{b}, \psi}$ is diagonal in the basis $\{|\psi_x\rangle\}$, O_ψ is also diagonal in this basis. The eigenvalue corresponding to $|\psi_x\rangle$ is

$$\Pr_m[x \in \text{span}\{m_i | i \in B\}], \quad (\text{F15})$$

where m_i is independently and uniformly picked from $\{(H^X)^T e_i, (H^Z)^T e_i, (H^X)^T e_i + (H^Z)^T e_i\}$. For random graph states, $H^X = I$ and H^Z is uniformly and randomly picked from all symmetric matrices with zero diagonal. Therefore, the result follows from the following lemma. ■

Lemma 12. Let $c > 0$ be any constant. Pick A uniformly from random symmetric matrices in $\mathbb{F}_2^{n \times n}$ with zero diagonal. Let a_i denote the i th row (or column) of A , and let e_i denote the unit vector having 1 on the i th entry. Then, with probability at least $1 - \exp[-\Omega(n)]$ over the choice of A , the following holds simultaneously for all nonzero $x \in \mathbb{F}_2^n$: $\Pr_m[x \in \text{span}\{m_i | 2 \leq i \leq n\}] \leq \frac{1}{2} + \frac{1}{3} + c$, where m_i is independently and uniformly picked from $\{e_i, a_i, e_i + a_i\}$.

Proof. For any matrix A and vector x , we have

$$\Pr_m[x \in \text{span}\{m_i | 2 \leq i \leq n\}] \leq \mathbb{E}_m \left[\sum_{k_2, \dots, k_n \in \{0, 1\}} 1_{k_2 m_2 + \dots + k_n m_n = x} \right] = 2^{n-1} \Pr_{m'}[m'_2 + \dots + m'_n = x], \quad (\text{F16})$$

where m'_i is picked from the following distribution: 0 with probability $\frac{1}{2}$, e_i with probability $\frac{1}{6}$, a_i with probability $\frac{1}{6}$, $e_i + a_i$ with probability $\frac{1}{6}$; and each m'_i is picked independently.

We have another way to choose m' : let $m'_i = f_i z_i$, where f_i is 1 with probability $\frac{2}{3}$ and 0 with probability $\frac{1}{3}$, z_i is uniformly picked from $\{0, e_i, a_i, e_i + a_i\}$; and each f_i, z_i are independent. Let

$$V_f = \text{span}\{e_i, a_i | f_i = 1\}, \quad |f| = \sum_{i=2}^n f_i, \quad (\text{F17})$$

where the addition is in $\mathbb{Z}$. Then, $\dim V_f \leq 2|f|$, and

$$\begin{aligned} \Pr_{m'}[m'_2 + \dots + m'_n = x] &= \mathbb{E}_f \Pr_z[f_2 z_2 + \dots + f_n z_n = x] = \mathbb{E}_f \Pr_{y \leftarrow V_f}[y = x] = \mathbb{E}_f[1_{x \in V_f} 2^{-\dim V_f}] \\ &= \mathbb{E}_f[1_{x \in V_f} 2^{-2|f|}] + \mathbb{E}_f[1_{x \in V_f} (2^{-\dim V_f} - 2^{-2|f|})]. \end{aligned} \quad (\text{F18})$$

Let f' be another random vector drawn from the following distribution: f'_i is 1 with probability $\frac{1}{3}$ and 0 with probability $\frac{2}{3}$. Then, for any function $X(f)$ of f ,

$$2^{n-1} \mathbb{E}_f[X(f) 2^{-2|f|}] = \sum_{f \in \{0,1\}^{n-1}} 2^{n-1} \frac{2^{|f|}}{3^{n-1}} X(f) 2^{-2|f|} = \sum_{f \in \{0,1\}^{n-1}} \frac{2^{n-1-|f|}}{3^{n-1}} X(f) = \mathbb{E}_{f'}[X(f')]. \quad (\text{F19})$$

Use this equality in Eqs. (F16) and (F18), we have

$$\begin{aligned} \Pr_m[x \in \text{span}\{m_i | 2 \leq i \leq n\}] &\leq 2^{n-1} \Pr_{m'}[m'_2 + \dots + m'_n = x] \\ &= 2^{n-1} (\mathbb{E}_f[1_{x \in V_f} 2^{-2|f|}] + \mathbb{E}_f[1_{x \in V_f} (2^{-\dim V_f} - 2^{-2|f|})]) \\ &= \mathbb{E}_{f'}[1_{x \in V_{f'}}] + 2^{n-1} \mathbb{E}_f[1_{x \in V_f} (2^{-\dim V_f} - 2^{-2|f|})] \\ &\leq \Pr_{f'}[x \in V_{f'}] + 2^{n-1} \mathbb{E}_f[2^{-\dim V_f} - 2^{-2|f|}]. \end{aligned} \quad (\text{F20})$$

When $x = 0$, it gives

$$\begin{aligned} 2^{n-1} \Pr_{m'}[m'_2 + \dots + m'_n = 0] &= \mathbb{E}_{f'}[1_{0 \in V_{f'}}] + 2^{n-1} \mathbb{E}_f[1_{0 \in V_f} (2^{-\dim V_f} - 2^{-2|f|})] \\ &= 1 + 2^{n-1} \mathbb{E}_f[2^{-\dim V_f} - 2^{-2|f|}]. \end{aligned} \quad (\text{F21})$$

Therefore,

$$\begin{aligned} \Pr_m[x \in \text{span}\{m_i | 2 \leq i \leq n\}] &\leq \Pr_{f'}[x \in V_{f'}] + 2^{n-1} \mathbb{E}_f[2^{-\dim V_f} - 2^{-2|f|}] \\ &= \Pr_{f'}[x \in V_{f'}] + 2^{n-1} \Pr_{m'}[m'_2 + \dots + m'_n = 0] - 1. \end{aligned} \quad (\text{F22})$$

The result can be derived from the following two lemmas. ■

Lemma 13. For any constant $c_1 > 0$, $2^{n-1} \Pr_{m'}[m'_2 + \dots + m'_n = 0] \leq 1 + \frac{1}{2} + c_1$ with probability at least $1 - \exp[-\Omega(n)]$ (with respect to the randomness of A), where m'_i is picked from the following distribution: 0 with probability $\frac{1}{2}$, e_i with probability $\frac{1}{6}$, a_i with probability $\frac{1}{6}$, $e_i + a_i$ with probability $\frac{1}{6}$; and each m'_i is picked independently.

Lemma 14. For any constant $c_2 > 0$, with probability at least $1 - \exp[-\Omega(n)]$ (with respect to the randomness of A), for all nonzero $x \in \mathbb{F}_2^n$, $\Pr_{f'}[x \in V_{f'}] \leq \frac{1}{3} + c_2$, where f' follows Bernoulli($1/3$) $^{n-1}$.

In the following, for any set S, T of indices, let $A_{S,T}$ denote the submatrix of A by keeping the rows with indices in S and columns with indices in T , i.e., $A_{S,T} = (A_{i,j})_{i \in S, j \in T}$; similarly, for vector a , let a_S be the vector by keeping the entries in a with indices in S , i.e., $a_S = (a_i)_{i \in S}$.

Before proving these two lemmas, we first prove another lemma.

Lemma 15. Let $x_1, \dots, x_k$ be k linearly independent vectors in $\mathbb{F}_2^n$, and $d_1, \dots, d_k \in \mathbb{F}_2^n$. Then,

$$\Pr_A[\forall 1 \leq i \leq k, Ax_i = d_i] \leq 2^{-k(n-k)}. \quad (\text{F23})$$

Proof. Let X and D be $n \times k$ matrices whose i th column is x_i and d_i , respectively. “ $\forall 1 \leq i \leq k, Ax_i = d_i$ ” is equivalent to $AX = D$. Since $\{x_i\}$ is linearly independent, there exists some indices set I of size k such that $X_{I,[k]}$ is an invertible matrix. Let $\bar{I}$ denote the complementary of I . $AX = D$ implies

$$D_{\bar{I},[k]} = (AX)_{\bar{I},[k]} = A_{\bar{I},[n]}X = A_{\bar{I},I}X_{I,[k]} + A_{\bar{I},\bar{I}}X_{\bar{I},[k]}, \quad (\text{F24})$$

which is equivalent to

$$A_{\bar{I},I} = (D_{\bar{I},[k]} - A_{\bar{I},\bar{I}}X_{\bar{I},[k]})X_{\bar{I},[k]}^{-1}. \quad (\text{F25})$$

Here, $A_{\bar{I},I}$ is independent of $A_{\bar{I},\bar{I}}$, each entry of $A_{\bar{I},I}$ is independently uniformly chosen from $\mathbb{F}_2$. Hence, we can first choose $A_{\bar{I},\bar{I}}$; given $A_{\bar{I},\bar{I}}$, the probability that the above equation holds is $2^{-k(n-k)}$. Therefore, $\Pr_A[(AX)_{\bar{I},[k]} = D_{\bar{I},[k]}] = 2^{-k(n-k)}$ and

$$\Pr_A[\forall 1 \leq i \leq k, Ax_i = d_i] \leq \Pr_A[(AX)_{\bar{I},[k]} = D_{\bar{I},[k]}] = 2^{-k(n-k)}. \quad (\text{F26})$$

Proof of Lemma 13. We compute the expectation and variance of $X = \Pr_{m'}[m'_2 + \dots + m'_n = 0]$. Here, we pick m' using the following method: first pick $y_i = y_i(a, r)$ from the following expressions: 0 with probability $\frac{1}{2}$, e_i with probability $\frac{1}{6}$, and $a + re_i$ with probability $\frac{1}{3}$; then plug in a_i and a random bit r_i to get $m'_i = y_i(a_i, r_i)$. This procedure produces the same distribution. Let

$$d_y = \sum_{i=2}^n 1_{y_i=e_i} e_i, \quad x_y = \sum_{i=2}^n 1_{y_i=a+re_i} e_i. \quad (\text{F27})$$

Then, for any i , $(d_y)_i$ and $(x_y)_i$ cannot both be 1, and

$$m'_2 + \dots + m'_n = y_2(a_2, r_2) + \dots + y_n(a_n, r_n) = d_y + Ax_y + \sum_{i=2}^n r_i(x_y)_i e_i. \quad (\text{F28})$$

To compute $\mathbb{E}_A[X]$, we have

$$\mathbb{E}_A[X] = \mathbb{E}_A \Pr_{m'}[m'_2 + \dots + m'_n = 0] = \Pr_{y,A,r}[y_2(a_2, r_2) + \dots + y_n(a_n, r_n) = 0]. \quad (\text{F29})$$

We first pick y and then compute the probability of $m'_2 + \dots + m'_n = 0$ under the randomness of A and r .

If, for all i , y_i is not $a_i + r_i e_i$, then $y_2(a_2, r_2) + \dots + y_n(a_n, r_n) = 0$ if and only if $y_i = 0$ for all i . The probability of such event is $2^{-(n-1)}$.

Otherwise, assume $y_i = a + re_i$ for some i . The probability of this case is $1 - (\frac{2}{3})^{n-1}$. Now,

$$\begin{aligned} (m'_2 + \dots + m'_n)_{\{\bar{i}\}} &= (d_y)_{\{\bar{i}\}} + (Ax_y)_{\{\bar{i}\}} + \left(\sum_{j=2}^n r_j(x_y)_j e_j \right)_{\{\bar{i}\}} \\ &= (d_y)_{\{\bar{i}\}} + A_{\{\bar{i}\},\{\bar{i}\}}(x_y)_{\{\bar{i}\}} + A_{\{\bar{i}\},i}(x_y)_i + \sum_{j \neq i} r_j(x_y)_j e_j \\ &= A_{\{\bar{i}\},i} + (d_y)_{\{\bar{i}\}} + A_{\{\bar{i}\},\{\bar{i}\}}(x_y)_{\{\bar{i}\}} + \sum_{j \neq i} r_j(x_y)_j e_j; \end{aligned} \quad (\text{F30})$$

$$(m'_2 + \dots + m'_n)_i = (d_y)_i + (Ax_y)_i + \left(\sum_{j=2}^n r_j(x_y)_j e_j \right)_i = r_i e_i + (d_y)_i + (Ax_y)_i. \quad (\text{F31})$$

We randomly pick $A_{\{\bar{i}\},\{\bar{i}\}}$ under the constraints “ A is symmetric” and “ $A_{jj} = 0$ for all j ” and the entries of r_j ($j \neq i$). Then, we randomly pick $A_{\{\bar{i}\},i}$. After that, $(m'_2 + \dots + m'_n)_{\{\bar{i}\}}$ is determined, and it is zero with probability $2^{-(n-1)}$. Then, we randomly pick r_i , and with probability $\frac{1}{2}$ $(m'_2 + \dots + m'_n)_i = 0$. Therefore, in this case, when y is given,

$$\Pr_{A,r}[y_2(a_2, r_2) + \dots + y_n(a_n, r_n) = 0] = 2^{-n}. \quad (\text{F32})$$

In conclusion,

$$\mathbb{E}_A[X] = \Pr_{y,A,r} [y_2(a_2, r_2) + \cdots + y_n(a_n, r_n) = 0] = 2^{-(n-1)} + \left(1 - \left(\frac{2}{3}\right)^{n-1}\right) 2^{-n}. \quad (\text{F33})$$

Now we bound $\mathbb{E}_A[X^2]$. We have

$$\begin{aligned} \mathbb{E}_A[X^2] &= \mathbb{E}_A[\Pr_{m'}[m'_2 + \cdots + m'_n = 0] \Pr_{m''}[m''_2 + \cdots + m''_n = 0]] \\ &= \Pr_{y,y',A,r,r'} [y_2(a_2, r_2) + \cdots + y_n(a_n, r_n) = y'_2(a_2, r'_2) + \cdots + y'_n(a_n, r'_n) = 0]. \end{aligned} \quad (\text{F34})$$

We first pick y, y' and then compute the probability of $m'_2 + \cdots + m'_n = m''_2 + \cdots + m''_n = 0$ under the randomness of A and r, r' .

If, for all i , y_i is not $a + r e_i$, then $y_2(a_2, r_2) + \cdots + y_n(a_n, r_n) = 0$ if and only if $y_i = 0$ for all i , and it is independent of A . Then, we can use the results when computing $\mathbb{E}_A[X]$. The case “for all i , y'_i is not $a_i + r'_i e_i$ ” is similar. These two cases have contribution $(2^{-(n-1)})^2 + 2 \cdot 2^{-(n-1)} \cdot (1 - (\frac{2}{3})^{n-1}) 2^{-n}$.

Now, we assume that there exists some i, i' such that $y_i = a_i + r_i e_i$, $y'_{i'} = a_{i'} + r'_{i'} e_{i'}$. Then, $x_y, x_{y'} \neq 0$.

