

Nonstabilizerness determining the hardness of direct fidelity estimation

Lorenzo Leone^{1,*}, Salvatore F. E. Oliviero,¹ and Alioscia Hamma^{2,3,1,†}

¹*Physics Department, University of Massachusetts Boston, Boston, Massachusetts 02125, USA*

²*Dipartimento di Fisica 'Ettore Pancini,' Università degli Studi di Napoli Federico II, Via Cintia 80126, Napoli, Italy*

³*INFN, Sezione di Napoli, Complesso universitario di Monte S. Angelo ed. 6 via Cintia, 80126 Napoli, Italy*



(Received 2 February 2023; accepted 6 February 2023; published 23 February 2023)

In this work, we show how the resource theory of nonstabilizerness quantifies the hardness of direct fidelity estimation protocols. In particular, the resources needed for a direct fidelity estimation conducted on generic states, such as Pauli fidelity estimation and shadow fidelity estimation protocols, grow exponentially with the stabilizer Rényi entropy. Remarkably, these protocols are shown to be feasible only for those states that are useless to attain any quantum speedup or advantage. This result suggests the impossibility of estimating efficiently fidelity for generic states and, at the same time, leaves the window open to those protocols specialized at directly estimating the fidelity of particular states. We then extend our results to quantum evolutions, showing that the resources needed to certify the quality of the implementation of a given unitary U are governed by the nonstabilizerness in the Choi state associated with U , which is shown to possess a profound connection with out-of-time order correlators.

DOI: [10.1103/PhysRevA.107.022429](https://doi.org/10.1103/PhysRevA.107.022429)

I. INTRODUCTION

Quantum computers promise efficient solutions to problems that are otherwise intractable on classical computers [1–6]. In order to fully harness the overwhelming computational advantage of quantum processors, it is first necessary to ensure their correct functioning. Unsurprisingly, the technology best suited for this task would be another quantum computer [7–10]. Until reliable quantum technology can be realized, one must use classical resources to implement methods of *quantum certification*. In the past decade, there have been many attempts in tackling this problem, with a large landscape of different protocols, ranging from benchmarking [11–24], quantum state [25–39], and process [40–49] learning to blind computation [50–57] and quantum supremacy [6,58,59] approaches. For a panoramic overview of the approaches within the field of quantum certification, see, e.g., Refs. [60–64].

A quantum certificate guarantees the correct application of a given quantum process or the correct preparation of a desired quantum state. This is commonly done in terms of a measure of quality, i.e., a measure of distance having the interpretation of worst-case distinguishability. Specifically, certifications of quantum states are phrased in terms of the fidelity between the target state $|\psi\rangle$ and the actual state $\tilde{\psi}$ prepared from the machine, while the quality of quantum gates U is commonly expressed in terms of average gate fidelity [18,65–67].

The bottleneck of any quantum certification protocol is the efficiency in terms of resources. They are conventionally quantified by (i) the *sample complexity* [60,61,64], i.e., the

minimal number of experiments and resulting samples that need to be prepared for a protocol to be successful, and (ii) the *classical postprocessing complexity*, i.e., the number of classical resources spent for postprocessing data. In particular, a protocol is said to be efficient if its total complexity scales polynomially in the number of qubits n ; conversely, a protocol is inefficient if its complexity scales exponentially in n .

In this paper, we point out a very striking fact: the complexity of direct fidelity estimation protocols aimed at certifying generic quantum states is exactly quantified by the amount of *nonstabilizerness* in the state. Nonstabilizerness is an expensive, but fundamental fuel for quantum computation [43, 68–81]: without nonstabilizerness, a quantum computer can do nothing more than a classical computer. While simulations of stabilizer states (stabilizer resources) and Clifford circuits (stabilizer operations) are efficient on classical computers, the injection of t non-Clifford gates makes the simulation exponentially harder in t , thus unlocking quantum advantage. Resource theory of nonstabilizerness has been widely studied and found copious applications in the broad field of fault-tolerant quantum computation [82–85], as well as classical algorithms for simulations of quantum computing architectures [86–91].

In this paper, we prove that the complexity of direct verification protocols scales exponentially with the nonstabilizerness and thus exponentially in the number of non-Clifford gates needed for the state preparation. This result implies that the certification protocol is efficient only as long as the amount of non-Clifford gates used is $O(\log_2 n)$. Remarkably, this is the same threshold for a quantum state to be efficiently simulated classically [89]. As a consequence, when quantum computation is able to unlock quantum speedup, then for this process direct fidelity estimation protocols are not feasible. In other words, the same complexity that makes quantum

*lorenzo.leone001@umb.edu

†alioscia.hamma@unina.it

technology powerful is the one that inhibits its certification. This is the main conceptual contribution of this work.

Along these lines, we extend our results to the certification of quantum processes via direct average gate fidelity estimation. We show that the sample complexity, i.e., the number of uses of a given U , is quantified by multipoints out-of-time-order correlators (OTOCs) associated with the target unitary operator U . OTOCs are conventionally employed to probe quantum chaos: a quantum evolution is commonly considered to be chaotic in terms of attaining the Haar value for general OTOCs [91–94], that is, the value that would be reached by a random unitary operator. We claim the closer these correlators are to the Haar value, the more chaotic the evolution [91] and the more inefficient the quantum verification. Quantum chaos is quantum—it requires an extensive quantity $O(n)$ of non-Clifford resources—and therefore it hinders quantum certification.

The paper proceeds in the following way: in Sec. II we give an overview of the problem and informally introduce the main result of the paper. Section III is devoted to the introduction of the main tools used throughout the paper. In particular, in Sec. III A, we introduce the resource theory of stabilizer Rényi entropy, which turns out to have a deep connection to quantum fidelity estimation protocols. In Sec. III B, we present the algorithm for classical simulations of Clifford circuit containing a finite number of non-Clifford gates, useful in proving the main result of the paper later presented in Sec. IV. In particular, in Sec. IV A, we introduce the Pauli fidelity estimation protocol and bound its complexity with the stabilizer entropy, while in Sec. IV B, we turn to analyzing the shadow fidelity estimation protocol and show how its complexity scales exponentially with the number of non-Clifford gates, and thus with the nonstabilizerness of a given state $|\psi\rangle$. Finally, in our conclusion, we summarize the main findings of the paper and sketch ideas for future directions.

II. FIDELITY ESTIMATION AS A QUANTUM CERTIFICATE: STATEMENT OF THE MAIN RESULT

Let $\psi \equiv |\psi\rangle\langle\psi|$ be the state one wants to prepare on a quantum processor and let $\tilde{\psi}$ be the state actually prepared by the quantum processor. The question behind the whole theory of quantum certification is how can one certify to what extent $\tilde{\psi} \sim \psi$ and how costly certification is? One of, if not the, most intuitive way to quantify the quality of the realization of the prepared state is to *measure* the probability that $\tilde{\psi}$ is ψ , i.e., measure the *fidelity* between $\tilde{\psi}$ and ψ , defined as

$$\mathcal{F}(|\psi\rangle, \tilde{\psi}) := \text{tr}(\psi \tilde{\psi}). \quad (1)$$

Operationally, the fidelity \mathcal{F} quantifies the probability that $\tilde{\psi} \mapsto |\psi\rangle\langle\psi|$ and $\mathcal{F}(|\psi\rangle, \tilde{\psi}) = 1$ if and only if $\tilde{\psi} = |\psi\rangle\langle\psi|$. In this work, we refer to *direct fidelity estimation* as a protocol aimed to directly measure the fidelity \mathcal{F} within an additive error ϵ [indeed an $\epsilon = O(1)$ error is sufficient for a quantum certification scope since we want $\mathcal{F} \simeq 1$]. The most direct method to measure the fidelity is to measure the state $\tilde{\psi}$ in the basis in which $|\psi\rangle$ is diagonal. In other words, one can access \mathcal{F} by measuring the positive operator valued measurement (POVM) given by the following set $\mathcal{S}_\psi = \{|\psi\rangle\langle\psi|, \mathbb{I} - |\psi\rangle\langle\psi|\}$. Unfortunately, for generic states measuring the