First, we compute the probability of the case with $x_y = x_{y'}$:

$$\begin{aligned} &\Pr_{y,y',A,r,r'} [y_2(a_2, r_2) + \cdots + y_n(a_n, r_n) = y'_2(a_2, r'_2) + \cdots + y'_n(a_n, r'_n) = 0 \wedge x_y = x_{y'} \neq 0] \\ &= \Pr_{y,y',A,r,r'} \left[d_y + A x_y + \sum_{i=2}^n r_i (x_y)_i e_i = d_{y'} + A x_{y'} + \sum_{i=2}^n r'_i (x_{y'})_i e_i = 0 \wedge x_y = x_{y'} \neq 0 \right] \\ &= \Pr_{y,y',A,r,r'} \left[d_y + A x_y + \sum_{i=2}^n r_i (x_y)_i e_i = 0 \wedge x_y = x_{y'} \neq 0 \wedge d_y + \sum_{i=2}^n r_i (x_y)_i e_i = d_{y'} + \sum_{i=2}^n r'_i (x_{y'})_i e_i \right]. \end{aligned} \quad (\text{F35})$$

Here, $d_y + \sum_{i=2}^n r_i (x_y)_i e_i = d_{y'} + \sum_{i=2}^n r'_i (x_{y'})_i e_i$ is equivalent to that for all $2 \leq i \leq n$, $(d_y)_i + r_i (x_y)_i = (d_{y'})_i + r'_i (x_{y'})_i$. Here, $(d_y)_i$ [$(d_{y'})_i$] and $(x_y)_i$ [$(x_{y'})_i$] are not both 1, so it is equivalent to that $d_y = d_{y'}$ and $r_i = r'_i$ for all i with $(x_y)_i = 1$. Therefore, by utilizing Eq. (F32),

$$\begin{aligned} &\Pr_{y,y',A,r,r'} [y_2(a_2, r_2) + \cdots + y_n(a_n, r_n) = y'_2(a_2, r'_2) + \cdots + y'_n(a_n, r'_n) = 0 \wedge x_y = x_{y'} \neq 0] \\ &= \Pr_{y,y',A,r,r'} \left[d_y + A x_y + \sum_{i=2}^n r_i (x_y)_i e_i = 0 \wedge x_y = x_{y'} \neq 0 \wedge d_y + \sum_{i=2}^n r_i (x_y)_i e_i = d_{y'} + \sum_{i=2}^n r'_i (x_{y'})_i e_i \right] \\ &= \mathbb{E}_{y,A,r} \left[1 \left[x_y \neq 0 \wedge d_y + A x_y + \sum_{i=2}^n r_i (x_y)_i e_i = 0 \right] \cdot \Pr_{y',r'} [x_y = x_{y'} \wedge d_y = d_{y'} \wedge r_i = r'_i \text{ for all } i \text{ with } (x_y)_i = 1] \right] \\ &= \mathbb{E}_{y,A,r} \left[1 \left[x_y \neq 0 \wedge d_y + A x_y + \sum_{i=2}^n r_i (x_y)_i e_i = 0 \right] 2^{-\sum_{i=2}^n (x_y)_i} \Pr_{y'} [x_y = x_{y'} \wedge d_y = d_{y'}] \right] \\ &= \mathbb{E}_y \left[1_{x_y \neq 0} \Pr_{A,r} \left[d_y + A x_y + \sum_{i=2}^n r_i (x_y)_i e_i = 0 \right] 2^{-\sum_{i=2}^n (x_y)_i} \Pr_{y'} [y = y'] \right] \\ &= \mathbb{E}_y \left[1_{x_y \neq 0} 2^{-n} 2^{-\sum_{i=2}^n (x_y)_i} \Pr_{y'} [y = y'] \right] \\ &= 2^{-n} \left(\mathbb{E}_y [2^{-\sum_{i=2}^n (x_y)_i} \Pr_{y'} [y = y']] - \mathbb{E}_y [1_{x_y=0} 2^{-\sum_{i=2}^n (x_y)_i} \Pr_{y'} [y = y']] \right) \\ &= 2^{-n} \left(\left(\frac{1}{2^2} + \frac{1}{6^2} + \frac{1}{3^2} \times \frac{1}{2} \right)^{n-1} - \left(\frac{1}{2^2} + \frac{1}{6^2} \right)^{n-1} \right) = 2^{-n} \left(3^{-(n-1)} - \left(\frac{5}{18} \right)^{n-1} \right). \end{aligned} \quad (\text{F36})$$

Then, we compute the probability of the case with $x_y \neq x_{y'}$, and there exists some i such that $(x_y)_i = (x_{y'})_i = 1$. The probability of entering this case is

$$\begin{aligned}
 & \Pr_{y,y'}[x_y, x_{y'} \neq 0 \wedge x_y \neq x_{y'} \wedge \exists i, (x_y)_i = (x_{y'})_i = 1] \\
 &= \Pr_{y,y'}[x_y \neq x_{y'} \wedge \exists i, (x_y)_i = (x_{y'})_i = 1] \\
 &= 1 - \Pr_{y,y'}[\forall i, ((x_y)_i = 0 \vee (x_{y'})_i = 0)] - \Pr_{y,y'}[x_y = x_{y'}] + \Pr_{y,y'}[x_y = x_{y'} = 0] \\
 &= 1 - \left(1 - \frac{1}{3^2}\right)^{n-1} - \left(\frac{1}{3^2} + \frac{2^2}{3^2}\right)^{n-1} + \left(\frac{2^2}{3^2}\right)^{n-1} = 1 - \left(\frac{8}{9}\right)^{n-1} - \left(\frac{5}{9}\right)^{n-1} + \left(\frac{4}{9}\right)^{n-1}. \tag{F37}
 \end{aligned}$$

Now we assume that y, y' are given and compute

$$\begin{aligned}
 & \Pr_{A,r,r'}[y_2(a_2, r_2) + \dots + y_n(a_n, r_n) = y'_2(a_2, r'_2) + \dots + y'_n(a_n, r'_n) = 0] \\
 &= \Pr_{A,r,r'}\left[d_y + Ax_y + \sum_{k=2}^n r_k(x_y)_k e_k = d_{y'} + Ax_{y'} + \sum_{k=2}^n r'_k(x_{y'})_k e_k = 0\right]. \tag{F38}
 \end{aligned}$$

Since $x_y \neq x_{y'}$, there exists some j such that $(x_y)_j \neq (x_{y'})_j$. Without loss of generality, we assume that $(x_y)_j = 0, (x_{y'})_j = 1$. Because $(x_y)_i = (x_{y'})_i = 1, i \neq j$. Then,

$$\begin{aligned}
 \left(d_y + Ax_y + \sum_{k=2}^n r_k(x_y)_k e_k\right)_{\overline{\{i,j\}}} &= A_{\overline{\{i,j\}}, \overline{\{i,j\}}}(x_y)_{\overline{\{i,j\}}} + A_{\overline{\{i,j\}}, i}(x_y)_i + A_{\overline{\{i,j\}}, j}(x_y)_j \\
 &\quad + (d_y)_{\overline{\{i,j\}}} + \sum_{k \neq i,j} r_k(x_y)_k e_k \\
 &= A_{\overline{\{i,j\}}, i} + A_{\overline{\{i,j\}}, \overline{\{i,j\}}}(x_y)_{\overline{\{i,j\}}} + (d_y)_{\overline{\{i,j\}}} + \sum_{k \neq i,j} r_k(x_y)_k e_k; \tag{F39}
 \end{aligned}$$

$$\left(d_y + Ax_y + \sum_{k=2}^n r_k(x_y)_k e_k\right)_i = (d_y)_i + A_{i,[n]}(x_y) + r_i(x_y)_i = r_i + (d_y)_i + A_{i,[n]}(x_y); \tag{F40}$$

$$\begin{aligned}
 \left(d_y + Ax_y + \sum_{k=2}^n r_k(x_y)_k e_k\right)_j &= (d_y)_j + A_{j,\overline{\{i,j\}}}(x_y)_{\overline{\{i,j\}}} + A_{j,i}(x_y)_i + A_{j,j}(x_y)_j + r_j(x_y)_j \\
 &= A_{j,i} + (d_y)_j + A_{j,\overline{\{i,j\}}}(x_y)_{\overline{\{i,j\}}}; \tag{F41}
 \end{aligned}$$

$$\begin{aligned}
 \left(d_{y'} + Ax_{y'} + \sum_{k=2}^n r'_k(x_{y'})_k e_k\right)_{\overline{\{i,j\}}} &= A_{\overline{\{i,j\}}, \overline{\{j\}}}(x_{y'})_{\overline{\{j\}}} + A_{\overline{\{i,j\}}, j}(x_{y'})_j + (d_{y'})_{\overline{\{i,j\}}} + \sum_{k \neq i,j} r'_k(x_{y'})_k e_k \\
 &= A_{\overline{\{i,j\}}, j} + A_{\overline{\{i,j\}}, \overline{\{j\}}}(x_{y'})_{\overline{\{j\}}} + (d_{y'})_{\overline{\{i,j\}}} + \sum_{k \neq i,j} r'_k(x_{y'})_k e_k; \tag{F42}
 \end{aligned}$$

$$\left(d_{y'} + Ax_{y'} + \sum_{k=2}^n r'_k(x_{y'})_k e_k\right)_i = (d_{y'})_i + A_{i,[n]}x_y + r'_i(x_{y'})_i = r'_i + (d_{y'})_i + A_{i,[n]}x_y; \tag{F43}$$

$$\left(d_{y'} + Ax_{y'} + \sum_{k=2}^n r'_k(x_{y'})_k e_k\right)_j = (d_{y'})_j + A_{j,[n]}x_y + r'_j(x_{y'})_j = r'_j + (d_{y'})_j + A_{j,[n]}x_y. \tag{F44}$$

We consider the following procedure to sample A , r , and r' : uniformly randomly sample r_k, r'_k for all $k \neq i, j$ and uniformly randomly sample $A_{\overline{\{i,j\}}, \overline{\{i,j\}}}$ under the constraints that “ $A_{\overline{\{i,j\}}, \overline{\{i,j\}}}$ is symmetric and $A_{k,k} = 0$ for all $k \neq i, j$ ”; set $A_{i,i} = A_{j,j} = 0$; uniformly randomly sample $A_{\overline{\{i,j\}}, i}$ and let $A_{i, \overline{\{i,j\}}}$ be its transpose, and now Eq. (F39) is determined and it is 0 with probability $2^{-(n-2)}$; uniformly randomly sample $A_{\overline{\{i,j\}}, j}$ and let $A_{j, \overline{\{i,j\}}}$ be its transpose, and now Eq. (F42) is determined and it is 0 with probability $2^{-(n-2)}$; uniformly randomly sample $A_{i,j} = A_{j,i}$, and now Eq. (F41)

is determined and it is 0 with probability 2^{-1} ; uniformly randomly sample r_i, r_j, r'_i, r'_j , and now Eqs. (F40), (F43), and (F44) are determined and they are all 0 with probability 2^{-3} . One can verify that this procedure produces the correct distribution of A, r, r' . Therefore, for fixed y, y' with $x_y \neq x_{y'}, x_y, x_{y'} \neq 0$ and $(x_y)_i = (x_{y'})_i = 1$ for some i , the probability of $m'_2 + \dots + m'_n = m''_2 + \dots + m''_n = 0$ is 2^{-2n} under the randomness of A and r, r' .

Finally, we compute the probability of the case with $x_y \neq x_{y'}$, and there does not exist i such that $(x_y)_i = (x_{y'})_i = 1$. The probability of entering this case is

$$\begin{aligned}
& \Pr_{y,y'}[x_y, x_{y'} \neq 0 \wedge x_y \neq x_{y'} \wedge \forall i, ((x_y)_i \neq (x_{y'})_i \vee (x_y)_i = (x_{y'})_i = 0)] \\
&= \Pr_{y,y'}[x_y, x_{y'} \neq 0 \wedge \forall i, ((x_y)_i \neq (x_{y'})_i \vee (x_y)_i = (x_{y'})_i = 0)] \\
&= \Pr_{y,y'}[\forall i, ((x_y)_i \neq (x_{y'})_i \vee (x_y)_i = (x_{y'})_i = 0)] - \Pr_{y,y'}[x_y = 0] - \Pr_{y,y'}[x_{y'} = 0] + \Pr_{y,y'}[x_y = x_{y'} = 0] \\
&= \left(1 - \frac{1}{3^2}\right)^{n-1} - 2\left(\frac{2}{3}\right)^{n-1} + \left(\frac{2^2}{3^2}\right)^{n-1} = \left(\frac{8}{9}\right)^{n-1} - 2\left(\frac{2}{3}\right)^{n-1} + \left(\frac{4}{9}\right)^{n-1}. \tag{F45}
\end{aligned}$$

In this case, $x_y \neq x_{y'}$ and $x_y, x_{y'} \neq 0$, so x_y and $x_{y'}$ are linearly independent. We pick r, r' first and then A and utilize Lemma 15; then, we get

$$\begin{aligned}
& \Pr_{A,r,r'}[y_2(a_2, r_2) + \dots + y_n(a_n, r_n) = y'_2(a_2, r'_2) + \dots + y'_n(a_n, r'_n) = 0] \\
&= \Pr_{A,r,r'}\left[d_y + Ax_y + \sum_{i=2}^n r_i(x_y)_i e_i = d_{y'} + Ax_{y'} + \sum_{i=2}^n r'_i(x_{y'})_i e_i = 0\right] \\
&= \mathbb{E}_{r,r'}\left[\Pr_A\left[Ax_y = -d_y - \sum_{i=2}^n r_i(x_y)_i e_i \wedge Ax_{y'} = -d_{y'} - \sum_{i=2}^n r'_i(x_{y'})_i e_i\right]\right] \leq 2^{-2(n-2)}. \tag{F46}
\end{aligned}$$

In summary,

$$\begin{aligned}
\mathbb{E}[X^2] &\leq (2^{-(n-1)})^2 + 2 \cdot 2^{-(n-1)} \cdot \left(1 - \left(\frac{2}{3}\right)^{n-1}\right) 2^{-n} + 2^{-n} \left(3^{-(n-1)} - \left(\frac{5}{18}\right)^{n-1}\right) \\
&\quad + 2^{-2n} \left(1 - \left(\frac{8}{9}\right)^{n-1} - \left(\frac{5}{9}\right)^{n-1} + \left(\frac{4}{9}\right)^{n-1}\right) + 2^{-2(n-2)} \left(\left(\frac{8}{9}\right)^{n-1} - 2\left(\frac{2}{3}\right)^{n-1} + \left(\frac{4}{9}\right)^{n-1}\right). \tag{F47}
\end{aligned}$$

Together with Eq. (F33), we have

$$\text{Var}[X] \leq 2^{-2n} \exp[-\Omega(n)]. \tag{F48}$$

Therefore, by Chebyshev's inequality,

$$\begin{aligned}
& \Pr_A\left[2^{n-1} \Pr_{m'}[m'_2 + \dots + m'_n = 0] > 1 + \frac{1}{2} + c_1\right] \\
&= \Pr_A\left[2^{n-1} X > 1 + \frac{1}{2} + c_1\right] \leq \Pr_A[2^{n-1} X > 2^{n-1} \mathbb{E}[X] + c_1] \leq \frac{2^{2(n-1)} \text{Var}[X]}{c_1^2} = \exp[-\Omega(n)]. \tag{F49}
\end{aligned}$$

Hence, $2^{n-1} \Pr_{m'}[m'_2 + \dots + m'_n = 0] \leq 1 + \frac{1}{2} + c_1$ with probability at least $1 - \exp[-\Omega(n)]$ (with respect to the randomness of A). ■

Proof of Lemma 14. Let T denote the event “for all nonzero $x \in \mathbb{F}_2^n$, $\Pr_{f'}[x \in V_{f'}] \leq \frac{1}{3} + c_2$,” and we need to prove that T happens with probability at least $1 - \exp[-\Omega(n)]$. Here, f' follows $\text{Bernoulli}(1/3)^{n-1}$.