set \mathcal{S}_ψ is as much difficult, and noisy, as preparing the state $|\psi\rangle$. One, maybe appealing, alternative is provided by the swap test [7,8], i.e., a quantum algorithm aimed to measure the fidelity between two states, say $|\psi\rangle$ and $\tilde{\psi}$. The algorithm uses an ancillary qubit in the state $\propto |0\rangle + |1\rangle$ as the qubit control of a swap operator T acting between $|\psi\rangle$ and $\tilde{\psi}$, and then measured in the basis $|0\rangle \pm |1\rangle$. The described protocol is efficient in terms of resources: a user must prepare the states $|\psi\rangle$ and $\tilde{\psi}$ an $O(\epsilon^{-2})$ number of times to access the fidelity within an error ϵ . As the reader might be already aware, the problem of such protocol is not the efficiency in terms of resources, but the fact that a verifier should be able to perfectly prepare the state $|\psi\rangle$ on another quantum processor. This is to say that a quantum computer is certainly able to certify the correct functioning of another noisy quantum computer.

Unfortunately, until the advent of a completely fault-tolerant quantum technology, one must opt for other strategies. For direct fidelity estimation protocols, the rules of the game are (i) the state $|\psi\rangle$ is a theoretical state, efficiently saved in a classical memory, (ii) a verifier must measure the fidelity in Eq. (1) of the state $\tilde{\psi}$ by having access to $N_{\tilde{\psi}}$ state preparations of $\tilde{\psi}$, and (iii) by using N_{cl} resources for classical postprocessing on each $\tilde{\psi}$. We define the number of resources \mathcal{N} —i.e., the total *complexity* of the protocol—necessary to estimate the fidelity within an error ϵ as the product of the, so-called, sample complexity N_ψ and the classical postprocessing complexity N_{cl} , i.e.,

$$\mathcal{N} = N_\psi \times N_{cl}, \quad (2)$$

and we define a protocol to be efficient iff $\mathcal{N} = O(\text{poly}(n))$. In this work, we discuss two protocols aimed to certify the correct state preparation by directly measuring the fidelity in Eq. (1), i.e., *Pauli fidelity estimation* [29,30] and *shadow fidelity estimation* [32,38,60]. These two protocols are the only two protocols introduced in the literature, beside quantum state tomography, that have the advantage to not rely on any assumption on the state $|\psi\rangle$ and general enough to work for every state. Let us briefly and informally summarize the main steps.

Definition 1 (Pauli fidelity estimation). Let Ξ_ψ be a state-dependent probability distribution on the space of a complete set of local observables. An unbiased estimator $\tilde{\mathcal{F}}$ for \mathcal{F} is built in the following way: (i) draw k observables O_i according to Ξ_ψ , (ii) estimate the expectation value $\langle O_i \rangle_{\tilde{\psi}}$ on $\tilde{\psi}$, and (iii) sum them up and define $\tilde{\mathcal{F}} := k^{-1} \sum_i \langle O_i \rangle_{\tilde{\psi}}$. Note that $N_{cl} = O(1)$, while the sample complexity $N_{\tilde{\psi}} \simeq k \times \max_i c_i$, where c_i is the number of shot measurements employed to estimate $\langle O_i \rangle_{\tilde{\psi}}$.

Definition 2 (Shadow fidelity estimation). Let $|\psi\rangle$ be a quantum state, $\tilde{\psi}$ its noisy realization on a quantum hardware, and $\{|x\rangle\}$ the computational basis. (i) Draw k independent Clifford circuits C_i uniformly at random, (ii) apply them on the prepared state, $\tilde{\psi}_i = C_i \tilde{\psi} C_i^\dagger$, (iii) measure the resulting state in the computational basis and record the result \bar{x}_i , and (iv) run a classical estimation algorithm to compute the outcome probability $|\langle \bar{x}_i | C_i | \psi \rangle|^2$ for \bar{x}_i the measurement result. (v) Finally define $\tilde{\mathcal{F}} := k^{-1} \sum_i [(d+1)|\langle \bar{x}_i | C_i | \psi \rangle|^2 - 1]$. Note that N_{cl} counts the number of resources necessary to

compute $|\langle \bar{x}_i | C_i | \psi \rangle|^2$ for each i , while the sample complexity $N_{\bar{\psi}} \simeq k$, i.e., the number of Clifford circuits sampled.

Now we are in the position to state the main result of the paper.

Theorem 1 (Informal). The number of resources \mathcal{N} for both Pauli fidelity and shadow fidelity estimation protocols scales exponentially with the stabilizer Rényi entropy and thus with the number of non-Clifford gates used to prepare the state. In particular, these protocols are feasible only for those states that can be efficiently simulable on a classical computer.

In the next section, we introduce the main tools used to prove the above statement.

III. TOOLS, DEFINITIONS, AND TECHNIQUES

A. Stabilizer Rényi entropy

The stabilizer Rényi entropy is a recently introduced nonstabilizer monotone [68], which possesses the nice property to be experimentally measurable [80]. In this section, we briefly review some useful properties to allow easy access to the main results of the paper. We also discuss the stabilizer Rényi entropy associated with a unitary evolution U , through the Choi-Jamiołkowski isomorphism, and establish a nontrivial connection with out-of-time-order correlators, which is a result of independent interest.

Let ρ be a quantum state, let $\mathbb{P}(n)$ be the Pauli group on n qubits, $\mathcal{C}(n)$ the Clifford group, and $d \equiv 2^n$ the dimension of the Hilbert space. The state ρ can be written in the Pauli basis as $\rho = \frac{1}{d} \sum_{P \in \mathbb{P}} \text{tr}(P\rho)P$ and we can associate a probability distribution to the coefficients of such expansion, $\Xi_\rho := \{\text{Pur}^{-1}(\rho)d^{-1}\text{tr}^2(P\rho) \mid P \in \mathbb{P}(n)\}$, where $\text{Pur}(\rho) := \text{tr}\rho^2$. Note that $\Xi_\rho(P) \geq 0$ and sum to one. The α -stabilizer Rényi entropy is defined as [68]

$$M_\alpha(\rho) := S_\alpha(\Xi_\rho) + S_2(\rho) - \log_2 d, \quad (3)$$

where $S_\alpha(\Xi_\rho)$ is the α -Rényi entropy of the probability distribution Ξ_ρ and $S_2(\rho) := -\log_2 \text{Pur}(\rho)$ is the quantum 2-Rényi entropy of ρ . $M_\alpha(\rho)$ has the following properties: (i) it follows a hierarchy $M_\alpha(\rho) \geq M_{\alpha'}(\rho)$ for $\alpha' < \alpha$; (ii) it is faithful, i.e., $M_\alpha(\rho) = 0$ iff $\rho = \frac{1}{d} \sum_{P \in G} \phi_P P$, where $G \subset \mathbb{P}(n)$ is a commuting subset of $\mathbb{P}(n)$ and $\phi_P = \pm 1$; (iii) it is invariant under Clifford rotations C , $M_\alpha(\rho) = M_\alpha(C\rho C^\dagger)$; (iv) it is additive: $M_\alpha(\rho \otimes \sigma) = M_\alpha(\rho) + M_\alpha(\sigma)$; (v) it is bounded $M_\alpha(|\psi\rangle) \leq \log_2 d$. We denote the stabilizer Rényi entropy for a pure state $|\psi\rangle$ as $M_\alpha(|\psi\rangle)$; for pure states only, we have that $M_\alpha(|\psi\rangle) \leq \nu(|\psi\rangle)$ [68], where $\nu(|\psi\rangle)$ is the stabilizer nullity [95] of $|\psi\rangle$, defined as $\nu(|\psi\rangle) = \log_2 d - \log_2 s(|\psi\rangle)$, where $s(|\psi\rangle) := |\{P : |\text{tr}(P|\psi\rangle\langle\psi|)| = 1\}|$. Additionally, thanks to the bound proven in [96], one has $M_\alpha(|\psi\rangle) \leq t$, where t is the number of T gates spent in the circuit that prepares $|\psi\rangle$ from $|0^n\rangle$.

The stabilizer Rényi entropy is defined on states, so it is natural to compute the stabilizer Rényi entropy of the Choi state $|U\rangle \in \mathcal{H}^{\otimes 2}$ associated with a unitary operator U , as $|U\rangle := (\mathbb{1} \otimes U)|I\rangle$, where $|I\rangle := \frac{1}{\sqrt{d}} \sum_i |i\rangle \otimes |i\rangle$. Let Ξ_U be a probability distribution whose elements are $\Xi_U(P, P') := d^{-4} \text{tr}^2(PUP'U^\dagger)$ for $P, P' \in \mathbb{P}(n)$; then the following lemma holds.