Assume that T does not happen; that is, there exists a nonzero $x \in \mathbb{F}_2^n$ such that $\Pr_{f'}[x \in V_{f'}] > \frac{1}{3} + c_2$. We consider the following procedure: for each $2 \leq i \leq n$, independently uniformly sample p_i from $\{0, 1, 2\}$. For $k = 0, 1, 2$, let $(f_k)_i = 1_{p_i=k}$; then f_k follows $\text{Bernoulli}(1/3)^{n-1}$. By assumption, $\Pr[x \in V_{f_k}] > \frac{1}{3} + c_2$, and, hence,

$$\begin{aligned} 1 + 3c_2 &< \Pr[x \in V_{f_0}] + \Pr[x \in V_{f_1}] + \Pr[x \in V_{f_2}] = \mathbb{E}[1[x \in V_{f_0}] + 1[x \in V_{f_1}] + 1[x \in V_{f_2}]] \\ &\leq \mathbb{E}\left[1 + \frac{1[x \in V_{f_0}] + 1[x \in V_{f_1}] + 1[x \in V_{f_2}]}{2}\right] \\ &= 1 + (\Pr[x \in V_{f_0} \cap V_{f_1}] + \Pr[x \in V_{f_1} \cap V_{f_2}] + \Pr[x \in V_{f_2} \cap V_{f_0}]). \end{aligned} \quad (\text{F50})$$

By symmetry, $\Pr[x \in V_{f_0} \cap V_{f_1}] = \Pr[x \in V_{f_1} \cap V_{f_2}] = \Pr[x \in V_{f_2} \cap V_{f_0}]$. Therefore,

$$\Pr[x \in V_{f_0} \cap V_{f_1}] > c_2. \quad (\text{F51})$$

We independently sample another q following the same distribution as p , and let $(g_k)_i = 1_{q_i=k}$ for $k = 0, 1, 2$. Then,

$$\begin{aligned} c_2^2 &< \Pr_{p,q}[x \in V_{f_0} \cap V_{f_1} \wedge x \in V_{g_0} \cap V_{g_1}] = \Pr_{p,q}[x \in V_{f_0} \cap V_{f_1} \cap V_{g_0} \cap V_{g_1}] \\ &\leq \Pr_{p,q}[V_{f_0} \cap V_{f_1} \cap V_{g_0} \cap V_{g_1} \neq \{0\}]. \end{aligned} \quad (\text{F52})$$

Let $X = \Pr_{p,q}[V_{f_0} \cap V_{f_1} \cap V_{g_0} \cap V_{g_1} \neq \{0\}]$. When event T does not happen, $X > c_2^2$.

Now we bound the expectation of X under the randomness of A ; that is,

$$\mathbb{E}_A[X] = \Pr_{p,q,A}[V_{f_0} \cap V_{f_1} \cap V_{g_0} \cap V_{g_1} \neq \{0\}]. \quad (\text{F53})$$

We first pick p, q and then A . Let $I_k = \{i | p_i = k\}$, $J_k = \{i | q_i = k\}$ for $k = 0, 1, 2$. $I_0 \cap I_1 = \emptyset$, $J_0 \cap J_1 = \emptyset$. $i \in I_k \cap J_{k'}$ if and only if $p_i = k$, $q_i = k'$, which happens with probability $\frac{1}{9}$; “ $p_i = k$, $q_i = k'$ ” and “ $p_j = k$, $q_j = k'$ ” are independent for $i \neq j$. Therefore, by Chernoff’s bound and union bound, with probability $1 - \exp[-\Omega(n)]$, $|I_k \cap J_{k'}| < (\frac{1}{9} + 0.01)n$ for all $k, k' \in \{0, 1, 2\}$.

Now, we fix p, q with assumption $|I_k \cap J_{k'}| < (\frac{1}{9} + 0.01)n$ for all $k, k' \in \{0, 1, 2\}$, which implies $0 < |I_k|, |J_k| < (\frac{1}{3} + 0.03)n$ for all $k \in \{0, 1, 2\}$; and we bound $\Pr_A[V_{f_0} \cap V_{f_1} \cap V_{g_0} \cap V_{g_1} \neq \{0\}]$. Here,

$$\begin{aligned} V_{f_k} &= \text{span}\{e_i, a_i | (f_k)_i = 1\} = \text{span}\{e_i, a_i | p_i = k\} = \text{span}\{e_i, a_i | i \in I_k\} \\ &= \left\{ \sum_{i \in I_k} (d_i e_i + x_i a_i) | x, d \in \mathbb{F}_2^{I_k} \right\} = \{Ax + d | x, d \in \mathbb{F}_2^{I_k}\} \end{aligned} \quad (\text{F54})$$

and similar for V_{g_k} . Then,

$$\begin{aligned} &\Pr_A[V_{f_0} \cap V_{f_1} \cap V_{g_0} \cap V_{g_1} \neq \{0\}] \\ &\leq \mathbb{E}_A \left[\sum_{x_1, d_1 \in \mathbb{F}_2^{I_0}} \sum_{x_2, d_2 \in \mathbb{F}_2^{I_1}} \sum_{x_3, d_3 \in \mathbb{F}_2^{J_0}} \sum_{x_4, d_4 \in \mathbb{F}_2^{J_1}} 1[Ax_1 + d_1 = Ax_2 + d_2 = Ax_3 + d_3 = Ax_4 + d_4 \neq 0] \right] \\ &= \sum_{x_1, d_1 \in \mathbb{F}_2^{I_0}} \sum_{x_2, d_2 \in \mathbb{F}_2^{I_1}} \sum_{x_3, d_3 \in \mathbb{F}_2^{J_0}} \sum_{x_4, d_4 \in \mathbb{F}_2^{J_1}} \Pr_A[Ax_1 + d_1 = Ax_2 + d_2 = Ax_3 + d_3 = Ax_4 + d_4 \neq 0]. \end{aligned} \quad (\text{F55})$$

We bound $\Pr_A[Ax_1 + d_1 = Ax_2 + d_2 = Ax_3 + d_3 = Ax_4 + d_4 \neq 0]$ for fixed $x_1, d_1 \in \mathbb{F}_2^{I_0}, x_2, d_2 \in \mathbb{F}_2^{I_1}, x_3, d_3 \in \mathbb{F}_2^{J_0}, x_4, d_4 \in \mathbb{F}_2^{J_1}$; denote it as $p_{x,d}$. By Lemma 15,

$$\begin{aligned}
p_{x,d} &= \Pr_A[Ax_1 + d_1 = Ax_2 + d_2 = Ax_3 + d_3 = Ax_4 + d_4 \neq 0] \\
&\leq \Pr_A[A(x_1 + x_2) = d_1 + d_2 \wedge A(x_3 + x_4) = d_3 + d_4 \wedge A(x_1 + x_3) = d_1 + d_3] \\
&\leq 2^{-k_{x,d}(n-k_{x,d})} = \mathcal{O}(2^{-k_{x,d}n})
\end{aligned} \tag{F56}$$

(in $\mathbb{F}_2$, plus and minus are the same), where

$$k_{x,d} = \dim \text{span}\{x_1 + x_2, x_3 + x_4, x_1 + x_3\}. \tag{F57}$$

We focus only on those x, d such that $p_{x,d} \neq 0$; that is, there exists some A such that $Ax_1 + d_1 = Ax_2 + d_2 = Ax_3 + d_3 = Ax_4 + d_4 \neq 0$.

When $x_1 = x_2 = 0$, $Ax_1 + d_1 = Ax_2 + d_2$ implies $d_1 = d_2$; but $d_1 \in \mathbb{F}_2^{I_0}$, $d_2 \in \mathbb{F}_2^{I_1}$, and $I_0 \cap I_1 = \emptyset$. Hence, $d_1 = d_2 = 0$, and $Ax_1 + d_1 = 0$. Therefore, in this case $p_{x,d} = 0$. We ignore this case; that is, we have $x_1 \neq 0$ or $x_2 \neq 0$. Similarly, $x_3 \neq 0$ or $x_4 \neq 0$.

Since $x_1 \in \mathbb{F}_2^{I_0}$, $x_2 \in \mathbb{F}_2^{I_1}$, and $I_0 \cap I_1 = \emptyset$, $x_1 \neq x_2$ (otherwise, $x_1 = x_2 = 0$); similarly, $x_3 \neq x_4$.

Now we discuss $k_{x,d}$ and count the number of x, d such that $p_{x,d} \neq 0$; that is, there exists some A such that $Ax_1 + d_1 = Ax_2 + d_2 = Ax_3 + d_3 = Ax_4 + d_4 \neq 0$. Here, $x_1 + x_2 = x_1 - x_2 \neq 0$, $x_3 + x_4 \neq 0$, so $k_{x,d} \in \{1, 2, 3\}$. Assume that $p_{x,d} \neq 0$.

- (i) $k_{x,d} = 3$ —The number of possible values of x_1 is $|\mathbb{F}_2^{I_0}| = 2^{|I_0|} < 2^{(1/3+0.03)n}$. Similarly, $x_2, x_3, x_4, d_1, d_2, d_3$, and d_4 each have less than $2^{(1/3+0.03)n}$ possible values. Hence,

$$\sum_{x,d:k_{x,d}=3} p_{x,d} \leq \sum_{x,d:k_{x,d}=3, p_{x,d} \neq 0} \mathcal{O}(2^{-3n}) \leq 2^{8(1/3+0.03)n} \mathcal{O}(2^{-3n}) = \exp[-\Omega(n)]. \tag{F58}$$

- (ii) $k_{x,d} = 1$ —Then, $x_1 + x_2 = x_3 + x_4$; $x_1 + x_3 = x_1 + x_2$ or $x_1 + x_3 = 0$. The first case implies $x_2 = x_3$ and then $x_1 = x_4$, and the second case implies $x_1 = x_3$ and then $x_2 = x_4$.

We assume $x_1 = x_4$, $x_2 = x_3$. Since $Ax_1 + d_1 = Ax_4 + d_4$, $d_1 = d_4$. Similarly, $d_2 = d_3$. Because $x_1 \in \mathbb{F}_2^{I_0}$, $x_4 \in \mathbb{F}_2^{I_1}$, $x_1 = x_4 \in \mathbb{F}_2^{I_0} \cap \mathbb{F}_2^{I_1} = \mathbb{F}_2^{I_0 \cap I_1}$, which has $2^{|I_0 \cap I_1|} < 2^{(1/9+0.01)n}$ possible values. Similarly, $x_2 = x_3$, $d_1 = d_4$, and $d_2 = d_3$ have less than $2^{(1/9+0.01)n}$ possible values. Hence, for this case, the number of possible x, d is less than $2^{(4/9+0.04)n}$.

The case for $x_1 = x_3$, $x_2 = x_4$ is similar. Therefore,

$$\sum_{x,d:k_{x,d}=1} p_{x,d} \leq \sum_{x,d:k_{x,d}=1, p_{x,d} \neq 0} \mathcal{O}(2^{-n}) < 2 \times 2^{(4/9+0.04)n} \mathcal{O}(2^{-n}) = \exp[-\Omega(n)]. \tag{F59}$$

- (iii) $k_{x,d} = 2$ with $x_1 + x_2 = x_3 + x_4$ —Since $x_1 + x_2 \in \mathbb{F}_2^{I_0 \cup I_1} = \mathbb{F}_2^{I_0} \oplus \mathbb{F}_2^{I_1}$, $x_3 + x_4 \in \mathbb{F}_2^{J_0 \cup J_1} = \mathbb{F}_2^{J_0} \oplus \mathbb{F}_2^{J_1}$, x_1, x_2, x_3, x_4 are determined by $x_1 + x_2 = x_3 + x_4 \in \mathbb{F}_2^{I_0 \cup J_1} \cap \mathbb{F}_2^{J_0 \cup I_1} = \mathbb{F}_2^{(I_0 \cap J_0) \cup (I_0 \cap J_1) \cup (I_1 \cap J_0) \cup (I_1 \cap J_1)}$, which has $2^{|I_0 \cap J_0| + |I_0 \cap J_1| + |I_1 \cap J_0| + |I_1 \cap J_1|} < 2^{(4/9+0.04)n}$ possible values.

Since $Ax_1 + d_1 = Ax_2 + d_2 = Ax_3 + d_3 = Ax_4 + d_4$, $A(x_1 + x_2) + (d_1 + d_2) = A(x_3 + x_4) + (d_3 + d_4)$ and, hence, $d_1 + d_2 = d_3 + d_4$. By the same reason, the number of possible values of (d_1, d_2, d_3, d_4) is less than $2^{(4/9+0.04)n}$. Therefore,

$$\sum_{\substack{x,d:k_{x,d}=2 \\ x_1+x_2=x_3+x_4}} p_{x,d} \leq \sum_{\substack{x,d:k_{x,d}=1, p_{x,d} \neq 0 \\ x_1+x_2=x_3+x_4}} \mathcal{O}(2^{-2n}) < 2^{2(4/9+0.04)n} \mathcal{O}(2^{-2n}) = \exp[-\Omega(n)]. \tag{F60}$$

- (iv) $k_{x,d} = 2$ with $x_1 + x_2 \neq x_3 + x_4$ —Since $x_1 + x_2, x_3 + x_4 \neq 0$, they are linearly independent, and, hence, $x_1 + x_3 \in \text{span}\{x_1 + x_2, x_3 + x_4\} = \{0, x_1 + x_2, x_3 + x_4, x_1 + x_2 + x_3 + x_4\}$. It implies that at least one of $x_1 + x_3, x_2 + x_3, x_1 + x_4, x_2 + x_4$ is 0.

If $x_1 + x_3 = 0$, then $x_1 = x_3 \in \mathbb{F}_2^{I_0} \cap \mathbb{F}_2^{J_0} = \mathbb{F}_2^{I_0 \cap J_0}$, which has $2^{|I_0 \cap J_0|} < 2^{(1/9+0.01)n}$ possible values. Together with $Ax_1 + d_1 = Ax_3 + d_3$, $d_1 = d_3$ and similarly $d_1 = d_3$ has no more than $2^{(1/9+0.01)n}$ possible values. x_2, x_4, d_2, d_4 each have less than $2^{(1/3+0.03)n}$ possible values. In total, in this case there are no more than $2^{2(1/9+0.01)n+4(1/3+0.03)n} = 2^{(14/9+0.14)n}$ possible (x, d) 's.

The cases for $x_2 + x_3 = 0$, $x_1 + x_4 = 0$, and $x_2 + x_4 = 0$ are similar. Therefore,

$$\sum_{\substack{x,d:k_{x,d}=2 \\ x_1+x_2 \neq x_3+x_4}} p_{x,d} \leq \sum_{\substack{x,d:k_{x,d}=1, p_{x,d} \neq 0 \\ x_1+x_2 \neq x_3+x_4}} \mathcal{O}(2^{-2n}) < 4 \times 2^{(14/9+0.14)n} \mathcal{O}(2^{-2n}) = \exp[-\Omega(n)]. \quad (\text{F61})$$

In conclusion,

$$\Pr_A[V_{f_0} \cap V_{f_1} \cap V_{g_0} \cap V_{g_1} \neq \{0\}] \leq \sum_{x,d} p_{x,d} \leq \exp[-\Omega(n)] \quad (\text{F62})$$

whenever $|I_k \cap J_{k'}| < (\frac{1}{9} + 0.01)n$ for all $k, k' \in \{0, 1, 2\}$ (which happens with probability $1 - \exp[-\Omega(n)]$ under the randomness of p, q). After including the randomness of p, q and applying union bound, we have

$$\mathbb{E}_A[X] = \Pr_{p,q,A}[V_{f_0} \cap V_{f_1} \cap V_{g_0} \cap V_{g_1} \neq \{0\}] \leq \exp[-\Omega(n)]. \quad (\text{F63})$$

By Markov's inequality,

$$\Pr_A[T \text{ does not happen}] \leq \Pr[X > c_2^2] \leq c_2^{-2} \mathbb{E}_A[X] \leq \exp[-\Omega(n)], \quad (\text{F64})$$

which finalizes the proof. ■

3. Nonzero gap for almost all states

In this subsection, we prove that the spectral gap $\Delta(O_\psi)$ is strictly positive almost surely.