Lemma 1. The stabilizer Rényi entropy for $|U\rangle$ reads

$$M_\alpha(|U\rangle) = S_\alpha(\Xi_U) - 2 \log_2 d. \quad (4)$$

See Appendix A for the proof. Now we are ready to state one of the main results of the paper, which builds a tight connection between the nonstabilizer of the Choi state $|U\rangle$ and OTOCs.

Lemma 2. The α -stabilizer Rényi entropy of $|U\rangle$, for $1 < \alpha \in \mathbb{N}$, equals the 4α -points out-of-time order correlator

$$M_\alpha(|U\rangle) = \frac{1}{1-\alpha} \log_2 \text{OTOC}_{4\alpha}(U), \quad (5)$$

where $\text{OTOC}_{4\alpha} := \frac{1}{d^2} \sum_{P, P'} \text{otoc}_{4\alpha}(P, P')$, where $d \times \text{otoc}_{4\alpha}(P, P') := \text{tr}[P_{2\alpha} \prod_{i=1}^{2\alpha} P^{(U)} P' P_{i-1} P_i]$ with $P_0 \equiv \mathbb{1}$ and $\langle \cdot \rangle$ is the average over $P_1, \dots, P_{2\alpha}$.

For a proof, see Appendix A. The above lemma tells the meaning of the nonstabilizer possessed by Choi states associated with unitary evolutions: the more the nonstabilizer $M_\alpha(|U\rangle)$, the more chaotic is the evolution generated by U [91]. Lastly, we show a bound with a nonstabilizer monotone defined by unitary operators, useful in proving the main results of the paper. Let $\nu(U)$ be the unitary stabilizer nullity defined in [96] as $\nu(U) := 2 \log_2 d - \log_2 s(U)$, where $s(U) := |\{P_1, P_2 : |\text{tr}(P_1 U P_2 U^\dagger)| = 1\}|$, i.e., $s(U)$ counts the elements of a subset of the Pauli group normalized by the adjoint action of U . We have the following bound.

Lemma 3. For any $0 \leq \alpha < \infty$, we have

$$M_\alpha(|U\rangle) \leq \nu(U). \quad (6)$$

The lemma easily follows from Lemma 1 and the bound proven in [68], i.e., $M_\alpha(|\psi\rangle) \leq \nu(|\psi\rangle)$ for any α . The lemma also shows that the unitary stabilizer nullity $\nu(U)$ is nothing but the stabilizer nullity of the Choi state associated with U , i.e., $\nu(|U\rangle) = \nu(U)$.

B. Strong classical simulation of states beyond stabilizer states

In this section, we present a brief and simplified review of the classical simulation method for states beyond stabilizer states, that will be useful in proving Theorem 3.

Imagine we are given the quantum circuit U_t , as a Clifford circuit plus a number t of T -gates circuit, that build a state $|\psi\rangle \equiv U_t |0^n\rangle$ starting from a reference state $|0^n\rangle$. Throughout the paper, we refer to “strong simulation” as the ability to (exactly) compute the outcome probability $|\langle x | \psi \rangle|^2$ for some n -bit string $|x\rangle$. The following simulation algorithm is not a *state of the art* kind of algorithm. We describe it to illustrate why and how the strong simulation of Clifford+ T circuits scales exponentially in t , keeping the technicalities as simple as possible. See, e.g., Refs. [89, 91, 97–99] for state-of-the-art simulation algorithms. We anticipate and remark that any simulation algorithm aimed to simulate Clifford + T circuits scales exponentially in the number of T gates.

First of all, thanks to the Gottesman-Knill theorem, one can compute the overlap between any two n -qubit stabilizer states $|\omega_1\rangle, |\omega_2\rangle$ as $\langle \omega_1 | \omega_2 \rangle = b 2^{-p/2} e^{i\pi m/4}$, for some $b = \{0, 1\}$, integer $p \in [1, n]$, and $m \in \mathbb{Z}_8$ with an algorithm having runtime $O(n^3)$ [87]. Conversely, if one is provided with the decomposition of $|\psi\rangle$ into elementary gates of Clifford + T circuits,

the simulation cost scales exponentially in the number of T gates, as shown below.

The algorithm starts from the following simple observation. Define the T gadget as the following state $|T\rangle \propto |0\rangle + e^{i\pi/4}|1\rangle$. The T gadget, together with a controlled-NOT—here denoted as $CX_{i,j}$, where i is the control and j the target—and measurement in the Z basis, can be spent to apply a T gate. The protocol is the following. Let $|\psi\rangle$ be a n qubit state on which one wants to apply a T gate on the i th qubit for $i \in \{1, n\}$. Let $n+1$ be the labeling of the ancillary qubit corresponding to $|T\rangle$. The first thing to do is to append the T gadget as $|\psi\rangle \mapsto |\psi\rangle|T\rangle$; then apply a CX , having control on i and target on $n+1$ as $|\psi\rangle|T\rangle \mapsto CX_{i,n+1}(|\psi\rangle|T\rangle)$; and then measure the $n+1$ qubit in the $\{|0\rangle, |1\rangle\}$ basis. If the measurement leads to the outcome “0,” then $|0\rangle\langle 0|C_{i,n+1}(|\psi\rangle|T\rangle) \propto T_i|\psi\rangle|0\rangle$, while, if it leads to the outcome “1,” then $|1\rangle\langle 1|C_{i,n+1}(|\psi\rangle|T\rangle) \propto S_i^\dagger T_i|\psi\rangle|1\rangle$. Thus *adapting* the application of an S gate, i.e., $S \equiv \text{diag}(1, i)$, on the i th qubit conditioned to the measurement result, leads to the application of a T gate on the i th qubit. For a generic n -qubit t -doped Clifford circuit $U_t := C_t T_{i_t} C_{t-1} T_{i_{t-1}} \cdots C_1 T_{i_1} C_0$, i.e., Clifford circuits interleaved with the application of t non-Clifford gates, we can define the following $(n+t)$ -qubit Clifford circuit:

$$C_{U_t} = C_t CX_{i_t, n+1} C_{t-1} CX_{i_{t-1}, n+2} \cdots C_1 CX_{i_1, n+t} C_0, \quad (7)$$

i.e., we replace all the T_{i_k} gates with CX gates $CX_{i_k, n+k}$ controlling on the i_k th qubit and acting on the k th auxiliary qubit for $k \in \{n+1, n+t\}$. C_{U_t} is called the *gadgetized* version of U_t . Thanks to the observation described above, one can write the outcome probability as

$$|\langle x|U_t|0^n\rangle|^2 = 2^t |\langle x, 0^t|C_{U_t}|0^n, T^{\otimes t}\rangle|^2, \quad (8)$$

i.e., the probability that the n -qubit circuit U_t acting on $|0^n\rangle$ leads to $|x\rangle$ is proportional to the probability that the *gadgetized* version C_{U_t} [Eq. (7)] acting on $|0^n\rangle \otimes |T^{\otimes t}\rangle$ leads to $|x\rangle \otimes |0^t\rangle$. The proportionality factor 2^t is due to post-selection [89]. Next, observe that one can write $|T^{\otimes t}\rangle = \sum_{y \in \{0,1\}^t} e^{i\frac{\pi}{4}hw(y)} |y\rangle$, where $hw(y)$ is the Hamming weight of the t -bit string $y \in \{0,1\}^t$. In other words, one can write t copies of the T gadget as a combination of 2^t computational basis states. We can thus estimate the outcome probability $|\langle x|U_t|0^n\rangle|^2$ as

$$|\langle x|U_t|0^n\rangle|^2 = 2^t \left| \sum_{y \in \{0,1\}^t} e^{i\frac{\pi}{4}hw(y)} \langle x, 0^t|C_{U_t}|0^n, y\rangle \right|^2, \quad (9)$$

i.e., by evaluating the overlaps between $C_{U_t}|0^n, y\rangle$ and $|x, 0^t\rangle$ via the Gottesman-Knill theorem for every $y \in \{0,1\}^t$ and then summing them up. The above method, for the exact computation of the outcome probability, leads to a classical simulation cost $O(2^t(n+t)^3)$, where the exponential scaling in t comes from the fact that there are exponentially many t -bit strings y in the sum of Eq. (9), while the factor $(n+t)^3$ comes directly from the Gottesman-Knill theorem.