Theorem 7. Let $|\psi\rangle$ be drawn Haar randomly from the n -qubit Hilbert space $\mathcal{H}_d$ with $d = 2^n$ and $n_A \geq 1$. Then, with probability 1, $\Delta(O_\psi) > 0$.

First, we show that a Haar-random pure state is almost surely entangled.

Lemma 16. Let $|\psi\rangle$ be drawn Haar randomly from the bipartite Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ with local dimensions $d_A, d_B \geq 2$. Then, with probability 1, $|\psi\rangle$ is entangled across the cut $A|B$.

Proof. The set of all pure states in $\mathcal{H}_{AB}$, modulo a global phase, forms the complex projective space $\mathbb{CP}^{d-1}$ with real dimension $2d - 2$, where $d = d_A d_B$. In contrast, the set of product (separable) states forms the Cartesian product $\mathbb{CP}^{d_A-1} \times \mathbb{CP}^{d_B-1}$, whose real dimension is $(2d_A - 2) + (2d_B - 2)$. Because $d_A, d_B \geq 2$, we have

$$(2d_A - 2) + (2d_B - 2) < 2d_A d_B - 2, \quad (\text{F65})$$

so the manifold of separable states has strictly lower dimension than the manifold of all pure states. A lower-dimensional submanifold has Haar measure zero within the larger manifold, implying that the probability of sampling a separable state under the Haar measure is zero. Hence, a Haar-random pure state is almost surely entangled. ■

The notation O_ψ suppresses the dependence on the size n_A of subsystem A . Here, we write O_{ψ, n_A} to make this dependence explicit. We now show that, when B consists of

a single qubit (i.e., $n_A = n - 1$), the observable $O_{\psi, n-1}$ has a strictly positive spectral gap almost surely.

Lemma 17. Let $|\psi\rangle$ be drawn Haar randomly from the n -qubit Hilbert space $\mathcal{H}_{AB}$ with $n_B = 1$. Then,

$$\Delta(O_{\psi, n-1}) > 0 \quad (\text{F66})$$

with probability 1.

Proof. Lemma 16 guarantees that $|\psi\rangle$ is entangled across $A|B$ almost surely. Observe that

$$O_{\psi, n-1} = \frac{1}{3}(O_X + O_Y + O_Z), \quad (\text{F67})$$

where

$$O_Z = \psi_0 \otimes |0\rangle\langle 0| + \psi_1 \otimes |1\rangle\langle 1|, \quad (\text{F68})$$

with

$$\psi_0 = \frac{\text{tr}_B[(I_A \otimes |0\rangle\langle 0|)\psi]}{\text{tr}[(I_A \otimes |0\rangle\langle 0|)\psi]}, \quad \psi_1 = \frac{\text{tr}_B[(I_A \otimes |1\rangle\langle 1|)\psi]}{\text{tr}[(I_A \otimes |1\rangle\langle 1|)\psi]}, \quad (\text{F69})$$

and O_X and O_Y are defined analogously in the $\{|\pm\rangle\}$ and $\{|\pm i\rangle\}$ bases. Entanglement implies $\psi_0 \neq \psi_1$; otherwise, $|\psi\rangle$ would be separable.

To prove $\Delta(O_{\psi, n-1}) > 0$, we show the maximal eigenvalue of $O_{\psi, n-1}$ is nondegenerate. Suppose a pure state $|\phi\rangle$ attains this maximum so that $\text{tr}(O_{\psi, n-1}\phi) = 1$. Then,

$$\text{tr}(O_X\phi) = \text{tr}(O_Y\phi) = \text{tr}(O_Z\phi) = 1. \quad (\text{F70})$$

The condition $\text{tr}(O_Z\phi) = 1$ implies that, when subsystem B of $|\phi\rangle$ is measured in the computational basis, the projected states on subsystem A are precisely ψ_0 (for outcome $|0\rangle$) and ψ_1 (for outcome $|1\rangle$). Hence,

$$|\phi\rangle = a_0|0\rangle_B|\psi_0\rangle_A + a_1|1\rangle_B|\psi_1\rangle_A, \quad a_0, a_1 \in \mathbb{C}. \quad (\text{F71})$$

The uncertainty principle dictates that ϕ_B cannot simultaneously be an eigenstate of at least two of the operators σ_X , σ_Y , and σ_Z . Assuming without loss of generality that ϕ_B is not an eigenstate of σ_X and σ_Z , it follows that $a_0, a_1 \neq 0$. Similarly, for the entangled state $|\psi\rangle$, we have

$$|\psi\rangle = b_0|0\rangle_B|\psi_0\rangle_A + b_1|1\rangle_B|\psi_1\rangle_A, \quad b_0, b_1 \neq 0. \quad (\text{F72})$$

Next, $\text{tr}(O_X\phi) = 1$ forces the projected states of $|\phi\rangle$ and $|\psi\rangle$ after measuring B in $\{|\pm\rangle\}$ to coincide. Thus,

$$a_0|\psi_0\rangle + a_1|\psi_1\rangle \propto b_0|\psi_0\rangle + b_1|\psi_1\rangle, \quad (\text{F73})$$

so $a_0 = eb_0$ and $a_1 = eb_1$ for some $e \in \mathbb{C}$. Therefore, $|\phi\rangle = e|\psi\rangle$, and normalization implies $|e| = 1$. Hence, $|\phi\rangle$ and $|\psi\rangle$ differ only by a global phase, proving the maximum eigenvalue is nondegenerate and $\Delta(O_{\psi,n-1}) > 0$ almost surely. ■

Proof of Theorem 7. We focus on the case $n_A = 1$; the extension to $n_A > 1$ is analogous. We proceed by induction on the number of qubits, n . For the base case, $n = 2$. A Haar-random $|\psi\rangle$ on 2 qubits satisfies $\Delta(O_{\psi,1}) > 0$ almost surely by Lemma 17. When $n \geq 3$, assume $\Delta(O_{\psi,1}) > 0$ holds for $(n-1)$ -qubit Haar-random state ψ almost surely. We now show it holds for n -qubit Haar-random states.

Let $|\psi\rangle$ be Haar random on n qubits and ψ_i for $i \in \mathbf{X}$ be the projected state corresponding to Pauli-basis measurement on the n th qubit. Each projected state is Haar randomly distributed on $n-1$ qubits by unitary invariance of the Haar measure. By the induction assumption, $\Delta(O_{\psi_i,1}) > 0$ almost surely for each i . Applying union bound shows this holds simultaneously for both outcomes with probability 1.

Note that

$$O_{\psi,1} = \frac{1}{3}(\tilde{O}_X + \tilde{O}_Y + \tilde{O}_Z), \quad (\text{F74})$$

where

$$\tilde{O}_Z = O_{\psi_0,1} \otimes |0\rangle\langle 0| + O_{\psi_1,1} \otimes |1\rangle\langle 1|, \quad (\text{F75})$$

and $\tilde{O}_X$ and $\tilde{O}_Y$ are defined analogously. Suppose ϕ is any pure state satisfying $\text{tr}(O_{\psi,1}\phi) = 1$; then,

$$\text{tr}(\tilde{O}_X\phi) = \text{tr}(\tilde{O}_Y\phi) = \text{tr}(\tilde{O}_Z\phi) = 1. \quad (\text{F76})$$

Since each $O_{\psi_i,1}$ satisfies $\Delta(O_{\psi_i,1}) > 0$, the above equalities imply

$$\text{tr}(O_X\phi) = \text{tr}(O_Y\phi) = \text{tr}(O_Z\phi) = 1, \quad (\text{F77})$$

which then implies $\phi = \psi$, with the same reasoning as in Lemma 17. Hence, the maximal eigenvalue of $O_{\psi,1}$ is nondegenerate almost surely. ■

4. Proof of Theorem 5

We first introduce the notation that is used extensively throughout this proof. Let $m = n_B = n - 1$ denote the number of qubits in the complementary subsystem, and define the corresponding Hilbert space dimension as $D = 2^m$. We denote the set of single-qubit Pauli basis states as $\mathbf{X} = \{0, 1, +, -, +i, -i\}$, and define the corresponding projectors as $\pi_x = |x\rangle\langle x|$ for $x \in \mathbf{X}^m$. Let $\mu = 3^{-m}$ denotes a uniform weight, which corresponds to the probability of selecting a specific Pauli basis. Consequently,

$$\sum_{x \in \mathbf{X}^m} \mu \pi_x = I_D. \quad (\text{F78})$$

We express the target pure state $|\psi\rangle$ as

$$|\psi\rangle = |0\rangle|u\rangle + |1\rangle|v\rangle, \quad \text{with } \|u\|^2 + \|v\|^2 = 1. \quad (\text{F79})$$

Consider an arbitrary state $|\phi\rangle = |0\rangle|a\rangle + |1\rangle|b\rangle$. For any measurement outcome x , define the amplitude $u_x = \langle x|u\rangle$ (with analogous definitions for v_x , a_x , and b_x), and let

$$p_x = |u_x|^2 + |v_x|^2, \quad d_x = |u_x b_x - v_x a_x|^2. \quad (\text{F80})$$

For Haar-random states, $p_x \neq 0$ for all x almost surely. Direct substitution into the definition of the conditional fidelity observable O_ψ yields

$$\langle \phi|(I - O_\psi)|\phi\rangle = \sum_{x \in \mathbf{X}^m} \mu \frac{d_x}{p_x}. \quad (\text{F81})$$

To bound this gap from below, we construct an auxiliary unnormalized vector

$$|w_x\rangle = (-\overline{v_x}|0\rangle + \overline{u_x}|1\rangle) \otimes |x\rangle, \quad (\text{F82})$$

and define two positive semidefinite operators, H_0 and H_1 , as follows:

$$\begin{aligned} H_0 &= \sum_{x \in \mathbf{X}^m} \mu |w_x\rangle\langle w_x|, \\ H_1 &= \sum_{x \in \mathbf{X}^m} \mu p_x |w_x\rangle\langle w_x|. \end{aligned} \quad (\text{F83})$$

By construction, $\langle \phi|H_0|\phi\rangle = \sum_x \mu d_x$ and $\langle \phi|H_1|\phi\rangle = \sum_x \mu p_x d_x$. Applying the Cauchy-Schwarz inequality,

we can lower bound the spectral gap as follows:

$$\langle \phi | (I - O_\psi) | \phi \rangle \geq \frac{\langle \phi | H_0 | \phi \rangle^2}{\langle \phi | H_1 | \phi \rangle}. \quad (\text{F84})$$

The problem is, thus, reduced to bounding the operators H_0 and H_1 . We accomplish this through the following two lemmas.

Lemma 18. With probability at least $1 - \exp[-\Omega(m)]$ over the Haar-random choice of $|\psi\rangle$, the kernel of H_0 is spanned exclusively by the target state (i.e., $\ker H_0 = \mathbb{C}|\psi\rangle$), and its smallest nonzero eigenvalue is bounded from below by

$$\lambda_{\min}^+(H_0) \geq \frac{c}{D},$$

where $c > 0$ is a universal constant.

Lemma 19. With probability at least $1 - \exp[-\Omega(m)]$ over the Haar-random choice of $|\psi\rangle$, the maximum eigenvalue of H_1 is bounded from above by

$$H_1 \leq \frac{C}{D^2} I,$$

where $C > 0$ is a universal constant.

By substituting Lemmas 18 and 19 into Eq. (F84), we establish Theorem 5. In the remainder of this section, we provide the detailed proofs for these two lemmas.

5. Proof of Lemma 18

In this subsection, we present the proof of Lemma 18. We begin by introducing several standard concentration

inequalities concerning Gaussian random matrices. Next, we demonstrate that the operator H_0 can be expressed in a specific Gaussian matrix form. Finally, we separately bound the diagonal and off-diagonal blocks of H_0 , synthesizing these bounds to establish the lemma.

a. Gaussian random matrices

Let $Z \sim \mathcal{N}_{\mathbb{C}}(0, 1)$ denote a standard complex Gaussian random variable, defined as $Z = (\xi + i\eta)/\sqrt{2}$, where ξ and η are independent standard real Gaussian variables distributed as $\mathcal{N}(0, 1)$. Accordingly, an $r \times s$ standard complex Gaussian matrix is defined as a matrix whose entries are i.i.d. standard complex Gaussian variables. The singular values of such matrices satisfy the following bounds.

Fact 3 [Singular value concentration (Proposition 6.33 in Ref. [137])]. There exists a universal constant $c > 0$. Let G be an $s \times n$ standard complex Gaussian matrix with $s \geq n$. Then, for any $t > 0$, the largest singular value $\|G\|$ satisfies

$$\Pr[\|G\| \geq \sqrt{s} + \sqrt{n} + t] \leq e^{-ct^2}. \quad (\text{F85})$$

If $s > n$, then for every $t > 4\sqrt{2\log n}/(\sqrt{s/n} - 1)$, the smallest singular value $s_{\min}(G)$ satisfies

$$\Pr[s_{\min}(G) \leq \sqrt{s} - \sqrt{n} - t] \leq e^{-ct^2}. \quad (\text{F86})$$

Lemma 20 (Linear summations). Let $\{\gamma_j\}$ be a sequence of independent standard complex Gaussian variables, and let $\{A_j\}$ be a sequence of matrices, each of dimension at most $D \times D$. Then, for any $p \geq 2$,

$$\left(\mathbb{E} \left\| \sum_j \gamma_j A_j \right\|^p \right)^{1/p} \leq C\sqrt{p}D^{1/p} \max \left\{ \left\| \sum_j A_j A_j^\dagger \right\|^{1/2}, \left\| \sum_j A_j^\dagger A_j \right\|^{1/2} \right\}, \quad (\text{F87})$$

where $C > 0$ is a universal constant.