Now we are ready to discuss the main contributions of the paper, showing that the efficiency of direct fidelity estimation protocols is governed by nonstabilizerness.

IV. STABILIZER RÉNYI ENTROPY AND FIDELITY ESTIMATION: FORMAL RESULTS

The following section is devoted to the presentation of the main theorems of the paper in a formal fashion. Specifically, in Sec. IV A, we first describe Pauli fidelity estimation protocol, first introduced by [29,30], and bound the number of resources \mathcal{N} with the stabilizer entropy. In Sec. IV B, we describe the shadow estimation protocol introduced in [32,38] and show that the total complexity scale exponentially with the number of non-Clifford gates spent to prepare the state. Finally, in Sec. IV C, we show that Pauli fidelity estimation performs better than shadow fidelity estimation in terms of resources. The analyzed protocols have the advantage of being problem-agnostic protocols, i.e., they do not rely on any additional assumption and work for generic states. We will demonstrate that, while these protocols have wide applicability, they are only feasible and scalable for the class of states that do not provide a quantum computational advantage.

A. Pauli fidelity estimation

Here we show that the stabilizer Rényi entropy directly quantifies the resources needed to estimate the fidelity, the distance in 2-norm—for pure states and mixed states—up to an accuracy ϵ and success probability lower bounded by $1 - \delta$. In particular, we prove that the stabilizer Rényi entropy quantifies the number of resources required for a direct fidelity estimation, conducted via Monte Carlo sampling: Pauli fidelity estimation. This protocol was first introduced in [29,30] to directly access the fidelity of a state preparation $\tilde{\psi}$ and then experimentally employed in [100,101].

The protocol proceeds as follows. Let $|\psi\rangle$ be the pure state one aims to prepare on a quantum processor and let $\tilde{\psi}$ be the state (in general mixed) actually prepared by the quantum processor. As discussed in Sec. II, a measure of quality of $\tilde{\psi}$ is provided by the fidelity \mathcal{F} between the theoretical state $|\psi\rangle$ and $\tilde{\psi}$, i.e.,

$$\mathcal{F}(|\psi\rangle, \tilde{\psi}) := \text{tr}(\psi \tilde{\psi}), \quad (10)$$

where $\psi := |\psi\rangle\langle\psi|$. One can rewrite Eq. (10) in the Pauli basis $\mathcal{P}(n)$ as $\mathcal{F}(|\psi\rangle, \tilde{\psi}) = \frac{1}{d} \sum_P \text{tr}(P\psi) \text{tr}(P\tilde{\psi})$ and define $X_P := \frac{\text{tr}(P\tilde{\psi})}{\text{tr}(P\psi)}$; note $\Xi_\psi := \{\Xi_\psi(P) \equiv d^{-1} \text{tr}^2(P\psi) | P \in \mathbb{P}(n)\}$ is the probability distribution introduced in Sec. III A for ψ being a pure state. Thus we can write the fidelity as an expectation value over Ξ_ψ :

$$\mathcal{F}(|\psi\rangle, \tilde{\psi}) = \sum_P X_P \Xi_\psi(P) \equiv \langle X_P \rangle_{\Xi_\psi}, \quad (11)$$

i.e., the fidelity between the theoretical pure state ψ and the prepared state $\tilde{\psi}$ can be recast as an average of measurable numbers X_P on the probability distribution Ξ_ψ . Following [29,60], we use the following protocol to estimate the average in Eq. (11): (i) extract k Pauli operators $P_1, \dots, P_k \in \mathbb{K}$ according to the state-dependent probability distribution Ξ_ψ ; (ii) for each extraction $P \in \mathbb{K}$ of the Pauli observable P construct $c_P(\tilde{\psi})$ copies of the state $\tilde{\psi}$ to estimate the expectation value $\text{tr}(P\tilde{\psi})$; (iii) compute the unbiased estimator of the fidelity $\mathcal{F}(|\psi\rangle, \tilde{\psi})$ given by $\tilde{\mathcal{F}} = \frac{1}{k} \sum_{P \in \mathbb{K}} \tilde{X}_P$, where $\tilde{X}_P = \text{tr}^{-1}(P\psi) c_P(\tilde{\psi})^{-1} \sum_{j=1}^{c_P(\tilde{\psi})} \mathcal{P}_{P_j}(\tilde{\psi})$ and $\mathcal{P}_{P_j}(\tilde{\psi})$ is the outcome