Proof. Let $\|T\|_{S_p} = (\text{tr}|T|^p)^{1/p}$ denote the Schatten- p norm of a matrix T . For any matrix of dimension at most $D \times D$, the standard operator norm is bounded by the Schatten- p norm such that $\|T\| \leq \|T\|_{S_p} \leq D^{1/p}\|T\|$. Then, we can bound the expectation as follows:

$$\begin{aligned} \left(\mathbb{E} \left\| \sum_j \gamma_j A_j \right\|^p \right)^{1/p} &\leq \left(\mathbb{E} \left\| \sum_j \gamma_j A_j \right\|_{S_p}^p \right)^{1/p} \\ &\leq C\sqrt{p} \max \left\{ \left\| \left(\sum_j A_j A_j^\dagger \right)^{1/2} \right\|_{S_p}, \left\| \left(\sum_j A_j^\dagger A_j \right)^{1/2} \right\|_{S_p} \right\} \\ &\leq C\sqrt{p}D^{1/p} \max \left\{ \left\| \sum_j A_j A_j^\dagger \right\|^{1/2}, \left\| \sum_j A_j^\dagger A_j \right\|^{1/2} \right\}. \end{aligned} \quad (\text{F88})$$

Here, the second inequality follows directly from the noncommutative Khintchine inequality (see Proposition 19 and Corollary 20 in Ref. [138]). ■

Lemma 21 (Complex Hanson-Wright inequality). Let $g \in \mathbb{C}^D$ be a standard complex Gaussian random vector, and let $A \in \mathbb{C}^{D \times D}$. Then, for any $t > 0$,

$$\Pr(|g^\dagger A g - \mathbb{E}[g^\dagger A g]| > t) \leq 4 \exp \left(-c \min \left\{ \frac{t^2}{\|A\|_F^2}, \frac{t}{\|A\|} \right\} \right), \quad (\text{F89})$$

where $c > 0$ is a universal constant and $\|A\|_F$ denotes the Frobenius norm of A .

Proof. We first reduce the complex quadratic form to a real one. Let $g = x + iy$, where $x, y \sim \mathcal{N}(0, I_D/2)$ are independent real Gaussian vectors. We define a $2D$ -dimensional standard real Gaussian vector $w = \sqrt{2}(x \oplus y) \sim \mathcal{N}(0, I_{2D})$.

By decomposing the matrix $A = A_R + iA_I$ into its real and imaginary parts, the quadratic form can be expanded as

$$g^\dagger A g = \frac{1}{2} w^T \tilde{A} w + i \frac{1}{2} w^T \tilde{B} w, \quad (\text{F90})$$

where

$$\tilde{A} = \begin{pmatrix} A_R & -A_I \\ A_I & A_R \end{pmatrix}, \quad \tilde{B} = \begin{pmatrix} A_I & A_R \\ -A_R & A_I \end{pmatrix} \quad (\text{F91})$$

are deterministic real $2D \times 2D$ matrices.

Applying the standard real Hanson-Wright inequality (see, e.g., Theorem 1.1 in Ref. [139]) to the real part $\frac{1}{2} w^T \tilde{A} w$, we obtain

$$\begin{aligned} \Pr(|w^T \tilde{A} w - \mathbb{E}[w^T \tilde{A} w]| > t) \\ \leq 2 \exp \left(-c \min \left\{ \frac{t^2}{\|\tilde{A}\|_F^2}, \frac{t}{\|\tilde{A}\|} \right\} \right), \end{aligned} \quad (\text{F92})$$

and a similar bound applies to $\tilde{B}$. Because the spectrum of $\tilde{A}$ (and analogously $\tilde{B}$) exactly matches the spectrum of A up to doubled multiplicities, their respective norms satisfy

$$\|\tilde{A}\| = \|A\|, \quad \|\tilde{A}\|_F^2 = 2\|A\|_F^2. \quad (\text{F93})$$

Therefore, the concentration bound for the real part scales directly with $\|A\|$ and $\|A\|_F$. Applying an identical argument to the imaginary part $\frac{1}{2} w^T \tilde{B} w$ and taking a union bound over both components yields the desired exponential tail bound, absorbing the scalar factors into the universal constant c . ■

b. Matrix representation of H_0

We define the channel Λ as

$$\Lambda(X) = \sum_{x \in X^m} \mu\langle x|X|x\rangle \pi_x. \quad (\text{F94})$$

For a single qubit, this channel takes the form $\Lambda_1(X) = [X + \text{tr}(X)I]/3$. Since $\Lambda = \Lambda_1^{\otimes m}$, we can expand this operator over subsets of qubits as

$$\Lambda(X) = 3^{-m} \sum_{S \subseteq [m]} \text{tr}_{S^c}(X) \otimes I_{S^c}. \quad (\text{F95})$$

Furthermore, utilizing the single-qubit identity $\sum_{P \in \mathcal{P}_1} PXP = 2\text{tr}(X)I_2$, we can alternatively express $\Lambda(X)$ as a Pauli channel:

$$\Lambda(X) = \sum_{P \in \mathcal{P}_m} p_P PXP, \quad p_P = D^{-1} 3^{-\text{wt}(P)}, \quad (\text{F96})$$

where $\mathcal{P}_m = \{I, X, Y, Z\}^{\otimes m}$ denotes the m -qubit Pauli group and $\text{wt}(P)$ is the Pauli weight of operator P .

Let $g, h \in \mathbb{C}^D$ be independent standard complex Gaussian vectors. Define $T = \|g\|^2 + \|h\|^2$, and set the normalized vectors as $u = g/\sqrt{T}$ and $v = h/\sqrt{T}$. The projector $|w_x\rangle\langle w_x|$ can be written in block matrix form with respect to the bipartition as

$$|w_x\rangle\langle w_x| = \begin{pmatrix} \langle x|vv^\dagger|x\rangle & -\langle x|uv^\dagger|x\rangle \\ -\langle x|vu^\dagger|x\rangle & \langle x|uu^\dagger|x\rangle \end{pmatrix} \otimes \pi_x. \quad (\text{F97})$$

Consequently, the operator H_0 can be expressed compactly using the map Λ :

$$\begin{aligned} H_0 &= \begin{pmatrix} \sum_x \mu\langle x|vv^\dagger|x\rangle \pi_x & -\sum_x \mu\langle x|uv^\dagger|x\rangle \pi_x \\ -\sum_x \mu\langle x|vu^\dagger|x\rangle \pi_x & \sum_x \mu\langle x|uu^\dagger|x\rangle \pi_x \end{pmatrix} \\ &= \frac{1}{T} \begin{pmatrix} \Lambda(hh^\dagger) & -\Lambda(gh^\dagger) \\ -\Lambda(hg^\dagger) & \Lambda(gg^\dagger) \end{pmatrix}. \end{aligned} \quad (\text{F98})$$

c. Diagonal blocks

We first analyze the diagonal block $\Lambda(gg^\dagger)$. For any subset $S \subseteq [m]$, let G_S denote the Gaussian matrix obtained by reshaping the vector g across the bipartition $S|S^c$. Using the subset expansion of Λ , we have

$$\begin{aligned} \Lambda(gg^\dagger) &= 3^{-m} \sum_S \text{tr}_{S^c}(gg^\dagger) \otimes I_{S^c} \\ &= 3^{-m} \sum_S G_S G_S^\dagger \otimes I_{S^c}. \end{aligned} \quad (\text{F99})$$

Setting $t = C'\sqrt{m}$ for a sufficiently large constant C' , we apply Fact 3. A union bound ensures that with probability at least $1 - e^{-\Omega(m)}$, the operator norm bound $\|G_S\| \leq \sqrt{2^{|S|}} + \sqrt{2^{m-|S|}} + t$ holds simultaneously for all 2^m subsets. Consequently,

$$\|\Lambda(gg^\dagger)\| \lesssim 3^{-m} \sum_S (2^{|S|} + 2^{m-|S|} + C'm) = \mathcal{O}(1), \quad (\text{F100})$$

where $A \lesssim B$ denotes $A \leq cB$ for some absolute constant $c > 0$.

To lower-bound the smallest singular value, we rewrite Eq. (F99) as a convex combination:

$$\Lambda(gg^\dagger) = \sum_S q_S \left(\frac{G_S G_S^\dagger}{2^{m-|S|}} \right) \otimes I_{S^c}, \quad q_S = (1/3)^{|S|} (2/3)^{m-|S|}. \quad (\text{F101})$$

The coefficients q_S correspond to a binomial distribution over the subsets S , where each element is included independently with probability $1/3$. By standard concentration bounds, the total probability mass on subsets sized $m/4 \leq |S| \leq 5m/12$ is $1 - e^{-\Omega(m)}$. Uniformly over these typical subsets, Fact 3 guarantees that $s_{\min}(G_S G_S^\dagger / 2^{m-|S|}) \geq 1 - o(1)$. Therefore, with probability at least $1 - e^{-\Omega(m)}$, we obtain

$$s_{\min}[\Lambda(gg^\dagger)] \geq 1 - o(1). \quad (\text{F102})$$

The same analysis also applies to the vector h . Combining the above, we conclude that with probability at least $1 - e^{-\Omega(m)}$, both diagonal blocks satisfy

$$[1 - o(1)]I \leq \Lambda(gg^\dagger), \quad \Lambda(hh^\dagger) \leq CI. \quad (\text{F103})$$

d. The off-diagonal block

We now analyze the off-diagonal block $B = \Lambda(gh^\dagger)$. By Eq. (F96), we can expand B as

$$B = D^{-1}gh^\dagger + \sum_{P \neq I} p_P Pgh^\dagger P. \quad (\text{F104})$$

We choose a cutoff weight $r = C_0 \log m$ for a sufficiently large constant C_0 and split the summation into low-weight and high-weight Pauli contributions:

$$E_L = \sum_{1 \leq \text{wt}(P) \leq r} p_P Pgh^\dagger P, \quad E_H = \sum_{\text{wt}(P) > r} p_P Pgh^\dagger P. \quad (\text{F105})$$

The number of Pauli operators with weight at most r is bounded by $\exp(\mathcal{O}[(\log m)^2]) = D^{o(1)}$.

We define the matrix $G := [Pg]_P$, where each column is given by Pg for $0 \leq \text{wt}(P) \leq r$. Setting $t = D^{2/3}$ and applying Lemma 21, we can bound the matrix entries $(G^\dagger G)_{PQ} = g^\dagger P Q g$:

$$\Pr(|(G^\dagger G)_{PQ} - \delta_{PQ} D| > t) = e^{-\Omega(D^{1/3})}. \quad (\text{F106})$$

Taking a union bound over all such P and Q , Eq. (F106) holds uniformly for all pairs with probability at least $1 - e^{-D^{\Omega(1)}}$. An analogous concentration bound applies to the matrix $H := [Ph]_P$. Applying Gershgorin's circle theorem to the rows of $G^\dagger G$ and $H^\dagger H$, the entrywise bounds imply that the spectra are highly concentrated around D :

$$D^{-1}G^\dagger G = [1 + o(1)]I, \quad D^{-1}H^\dagger H = [1 + o(1)]I. \quad (\text{F107})$$

The low-weight component can be factored as $E_L = GWH^\dagger$, where W is a diagonal matrix with $W_{PP} = p_P$ for $P \neq I$ and $W_{II} = 0$. Because $\max_{P \neq I} p_P = 1/(3D)$, we can bound the operator norm as

$$\begin{aligned} \|E_L\| &\leq \|G\| \|W\| \|H\| \\ &\leq \sqrt{D[1 + o(1)]} \cdot \frac{1}{3D} \cdot \sqrt{D[1 + o(1)]} \\ &= \frac{1}{3} + o(1). \end{aligned} \quad (\text{F108})$$

For the high-weight component E_H , we write

$$E_H = \sum_j \bar{h}_j A_j, \quad A_j = \sum_{\text{wt}(P) > r} p_P P g e_j^\dagger P. \quad (\text{F109})$$

We aim to bound E_H using Lemma 20. First, with probability at least $1 - e^{-\Omega(m)}$, we have

$$\begin{aligned} \sum_j A_j A_j^\dagger &= \sum_j \sum_{\text{wt}(P), \text{wt}(Q) > r} p_P p_Q P g e_j^\dagger P Q e_j g^\dagger Q \\ &= D \sum_{\text{wt}(P) > r} p_P^2 P g g^\dagger P \\ &\leq 3^{-r} \sum_P p_P P g g^\dagger P \\ &= 3^{-r} \Lambda(gg^\dagger) \\ &\leq C 3^{-r} I, \end{aligned} \quad (\text{F110})$$

where the final inequality follows from Eq. (F103).

To bound $\sum_j A_j^\dagger A_j$, we introduce

$$A_j^{\text{all}} = \sum_{P \in \mathcal{P}_m} p_P P g e_j^\dagger P, \quad A_j^{\leq r} = \sum_{\text{wt}(P) \leq r} p_P P g e_j^\dagger P. \quad (\text{F111})$$

Evaluating the full summation yields

$$\begin{aligned}
\sum_j (A_j^{\text{all}})^\dagger A_j^{\text{all}} &= \sum_{P,Q} p_P p_Q Q \left(\sum_j e_j g^\dagger Q P g e_j^\dagger \right) P \\
&= \sum_{P,Q} p_P p_Q (g^\dagger Q P g) Q P \\
&= \sum_R \left(\sum_{P,Q: QP=\omega R} p_P p_Q \omega^2 \right) (g^\dagger R g) R \\
&= \sum_R c_R (g^\dagger R g) R, \tag{F112}
\end{aligned}$$

where $c_R := \sum_{P,Q: QP=\omega R} p_P p_Q \omega^2$.

For single-qubit Paulis, these coefficients evaluate to

$$c_I = \frac{1}{4} + \frac{3}{36} = \frac{1}{3}, \quad c_X = c_Y = c_Z = 2 \frac{1}{2} \frac{1}{6} - 2 \frac{1}{36} = \frac{1}{9}. \tag{F113}$$

Consequently,

$$\begin{aligned}
\sum_R c_R (g^\dagger R g) R &= \frac{1}{3} \|g\|^2 I \\
&\quad + \frac{1}{9} [(g^\dagger X g) X + (g^\dagger Y g) Y + (g^\dagger Z g) Z] \\
&= \frac{1}{3} \|g\|^2 I + \frac{1}{9} (2gg^\dagger - \|g\|^2 I) \\
&= \frac{2}{3} \left(\frac{\|g\|^2 I + gg^\dagger}{3} \right) = \frac{2}{3} \Lambda_1(gg^\dagger), \tag{F114}
\end{aligned}$$

where we utilized the identity $\sum_{P \in \mathcal{P}_1} (g^\dagger P g) P = 2gg^\dagger$ alongside Eq. (F95). Substituting this into Eq. (F112), we obtain

$$\sum_j (A_j^{\text{all}})^\dagger A_j^{\text{all}} = (2/3)^m \Lambda(gg^\dagger). \tag{F115}$$

Similarly, for the low-weight component, we have

$$\begin{aligned}
\sum_j (A_j^{\leq r})^\dagger A_j^{\leq r} &= \sum_{\text{wt}(P), \text{wt}(Q) \leq r} p_P p_Q (g^\dagger Q P g) Q P \\
&= \sum_{\text{wt}(P), \text{wt}(Q) \leq r} p_P p_Q (G^\dagger G)_{QP} Q P \\
&\leq D[1 + o(1)] \sum_{\text{wt}(P) \leq r} p_P^2 I \\
&\leq D^{-1+o(1)} [1 + o(1)] I, \tag{F116}
\end{aligned}$$

where the first inequality uses Eq. (F107).

Because $A_j = A_j^{\text{all}} - A_j^{\leq r}$, we can apply the Loewner inequality $(X - Y)^\dagger (X - Y) \leq 2X^\dagger X + 2Y^\dagger Y$. Combined with Eq. (F103), this ensures that with probability at least $1 - e^{-\Omega(m)}$,

$$\left\| \sum_j A_j^\dagger A_j \right\| \leq 2(2/3)^m \|\Lambda(gg^\dagger)\| + 2D^{-1+o(1)} = e^{-\Omega(m)}. \tag{F117}$$

Combining Eq. (F110), Eq. (F117), and Lemma 20 evaluated at $p = m$, we obtain

$$(\mathbb{E} \|E_H\|^m)^{1/m} := \epsilon = o(1) \tag{F118}$$

with probability $1 - e^{-\Omega(m)}$. Conditional on this event, applying Markov's inequality yields

$$\begin{aligned}
\Pr[\|E_H\| \geq \epsilon] &= \Pr[\|E_H\|^m \geq \epsilon^m \epsilon^m] \\
&\leq \frac{\epsilon^m}{\epsilon^m \epsilon^m} = e^{-m}. \tag{F119}
\end{aligned}$$

Therefore, a union bound guarantees that $\|E_H\| = o(1)$ with probability at least $1 - e^{-\Omega(m)}$. We now combine this result with the decomposition of B in Eqs. (F104) and (F108). Applying the Eckart-Young inequality, the second singular value of B is bounded by

$$s_2(B) \leq \|E_L\| + \|E_H\| = \frac{1}{3} + o(1). \tag{F120}$$

Let $A = \Lambda(hh^\dagger)$, $C = \Lambda(gg^\dagger)$, $K = A^{-1/2} B C^{-1/2}$, $M = \begin{pmatrix} I & -K \\ -K^\dagger & I \end{pmatrix}$, and $D_0 = \text{diag}(A^{1/2}, C^{1/2})$. Then, the second singular value of K satisfies

$$s_2(K) \leq \|A^{-1/2}\| \|C^{-1/2}\| s_2(B) \leq \frac{1}{3} + o(1) < \frac{1}{2}. \tag{F121}$$

Moreover, by Eq. (F98), H_0 factorizes as $H_0 = (1/T) D_0 M D_0$, and by its definition in Eq. (F83), $H_0(|0\rangle g + |1\rangle |h\rangle) = 0$. Consequently, K has its largest singular value $s_1(K) = 1$. Thus, H_0 has a one-dimensional kernel, and the smallest nonzero eigenvalue of M is bounded by $\lambda_{\min}^+(M) = 1 - s_2(K) > 1/2$.

Furthermore, the nonzero spectrum of $D_0 M D_0$ is identical to the nonzero spectrum of $M^{1/2} D_0^2 M^{1/2}$. Since the diagonal blocks satisfy $D_0^2 \geq (1 - o(1))I$, we have

$$\lambda_{\min}^+(H_0) \geq \frac{1}{T} \lambda_{\min}(D_0)^2 \lambda_{\min}^+(M) = \Omega(T^{-1}). \tag{F122}$$

Finally, by Fact 3, the normalization constant

$$T = \|g\|^2 + \|h\|^2 = \Theta(D) \tag{F123}$$

except with probability e^{-cD} . This establishes the lower bound $\lambda_{\min}^+(H_0) \geq \Omega(D^{-1})$ and completes the proof of Lemma 18.

6. Proof of Lemma 19

In this subsection, we present the proof of Lemma 19. We begin by introducing several integration tools for complex Gaussian random variables, which we subsequently use to calculate matrix moments. These tools primarily rely on Wick ordering and the Wick formula.

a. Wick ordering and Wick formula

A family of complex random variables $\{Z_1, \dots, Z_r\}$ is termed *proper* if

$$\mathbb{E}[Z_i Z_j] = 0 \quad \forall i, j. \quad (\text{F124})$$

For the standard complex Gaussian vector $g \sim \mathcal{N}_{\mathbb{C}}(0, I_D)$ introduced above, $\mathbb{E}[gg^T] = 0$. Hence, for any set of unit vectors $\{x_1, \dots, x_r\}$, the random variables

$$g_{x_i} := \langle x_i | g \rangle \quad (\text{F125})$$

form a proper standard complex Gaussian family with covariance

$$C_{ij} := \mathbb{E}[g_{x_i} \overline{g_{x_j}}] = \langle x_i | x_j \rangle. \quad (\text{F126})$$

For a standard proper complex Gaussian variable Z , its Wick-ordered monomials are defined via the generating function

$$\exp(sZ + t\bar{Z} - st) = \sum_{p, q \geq 0} \frac{s^p t^q}{p! q!} : Z^p \bar{Z}^q :. \quad (\text{F127})$$

In particular [see Eqs. (1.2) and (1.3) in Ref. [140]], the quartic Wick polynomial is given by

$$: Z^2 \bar{Z}^2 : = |Z|^4 - 4|Z|^2 + 2. \quad (\text{F128})$$

The key tool we use is the following formula.

Lemma 22 (Wick formula). Let $Z_1, \dots, Z_r$ be jointly proper standard complex Gaussian variables, and let $C_{ij} = \mathbb{E}[Z_i \bar{Z}_j]$. For non-negative integers p_i and q_i , let $\mathcal{M}(\mathbf{p}, \mathbf{q})$ be the set of matrices $N = (n_{ij})_{i,j=1}^r$ with non-negative integer entries satisfying the constraints

$$n_{ii} = 0, \quad \sum_j n_{ij} = p_i, \quad \sum_i n_{ij} = q_j. \quad (\text{F129})$$

Then,

$$\mathbb{E} \prod_{i=1}^r : Z_i^{p_i} \bar{Z}_i^{q_i} : = \sum_{N \in \mathcal{M}(\mathbf{p}, \mathbf{q})} \frac{\prod_{i=1}^r p_i! q_i!}{\prod_{i \neq j} n_{ij}!} \prod_{i \neq j} C_{ij}^{n_{ij}}. \quad (\text{F130})$$

Proof. This formula follows directly by extracting the coefficients of $\prod_i s_i^{p_i} t_i^{q_i}$ on both sides of the generating

function identity. Utilizing the properness and unit variance of the variables, we have

$$\begin{aligned} \mathbb{E} \prod_{i=1}^r \exp(s_i Z_i + t_i \bar{Z}_i - s_i t_i) &= \exp\left(\sum_{i,j} s_i C_{ij} t_j - \sum_i s_i t_i\right) \\ &= \exp\left(\sum_{i \neq j} s_i C_{ij} t_j\right). \end{aligned} \quad (\text{F131})$$

Here, the first equality uses the standard moment generating function identity $\mathbb{E}[\exp(A)] = \exp(\frac{1}{2} \mathbb{E}[A^2])$ for a zero-mean Gaussian exponent A . Expanding the left-hand side using Eq. (F127), the coefficient of $\prod_i s_i^{p_i} t_i^{q_i}$ is exactly

$$\frac{1}{\prod_i p_i! q_i!} \mathbb{E} \prod_{i=1}^r : Z_i^{p_i} \bar{Z}_i^{q_i} :. \quad (\text{F132})$$

Expanding the right-hand side of Eq. (F131) as a multi-variate Taylor series, we obtain

$$\begin{aligned} \exp\left(\sum_{i \neq j} s_i C_{ij} t_j\right) &= \prod_{i \neq j} \sum_{n_{ij}=0}^{\infty} \frac{(s_i C_{ij} t_j)^{n_{ij}}}{n_{ij}!} \\ &= \sum_N \frac{\prod_{i \neq j} C_{ij}^{n_{ij}}}{\prod_{i \neq j} n_{ij}!} \prod_i s_i^{\sum_j n_{ij}} \prod_j t_j^{\sum_i n_{ij}}, \end{aligned} \quad (\text{F133})$$

where the sum runs over all matrices N with zero diagonal ($n_{ii} = 0$). Matching the powers of s_i and t_j on both sides imposes the exact constraints $\sum_j n_{ij} = p_i$ and $\sum_i n_{ij} = q_j$, which directly recovers Eq. (F130). ■

Equivalently, the Wick formula can be interpreted through a labeled-diagrammatic representation: each block i possesses p_i labeled slots and q_i labeled antislots. A directed edge $i \rightarrow j$ pairs one slot of each type and contributes a factor of C_{ij} . The condition $n_{ii} = 0$ removes all internal edges within each block i .

b. Concentration of H_1

We define

$$\tilde{R}_g := \sum_{x \in X^m} \mu |g_x|^4 \pi_x, \quad g_x = \langle x | g \rangle. \quad (\text{F134})$$

Next, we use the quartic Wick polynomial $\mathfrak{h}(z)$ and its corresponding operator sum Z_g :

$$\mathfrak{h}(z) := : z^2 \bar{z}^2 : = |z|^4 - 4|z|^2 + 2, \quad Z_g := \sum_{x \in X^m} \mu \mathfrak{h}(g_x) \pi_x. \quad (\text{F135})$$

Because $\sum_x \mu \pi_x = I_D$, we obtain the decomposition

$$\tilde{R}_g = Z_g + 4\Lambda(gg^\dagger) - 2I_D. \quad (\text{F136})$$

The operator norm of $\Lambda(gg^\dagger)$ is already bounded by Eq. (F103). Thus, it suffices to bound Z_g .

Let S_g denote the squared Frobenius norm of Z_g :

$$S_g := \|Z_g\|_F^2 = \sum_{x,y \in \mathbf{X}^m} \mu^2 \mathfrak{h}(g_x) \mathfrak{h}(g_y) |\langle x|y \rangle|^2. \quad (\text{F137})$$

For any fixed pair of outcomes x and y , we evaluate the expectation using Lemma 22 with two blocks, setting $p_i = q_i = 2$. This leaves exactly two edges from the first block to the second and two in the reverse direction. Therefore,

$$\begin{aligned} \mathbb{E}[\mathfrak{h}(g_x) \mathfrak{h}(g_y)] &= (2!)^2 \mathbb{E}[g_x \bar{g}_y]^2 \mathbb{E}[g_y \bar{g}_x]^2 \\ &= 4 |\langle x|y \rangle|^4. \end{aligned} \quad (\text{F138})$$

Consequently, taking the expectation over S_g factors into a tensor product structure:

$$\begin{aligned} \mathbb{E}[S_g] &= 4 \sum_{x,y \in \mathbf{X}^m} \mu^2 |\langle x|y \rangle|^6 \\ &= 4 [3^{-2} \sum_{a,b \in \mathbf{X}} |\langle a|b \rangle|^6]^m \\ &= 4. \end{aligned} \quad (\text{F139})$$

The final equality follows by analyzing the single-qubit overlaps. For any fixed basis state $a \in \mathbf{X}$, exactly one of the six Pauli states $b \in \mathbf{X}$ yields a squared overlap of 1, one yields a squared overlap of 0, and the remaining four yield a squared overlap of 1/2. Therefore, the one-qubit factor evaluates identically to $3^{-2}(6)[1 + 4(1/2)^3] = 1$.

We next bound the variance of S_g . Expanding Eq. (F137) yields

$$\begin{aligned} \text{Var}(S_g) &= \sum_{x_1, \dots, x_4 \in \mathbf{X}^m} \mu^4 |\langle x_1|x_2 \rangle|^2 |\langle x_3|x_4 \rangle|^2 \\ &\quad \times \text{Cov}[\mathfrak{h}(g_{x_1}) \mathfrak{h}(g_{x_2}), \mathfrak{h}(g_{x_3}) \mathfrak{h}(g_{x_4})]. \end{aligned} \quad (\text{F140})$$

In the labeled-diagram representation of Eq. (F130), each of the four Wick blocks contains two labeled slots and two labeled antislots, resulting in at most 8! possible diagrams. Because the covariance $\text{Cov}[\mathfrak{h}(g_{x_1}) \mathfrak{h}(g_{x_2}), \mathfrak{h}(g_{x_3}) \mathfrak{h}(g_{x_4})]$ subtracts the disconnected contributions $\mathbb{E}[\mathfrak{h}(g_{x_1}) \mathfrak{h}(g_{x_2})] \times \mathbb{E}[\mathfrak{h}(g_{x_3}) \mathfrak{h}(g_{x_4})]$, any surviving diagram must contain at least one edge crossing the bipartition $\{1, 2\}|\{3, 4\}$. Let $\mathcal{D}_{\text{surv}}$ denote the set of these surviving diagrams.

For each diagram $\beta \in \mathcal{D}_{\text{surv}}$, we define its corresponding one-qubit factor as

$$s_\beta := 3^{-4} \sum_{a_1, \dots, a_4 \in \mathbf{X}} |\langle a_1|a_2 \rangle|^2 |\langle a_3|a_4 \rangle|^2 \prod_{(i \rightarrow j) \in \beta} \langle a_i|a_j \rangle. \quad (\text{F141})$$

Because each basis state $x_i \in \mathbf{X}^m$ is a product state, the inner products perfectly tensorize over the m independent qubits. Consequently, the variance in Eq. (F140) simplifies to

$$\text{Var}(S_g) = \sum_{\beta \in \mathcal{D}_{\text{surv}}} s_\beta^m. \quad (\text{F142})$$

It remains to establish a uniform upper bound on $|s_\beta|$. We augment the eight directed Wick edges of β with the four directed edges originating from the two trace factors in Eq. (F141), namely, $1 \rightarrow 2$, $2 \rightarrow 1$, $3 \rightarrow 4$, and $4 \rightarrow 3$. By ignoring the edge orientations, this construction yields a loopless 6-regular multigraph G_β on four vertices, comprising exactly 12 edges.

Let $A_1, \dots, A_4$ be independent random variables uniformly distributed over the set of Pauli basis states $\mathbf{X}$, and define the overlap function

$$k(a, b) := |\langle a|b \rangle|. \quad (\text{F143})$$

Taking the absolute value of Eq. (F141) and applying the triangle inequality yields

$$\begin{aligned} |s_\beta| &\leq 16 I(G_\beta), \\ I(G) &:= \mathbb{E} \prod_{\{i,j\} \in E(G)} k(A_i, A_j), \end{aligned} \quad (\text{F144})$$

where the prefactor $16 = (6/3)^4$ arises from multiplying the original weight 3^{-4} by 6^4 to convert the explicit summations over the six Pauli states into expectations over the uniform random variables A_i .

For any loopless multigraph G with a maximum degree of at most six, we have the bound

$$I(G) \leq (1/4)^{|E(G)|/6}. \quad (\text{F145})$$

To establish this, we eliminate the vertices of the graph one at a time. Suppose the current vertex being removed has $r \leq 6$ remaining incident edges, and its neighboring states are fixed as $b_1, \dots, b_r$. Applying the generalized Hölder inequality yields

$$\begin{aligned} \mathbb{E}_A \prod_{\ell=1}^r k(A, b_\ell) &\leq \prod_{\ell=1}^r [\mathbb{E}_A k(A, b_\ell)^6]^{1/6} \\ &= (1/4)^{r/6}. \end{aligned} \quad (\text{F146})$$

Here, for every fixed basis state $b \in \mathbf{X}$, evaluating the sixth moment explicitly gives

$$\mathbb{E}_A k(A, b)^6 = \frac{1}{6} [1 + 4(1/2)^3] = \frac{1}{4}. \quad (\text{F147})$$

Because each edge in the multigraph is removed exactly once during this vertex elimination process, accumulating these individual bounds directly proves Eq. (F145).

We now examine the conditions for equality in Eq. (F145) for a 6-regular graph. Consider the first eliminated vertex v , which has exactly six incident edges. Achieving equality in Eq. (F146) requires the six non-negative functions $k(\cdot, b_\ell)^6$ to be strictly proportional. Because their L^1 norms are identically $1/4$, these functions must be equal, which consequently requires all six neighboring states b_ℓ to coincide.

If v were connected to two distinct neighboring vertices, those vertices would be assigned distinct random states with constant probability, rendering the Hölder inequality strict. Therefore, saturating the inequality in Eq. (F145) requires that all six edges incident on v connect to a single adjacent vertex w . Because w also has a maximum degree of six, the pair $\{v, w\}$ must form an isolated graph component.

For the specific graph G_β , applying Eq. (F145) with $|E(G_\beta)| = 12$ yields the upper bound $|s_\beta| \leq 1$. Reaching equality would force G_β to be a union of exactly two disconnected components, each consisting of two vertices joined by six edges. Because G_β is constructed with the fixed edges connecting vertices 1 and 2, as well as 3 and 4, these two isolated components must be precisely $\{1, 2\}$ and $\{3, 4\}$. However, this configuration implies that the underlying Wick diagram contains no edges crossing the bipartition $\{1, 2\}|\{3, 4\}$, which contradicts the definition of the surviving diagrams $\beta \in \mathcal{D}_{\text{surv}}$. Thus, every surviving diagram must strictly satisfy $|s_\beta| < 1$:

$$\rho := \max_{\beta \in \mathcal{D}_{\text{surv}}} |s_\beta| < 1. \quad (\text{F148})$$

Combining Eq. (F142) with the uniform bound in Eq. (F148), we obtain the variance bound:

$$\text{Var}(S_g) \leq |\mathcal{D}_{\text{surv}}| \rho^m \leq 8! \rho^m = e^{-\Omega(m)}. \quad (\text{F149})$$

Because Z_g is Hermitian, $\|Z_g\| \leq \|Z_g\|_F = \sqrt{S_g}$. Combining this with the expectation $\mathbb{E}[S_g] = 4$ from Eq. (F139), Chebyshev's inequality yields

$$\Pr[\|Z_g\| > \sqrt{5}] \leq \Pr[S_g > 5] \leq \text{Var}(S_g) = e^{-\Omega(m)}. \quad (\text{F150})$$

Substituting this bound into Eq. (F136) and utilizing the diagonal bound from Eq. (F103), we obtain

$$\|\tilde{R}_g\| \leq C \quad (\text{F151})$$

with probability at least $1 - e^{-\Omega(m)}$. The analogous bound $\|\tilde{R}_h\| \leq C$ holds for the vector h .

For the Haar-random target state $|\psi\rangle$, the outcome probabilities are given by

$$p_x = \frac{|g_x|^2 + |h_x|^2}{T}, \quad T = \|g\|^2 + \|h\|^2. \quad (\text{F152})$$

By Eq. (F123), $T = \Theta(D)$ with probability at least $1 - e^{-\Omega(D)}$. We define the composite operator

$$R_\psi := \sum_{x \in X^m} \mu p_x^2 \pi_x. \quad (\text{F153})$$

Applying $(a + b)^2 \leq 2(a^2 + b^2)$ alongside the bounds for $\tilde{R}_g$ and $\tilde{R}_h$, we can upper bound R_ψ as

$$R_\psi \leq \frac{2}{T^2} (\tilde{R}_g + \tilde{R}_h) \leq \frac{C}{D^2} I_D, \quad (\text{F154})$$

where $C > 0$ is a universal constant. This inequality holds with probability at least $1 - e^{-\Omega(m)}$.

Finally, observe that the unnormalized vector $|w_x\rangle$ satisfies $\|w_x\|^2 = p_x$ and resides entirely within the subspace $\mathbb{C}^2 \otimes \text{span}\{|x\rangle\}$. Consequently, its rank-one projector satisfies

$$p_x |w_x\rangle\langle w_x| \leq p_x^2 (I_2 \otimes \pi_x). \quad (\text{F155})$$

Summing this inequality over all outcomes x and applying Eq. (F154), we arrive at the final bound for H_1 :

$$H_1 \leq I_2 \otimes R_\psi \leq \frac{C}{D^2} I_{2D}. \quad (\text{F156})$$

This completes the proof of Lemma 19.

-
- [1] J. Haah, A. W. Harrow, Z. Ji, X. Wu, and N. Yu, *Sample-optimal tomography of quantum states*, in *Proceedings of the Forty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '16 (2016), pp. 913–925, [10.1145/2897518.2897585](#).
 - [2] P. Liu, Z. Liu, S. Chen, and X. Ma, *Fundamental limitation on the detectability of entanglement*, *Phys. Rev. Lett.* **129**, 230503 (2022).
 - [3] X.-L. Wang *et al.*, *Experimental ten-photon entanglement*, *Phys. Rev. Lett.* **117**, 210502 (2016).
 - [4] S. Cao *et al.*, *Generation of genuine entanglement up to 51 superconducting qubits*, *Nature (London)* **619**, 738 (2023).
 - [5] Y. Kim *et al.*, *Evidence for the utility of quantum computing before fault tolerance*, *Nature (London)* **618**, 500 (2023).
 - [6] R. Acharya *et al.*, *Quantum error correction below the surface code threshold*, *Nature (London)* **638**, 920 (2024).

- [7] J. Eisert, D. Hangleiter, N. Walk, I. Roth, D. Markham, R. Parekh, U. Chabaud, and E. Kashefi, *Quantum certification and benchmarking*, *Nat. Rev. Phys.* **2**, 382 (2020).
- [8] M. Kliesch and I. Roth, *Theory of quantum system certification*, *PRX Quantum* **2**, 010201 (2021).
- [9] J. Carrasco, A. Elben, C. Kokail, B. Kraus, and P. Zoller, *Theoretical and experimental perspectives of quantum verification*, *PRX Quantum* **2**, 010102 (2021).
- [10] D. Mayers and A. C. Yao, *Self testing quantum apparatus*, *Quantum Inf. Comput.* **4**, 273 (2004).
- [11] J. C. Hoke *et al.*, *Measurement-induced entanglement and teleportation on a noisy quantum processor*, *Nature (London)* **622**, 481 (2023).
- [12] P. Niroula, C. D. White, Q. Wang, S. Johri, D. Zhu, C. Monroe, C. Noel, and M. J. Gullans, *Phase transition in magic with random quantum circuits*, *Nat. Phys.* **20**, 1786 (2024).
- [13] E. Knill, D. Leibfried, R. Reichle, J. Britton, R. B. Blakestad, J. D. Jost, C. Langer, R. Ozeri, S. Seidelin, and D. J. Wineland, *Randomized benchmarking of quantum gates*, *Phys. Rev. A* **77**, 012307 (2008).
- [14] F. Arute *et al.*, *Quantum supremacy using a programmable superconducting processor*, *Nature (London)* **574**, 505 (2019).
- [15] Y. Liu, M. Otten, R. Bassirianjahromi, L. Jiang, and B. Fefferman, *Benchmarking near-term quantum computers via random circuit sampling*, *arXiv:2105.05232*.
- [16] D. K. Mark, J. Choi, A. L. Shaw, M. Endres, and S. Choi, *Benchmarking quantum simulators using ergodic quantum dynamics*, *Phys. Rev. Lett.* **131**, 110601 (2023).
- [17] J. Choi *et al.*, *Preparing random states and benchmarking with many-body quantum chaos*, *Nature (London)* **613**, 468 (2023).
- [18] A. K. Ekert, *Quantum cryptography based on Bell's theorem*, *Phys. Rev. Lett.* **67**, 661 (1991).
- [19] B. W. Reichardt, F. Unger, and U. V. Vazirani, *Classical command of quantum systems*, *Nature (London)* **496**, 456 (2013).
- [20] M. Liu *et al.*, *Certified randomness using a trapped-ion quantum processor*, *Nature (London)* **640**, 343 (2025).
- [21] S. T. Flammia and Y.-K. Liu, *Direct fidelity estimation from few Pauli measurements*, *Phys. Rev. Lett.* **106**, 230501 (2011).
- [22] S. Pallister, N. Linden, and A. Montanaro, *Optimal verification of entangled states with local measurements*, *Phys. Rev. Lett.* **120**, 170502 (2018).
- [23] Y. Takeuchi and T. Morimae, *Verification of many-qubit states*, *Phys. Rev. X* **8**, 021060 (2018).
- [24] A. Elben, B. Vermersch, R. van Bijnen, C. Kokail, T. Brydges, C. Maier, M. K. Joshi, R. Blatt, C. F. Roos, and P. Zoller, *Cross-platform verification of intermediate scale quantum devices*, *Phys. Rev. Lett.* **124**, 010504 (2020).
- [25] M. Zwerger, W. Dür, J.-D. Bancal, and P. Sekatski, *Device-independent detection of genuine multipartite entanglement for all pure states*, *Phys. Rev. Lett.* **122**, 060502 (2019).
- [26] A. Rodriguez-Blanco, A. Bermudez, M. Müller, and F. Shahandeh, *Efficient and robust certification of genuine multipartite entanglement in noisy quantum error correction circuits*, *PRX Quantum* **2**, 020304 (2021).
- [27] H.-Y. Huang, J. Preskill, and M. Soleimanifar, *Certifying almost all quantum states with few single-qubit measurements*, *Nat. Phys.* **21**, 1834 (2025).
- [28] M. Gupta, W. He, and R. O'Donnell, *Few single-qubit measurements suffice to certify any quantum state*, in *Proceedings of the 58th Annual ACM Symposium on Theory of Computing*, STOC '26 (2026), pp. 54–60, [10.1145/3798129.3800726](https://doi.org/10.1145/3798129.3800726).
- [29] Y. Li and H. Zhu, *Universal and efficient quantum state verification via Schmidt decomposition and mutually unbiased bases*, *Quantum* **10**, 2011 (2026).
- [30] T. Haug and M. S. Kim, *Scalable measures of magic resource for quantum computers*, *PRX Quantum* **4**, 010301 (2023).
- [31] H.-Y. Huang, Y. Liu, M. Broughton, I. Kim, A. Anshu, Z. Landau, and J. R. McClean, *Learning shallow quantum circuits*, in *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*, STOC 2024 (2024), pp. 1343–1351, [10.1145/3618260.3649722](https://doi.org/10.1145/3618260.3649722).
- [32] Z. Landau and Y. Liu, *Learning quantum states prepared by shallow circuits in polynomial time*, in *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*, STOC '25 (2025), pp. 1828–1838, [10.1145/3717823.3718311](https://doi.org/10.1145/3717823.3718311).
- [33] F. Verstraete, M. Popp, and J. I. Cirac, *Entanglement versus correlations in spin systems*, *Phys. Rev. Lett.* **92**, 027901 (2004).
- [34] M. Popp, F. Verstraete, M. A. Martín-Delgado, and J. I. Cirac, *Localizable entanglement*, *Phys. Rev. A* **71**, 042306 (2005).
- [35] H.-S. Kim, I. H. Kim, and D. Ranard, *Learning state preparation circuits for quantum phases of matter*, *arXiv:2410.23544*.
- [36] J. Eisert and D. Gross, *Multi-particle entanglement*, *arXiv:quant-ph/0505149*.
- [37] J. S. Cotler, D. K. Mark, H.-Y. Huang, F. Hernández, J. Choi, A. L. Shaw, M. Endres, and S. Choi, *Emergent quantum state designs from individual many-body wave functions*, *PRX Quantum* **4**, 010311 (2023).
- [38] W. W. Ho and S. Choi, *Exact emergent quantum state designs from quantum chaotic dynamics*, *Phys. Rev. Lett.* **128**, 060601 (2022).
- [39] M. Ippoliti and W. W. Ho, *Dynamical purification and the emergence of quantum state designs from the projected ensemble*, *PRX Quantum* **4**, 030322 (2023).
- [40] R.-A. Chang, H. Shrotriya, W. W. Ho, and M. Ippoliti, *Deep thermalization under charge-conserving quantum dynamics*, *PRX Quantum* **6**, 020343 (2025).
- [41] D. K. Mark, F. Surace, A. Elben, A. L. Shaw, J. Choi, G. Refael, M. Endres, and S. Choi, *Maximum entropy principle in deep thermalization and in Hilbert-space ergodicity*, *Phys. Rev. X* **14**, 041051 (2024).
- [42] M. McGinley, *Postselection-free learning of measurement-induced quantum dynamics*, *PRX Quantum* **5**, 020347 (2024).
- [43] Z. Du, Z.-W. Liu, and X. Ma, *Spacetime quantum circuit complexity via measurements*, *arXiv:2408.16602*.
- [44] L. Piroli, G. Styliaris, and J. I. Cirac, *Quantum circuits assisted by local operations and classical communication:*

- Transformations and phases of matter*, *Phys. Rev. Lett.* **127**, 220503 (2021).
- [45] T.-C. Lu, L. A. Lessa, I. H. Kim, and T. H. Hsieh, *Measurement as a shortcut to long-range entangled quantum matter*, *PRX Quantum* **3**, 040337 (2022).
- [46] X. Chen, Z.-C. Gu, and X.-G. Wen, *Local unitary transformation, long-range quantum entanglement, wave function renormalization, and topological order*, *Phys. Rev. B* **82**, 155138 (2010).
- [47] X.-G. Wen, *Topological order: From long-range entangled quantum matter to an unification of light and electrons* *ISRN Condens. Matter Phys.* **2013**, 198710 (2013).
- [48] N. Tantivasadakarn, A. Vishwanath, and R. Verresen, *Hierarchy of topological order from finite-depth unitaries, measurement, and feedforward*, *PRX Quantum* **4**, 020339 (2023).
- [49] C. Palazuelos and J. I. d. Vicente, *Genuine multipartite entanglement of quantum states in the multiple-copy scenario*, *Quantum* **6**, 735 (2022).
- [50] S. Bravyi and A. Kitaev, *Universal quantum computation with ideal Clifford gates and noisy ancillas*, *Phys. Rev. A* **71**, 022316 (2005).
- [51] A. Coladangelo, J. Li, J. Sloate, and E. Wu, *The power of two bases: Robust and copy-optimal certification of nearly all quantum states with few-qubit measurements*, in *Proceedings of the 58th Annual ACM Symposium on Theory of Computing*, STOC '26 (2026), pp. 1771–1776, [10.1145/3798129.3800884](https://arxiv.org/abs/10.1145/3798129.3800884).
- [52] H.-Y. Huang, R. Kueng, and J. Preskill, *Predicting many properties of a quantum system from very few measurements*, *Nat. Phys.* **16**, 1050 (2020).
- [53] D. A. Abanin *et al.*, *Observation of constructive interference at the edge of quantum ergodicity*, *Nature (London)* **646**, 825 (2025).
- [54] W. Kretschmer *et al.*, *Demonstrating an unconditional separation between quantum and classical information resources*, [arXiv:2509.07255](https://arxiv.org/abs/2509.07255).
- [55] G. Vidal, *Efficient classical simulation of slightly entangled quantum computations*, *Phys. Rev. Lett.* **91**, 147902 (2003).
- [56] F. Verstraete and J. I. Cirac, *Matrix product states represent ground states faithfully*, *Phys. Rev. B* **73**, 094423 (2006).
- [57] J. Jordan, R. Orús, G. Vidal, F. Verstraete, and J. I. Cirac, *Classical simulation of infinite-size quantum lattice systems in two spatial dimensions*, *Phys. Rev. Lett.* **101**, 250602 (2008).
- [58] G. Vidal, *Class of quantum many-body states that can be efficiently simulated*, *Phys. Rev. Lett.* **101**, 110501 (2008).
- [59] F. Pan and P. Zhang, *Simulation of quantum circuits using the big-batch tensor network method*, *Phys. Rev. Lett.* **128**, 030501 (2022).
- [60] Y.-Y. Shi, L.-M. Duan, and G. Vidal, *Classical simulation of quantum many-body systems with a tree tensor network*, *Phys. Rev. A* **74**, 022320 (2006).
- [61] A. S. Darmawan and D. Poulin, *Tensor-network simulations of the surface code under realistic noise*, *Phys. Rev. Lett.* **119**, 040502 (2017).
- [62] N. Tantivasadakarn, R. Thorngren, A. Vishwanath, and R. Verresen, *Long-range entanglement from measuring symmetry-protected topological phases*, *Phys. Rev. X* **14**, 021040 (2024).
- [63] G. Carleo and M. Troyer, *Solving the quantum many-body problem with artificial neural networks*, *Science* **355**, 602 (2017).
- [64] G. Torlai, G. Mazzola, J. Carrasquilla, M. Troyer, R. Melko, and G. Carleo, *Neural-network quantum state tomography*, *Nat. Phys.* **14**, 447 (2018).
- [65] J. Carrasquilla, G. Torlai, R. G. Melko, and L. Aolita, *Reconstructing quantum states with generative models*, *Nat. Mach. Intell.* **1**, 155 (2019).
- [66] H. Hamaguchi, K. Hamada, and N. Yoshioka, *Handbook for quantifying robustness of magic*, *Quantum* **8**, 1461 (2024).
- [67] S. Aaronson, *The complexity of quantum states and transformations: From quantum money to black holes*, [arXiv:1607.05256](https://arxiv.org/abs/1607.05256).
- [68] J. Yi, W. Ye, D. Gottesman, and Z.-W. Liu, *Complexity and order in approximate quantum error-correcting codes*, *Nat. Phys.* **20**, 1798 (2024).
- [69] H. Zhao, L. Lewis, I. Kannan, Y. Quek, H.-Y. Huang, and M. C. Caro, *Learning quantum states and unitaries of bounded gate complexity*, *PRX Quantum* **5**, 040306 (2024).
- [70] F. G. S. L. Brandão, W. Chemissany, N. Hunter-Jones, R. Kueng, and J. Preskill, *Models of quantum complexity growth*, *PRX Quantum* **2**, 030316 (2021).
- [71] A. R. Brown and L. Susskind, *Second law of quantum complexity*, *Phys. Rev. D* **97**, 086015 (2018).
- [72] L. Susskind, *Black holes and complexity classes*, [arXiv:1802.02175](https://arxiv.org/abs/1802.02175).
- [73] M. Oszmaniec, M. Kotowski, M. Horodecki, and N. Hunter-Jones, *Saturation and recurrence of quantum complexity in random local quantum dynamics*, *Phys. Rev. X* **14**, 041068 (2024).
- [74] M. B. Hastings and X.-G. Wen, *Quasiadiabatic continuation of quantum states: The stability of topological ground-state degeneracy and emergent gauge invariance*, *Phys. Rev. B* **72**, 045141 (2005).
- [75] H. J. Briegel and R. Raussendorf, *Persistent entanglement in arrays of interacting particles*, *Phys. Rev. Lett.* **86**, 910 (2001).
- [76] S. Bravyi, I. Kim, A. Kliesch, and R. Koenig, *Adaptive constant-depth circuits for manipulating non-Abelian anyons*, [arXiv:2205.01933](https://arxiv.org/abs/2205.01933).
- [77] M. McGinley, W. W. Ho, and D. Malz, *Measurement-induced entanglement and complexity in random constant-depth 2d quantum circuits*, *Phys. Rev. X* **15**, 021059 (2025).
- [78] G. Vidal, *Entanglement monotones*, *J. Mod. Opt.* **47**, 355 (2000).
- [79] Z.-W. Liu, S. Lloyd, E. Zhu, and H. Zhu, *Entanglement, quantum randomness, and complexity beyond scrambling*, *J. High Energy Phys.* **07** (2018) 041.
- [80] F. G. S. L. Brandão, A. W. Harrow, and M. Horodecki, *Local random quantum circuits are approximate polynomial-designs*, *Commun. Math. Phys.* **346**, 397 (2016).

- [81] A. Nahum, J. Ruhman, S. Vijay, and J. Haah, *Quantum entanglement growth under random unitary dynamics*, *Phys. Rev. X* **7**, 031016 (2017).
- [82] J. Haferkamp, P. Faist, N. B. T. Kothakonda, J. Eisert, and N. Yunger Halpern, *Linear growth of quantum circuit complexity*, *Nat. Phys.* **18**, 528 (2022).
- [83] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, *Quantum entanglement*, *Rev. Mod. Phys.* **81**, 865 (2009).
- [84] O. Gühne and G. Tóth, *Entanglement detection*, *Phys. Rep.* **474**, 1 (2009).
- [85] N. Friis, G. Vitagliano, M. Malik, and M. Huber, *Entanglement certification from theory to experiment*, *Nat. Rev. Phys.* **1**, 72 (2019).
- [86] G. Riccardi, D. E. Jones, X.-D. Yu, O. Gühne, and B. T. Kirby, *Exploring the relationship between the faithfulness and entanglement of two qubits*, *Phys. Rev. A* **103**, 042417 (2021).
- [87] L. Gurvits, *Classical deterministic complexity of Edmonds' problem and quantum entanglement*, in *Proceedings of the Thirty-Fifth Annual ACM Symposium on Theory of Computing*, STOC '03 (2023), pp. 10–19, 10.1145/780542.780545.
- [88] Z. Liu and F. Wei, *Separation between entanglement criteria and entanglement detection protocols*, *Phys. Rev. Res.* **7**, 033121 (2025).
- [89] A. Dimić and B. Dakić, *Single-copy entanglement detection*, *npj Quantum Inf.* **4** (2018).
- [90] J. Acharya, I. Issa, N. V. Shende, and A. B. Wagner, *Estimating quantum entropy*, *IEEE J. Sel. Areas Inf. Theor.* **1**, 454 (2020).
- [91] L. Leone, J. Rizzo, J. Eisert, and S. Jerbi, *Entanglement theory with limited computational resources*, *Nat. Phys.* **21**, 1847 (2025).
- [92] M. Takahashi, *Thermodynamics of One-Dimensional Solvable Models* (Cambridge University Press, Cambridge, England, 1999).
- [93] P. Calabrese and J. Cardy, *Entanglement entropy and quantum field theory*, *J. Stat. Mech.* (2004) P06002.
- [94] S.-J. Gu, G.-S. Tian, and H.-Q. Lin, *Ground-state entanglement in the XXZ model*, *Phys. Rev. A* **71**, 052322 (2005).
- [95] T. Brydges, A. Elben, P. Jurcevic, B. Vermersch, C. Maier, B. P. Lanyon, P. Zoller, R. Blatt, and C. F. Roos, *Probing Rényi entanglement entropy via randomized measurements*, *Science* **364**, 260 (2019).
- [96] C. Luo, H. Zhang, A. Chu, C. Maruko, A. M. Rey, and J. K. Thompson, *Hamiltonian engineering of collective XYZ spin models in an optical cavity*, *Nat. Phys.* **21**, 916 (2025).
- [97] S. R. White, *Density matrix formulation for quantum renormalization groups*, *Phys. Rev. Lett.* **69**, 2863 (1992).
- [98] K. Okamoto and K. Nomura, *Fluid-dimer critical point in $s = 12$ antiferromagnetic Heisenberg chain with next nearest neighbor interactions*, *Phys. Lett. A* **169**, 433 (1992).
- [99] C. K. Majumdar and D. K. Ghosh, *On next-nearest-neighbor interaction in linear chain. I*, *J. Math. Phys. (N.Y.)* **10**, 1388 (1969).
- [100] R. Bursill, G. A. Gehring, D. J. J. Farnell, J. B. Parkinson, T. Xiang, and C. Zeng, *Numerical and approximate analytical results for the frustrated spin-1/2 quantum spin chain*, *J. Phys. Condens. Matter* **7**, 8605 (1995).
- [101] M. Pregelj, A. Zorko, O. Zaharko, H. Nojiri, H. Berger, L. C. Chapon, and D. Arčon, *Spin-stripe phase in a frustrated zigzag spin-1/2 chain*, *Nat. Commun.* **6**, 7255 (2015).
- [102] T. A. Chowdhury, K. Yu, M. A. Shamim, M. L. Kabir, and R. S. Sufian, *Enhancing quantum utility: Simulating large-scale quantum spin chains on superconducting quantum computers*, *Phys. Rev. Res.* **6**, 033107 (2024).
- [103] S. Bravyi, G. Smith, and J. A. Smolin, *Trading classical and quantum computational resources*, *Phys. Rev. X* **6**, 021043 (2016).
- [104] S. Bravyi, D. Browne, P. Calpin, E. Campbell, D. Gosset, and M. Howard, *Simulation of quantum circuits by low-rank stabilizer decompositions*, *Quantum* **3**, 181 (2019).
- [105] J. R. Seddon, B. Regula, H. Pashayan, Y. Ouyang, and E. T. Campbell, *Quantifying quantum speedups: Improved classical simulation from tighter magic monotones*, *PRX Quantum* **2**, 010345 (2021).
- [106] Z.-W. Liu and A. Winter, *Many-body quantum magic*, *PRX Quantum* **3**, 020333 (2022).
- [107] L. Leone, Salvatore F. E. Oliviero, and A. Hamma, *Stabilizer Rényi entropy*, *Phys. Rev. Lett.* **128**, 050402 (2022).
- [108] T. Haug, S. Lee, and M. S. Kim, *Efficient quantum algorithms for stabilizer entropies*, *Phys. Rev. Lett.* **132**, 240602 (2024).
- [109] D. Gross, S. Nezami, and M. Walter, *Schur–Weyl duality for the Clifford group with applications: Property testing, a robust Hudson theorem, and de Finetti representations*, *Commun. Math. Phys.* **385**, 1325 (2021).
- [110] M. Hinsche and J. Helsen, *Single-copy stabilizer testing*, in *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*, STOC '25 (2025), pp. 439–450, 10.1145/3717823.3718169.
- [111] K. Warmuz, E. Dokułowicz, C. Radhakrishnan, and T. Byrnes, *Magic monotone for faithful detection of non-stabilizerness in mixed states*, *Phys. Rev. Lett.* **135**, 010203 (2025).
- [112] F. Wei and Z.-W. Liu, *Long-range nonstabilizerness and quantum codes, phases, and complexity*, *arXiv:2503.04566*.
- [113] D. Gottesman, *Stabilizer codes and quantum error correction*, *arXiv:quant-ph/9705052*.
- [114] X. Turkishi, E. Tirrito, and P. Sierant, *Magic spreading in random quantum circuits*, *Nat. Commun.* **16** (2025).
- [115] L. Leone, S. F. E. Oliviero, A. Hamma, J. Eisert, and L. Bittel, *The non-Clifford cost of random unitaries*, *PRX Quantum* **7**, 020321 (2026).
- [116] C. Gidney, N. Shutty, and C. Jones, *Magic state cultivation: Growing t states as cheap as CNOT gates*, *arXiv:2409.17595*.
- [117] Y. Zhang and Y. Gu, *Quantum magic dynamics in random circuits*, *npj Quantum Inf.* **12**, 87 (2026).
- [118] A. M. Dalzell, N. Hunter-Jones, and F. G. S. L. Brandão, *Random quantum circuits transform local noise into global white noise*, *Commun. Math. Phys.* **405** (2024).

- [119] J. J. Wallman and J. Emerson, *Noise tailoring for scalable quantum computation via randomized compiling*, *Phys. Rev. A* **94**, 052325 (2016).
- [120] A. Hashim, R. K. Naik, A. Morvan, J. L. Ville, B. Mitchell, J. M. Kreikebaum, M. Davis, E. Smith, C. Iancu, K. P. O'Brien, I. Hincks, J. J. Wallman, J. Emerson, and I. Siddiqi, *Randomized compiling for scalable quantum computing on a noisy superconducting quantum processor*, *Phys. Rev. X* **11**, 041039 (2021).
- [121] R. Raussendorf and H. J. Briegel, *A one-way quantum computer*, *Phys. Rev. Lett.* **86**, 5188 (2001).
- [122] M. Hein, J. Eisert, and H. J. Briegel, *Multipartite entanglement in graph states*, *Phys. Rev. A* **69**, 062311 (2004).
- [123] Z. Li, H. Zhu, and M. Hayashi, *Robust and efficient verification of graph states in blind measurement-based quantum computation*, *npj Quantum Inf.* **9**, 115 (2023).
- [124] H. Zhu and M. Hayashi, *Efficient verification of hypergraph states*, *Phys. Rev. Appl.* **12**, 054047 (2019).
- [125] H. Lóio, G. Lami, L. Leone, M. McGinley, X. Turkeshi, and J. D. Nardis, *Quantum state designs via magic teleportation*, [arXiv:2510.13950](https://arxiv.org/abs/2510.13950).
- [126] Z.-Y. Ge and F. Nori, *Identifying entanglement phases with bipartite projected ensembles*, *Phys. Rev. Res.* **7**, 043022 (2025).
- [127] A. Elben, S. T. Flammia, H.-Y. Huang, R. Kueng, J. Preskill, B. Vermersch, and P. Zoller, *The randomized measurement toolbox*, *Nat. Rev. Phys.* **5**, 9 (2022).
- [128] A. Mari, K. Kieling, B. M. Nielsen, E. S. Polzik, and J. Eisert, *Directly estimating nonclassicality*, *Phys. Rev. Lett.* **106**, 010403 (2011).
- [129] M. Hebenstreit, R. Jozsa, B. Kraus, S. Strelchuk, and M. Yoganathan, *All pure fermionic non-Gaussian states are magic states for matchgate computations*, *Phys. Rev. Lett.* **123**, 080503 (2019).
- [130] M. Gluza, M. Kliesch, J. Eisert, and L. Aolita, *Fidelity witnesses for fermionic quantum simulations*, *Phys. Rev. Lett.* **120**, 190501 (2018).
- [131] M. Fishman, S. R. White, and E. M. Stoudenmire, *The ITensor software library for tensor network calculations*, *SciPost Phys. Codebases* **4** (2022).
- [132] A. Javadi-Abhari *et al.*, *Quantum computing with qiskit*, [arXiv:2405.08810](https://arxiv.org/abs/2405.08810).
- [133] Z. Du, *Certifying localizable quantum properties with constant sample complexity (code repository)*, <https://github.com/ZhenyuDu01/Certifying-localizable-quantum-properties-with-constant-sample-complexity> (2025).
- [134] A. W. Harrow, L. Kong, Z.-W. Liu, S. Mehraban, and P. W. Shor, *Separation of out-of-time-ordered correlation and entanglement*, *PRX Quantum* **2**, 020339 (2021).
- [135] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, Cambridge, England, 2012).
- [136] J. Watrous, *The Theory of Quantum Information* (Cambridge University Press, Cambridge, England, 2018).
- [137] G. Aubrun and S. Szarek, *Alice and Bob Meet Banach* (American Mathematical Society, Providence, RI, 2017).
- [138] J. A. Tropp, *On the conditioning of random subdictionaries*, *Appl. Comput. Harmon. Anal.* **25**, 1 (2008).
- [139] M. Rudelson and R. Vershynin, *Hanson-Wright inequality and sub-Gaussian concentration*, *Electron. Commun. Probab.* **18**, 1 (2013).
- [140] M. E. H. Ismail and P. Simeonov, *Complex Hermite polynomials: Their combinatorics and integral operators*, *Proc. Am. Math. Soc.* **143**, 1397 (2015).