of a one-shot measurement of the observable P on the j th copy of $\tilde{\psi}$. We quantify the resources needed for the estimation—up to an accuracy ϵ and failure probability $\leq \delta$ —as the number of copies of $\tilde{\psi}$ to be prepared on the machine:

$$N_{\tilde{\psi}} := \sum_{P \in \mathbb{K}} c_P(\tilde{\psi}). \quad (12)$$

Surprisingly, the total resources $N_{\tilde{\psi}}$ are exactly quantified by the nonstabilizerlessness of $|\psi\rangle$, measured via the stabilizer Rényi entropy $M_\alpha(|\psi\rangle)$ as the next theorem states.

Theorem 2. The sample complexity $N_{\tilde{\psi}}$ needed to measure the fidelity \mathcal{F} with accuracy ϵ and success probability $1 - \delta$ is bounded:

$$\frac{2}{\epsilon^2} \ln(2/\delta) \exp[M_2(|\psi\rangle)] \leq N_{\tilde{\psi}} \leq \frac{64}{\epsilon^4} \ln(2/\delta) \exp[M_0(|\psi\rangle)], \quad (13)$$

where $M_2(|\psi\rangle)$ and $M_0(|\psi\rangle)$ are the 2 and the 0-stabilizer Rényi entropy, respectively. Then, since $N_{cl} = \Theta(1)$, one has that the number of resources obeys $\mathcal{N}_P = \Theta(N_{\tilde{\psi}})$.

See Appendix B 1 for a proof. The above theorem tells us that the more the nonstabilizerlessness of the quantum state one aims to prepare on the quantum machine, the harder is the verification through Pauli fidelity estimation protocol. Let us use the theorem to determine the scaling of $N_{\tilde{\psi}}$ for an important class of states, i.e., the t -doped stabilizer states. A t -doped stabilizer state, denoted as $|\psi_t\rangle$, is the output state of a circuit composed by Clifford gates doped with a finite amount t of non-Clifford resources. The best classical algorithm able to simulate such states scales as $O(\text{poly}(n) \exp[t])$ [89], providing an insightful threshold for the onset of quantum advantage: as long as $t = O(\log_2 n)$, such states can be efficiently simulated classically and therefore cannot provide any quantum speedup. We have the following result.

Corollary 1. The (average) number of resources to verify a t -doped stabilizer state ψ_t grows exponentially in t :

$$\Theta(\exp[t \log_2 4/3]) \leq \langle N_{\psi_t} \rangle \leq \Theta(\exp[t]) \leq \Theta(d). \quad (14)$$

See Appendix B 2 for a proof. Two comments are in order here: first, the hardness of the verification of t -doped stabilizer states quickly saturates the bound, growing exponentially in t . Second, this is telling us that the above protocol is efficient only for those states with t at most $O(\log_2 n)$, which is useless for quantum computation.

Let us now extend the above results to mixed states. Suppose one aims to prepare a mixed state ρ on a quantum processor. Let $\tilde{\rho}$ be the actual state prepared from the quantum machine. One way to check whether the preparation is faithful is to evaluate the difference in 2-norm between ρ and $\tilde{\rho}$ [102]:

$$\|\rho - \tilde{\rho}\|_2 = \sqrt{\text{Pur}(\rho)} \sqrt{1 + \frac{\text{Pur}(\tilde{\rho})}{\text{Pur}(\rho)} - 2\Phi(\rho, \tilde{\rho})}, \quad (15)$$

where we defined $\Phi(\rho, \tilde{\rho}) := \frac{\text{tr}(\rho\tilde{\rho})}{\text{Pur}(\rho)}$ as the overlap between ρ and $\tilde{\rho}$. In order to evaluate the above, one needs to measure both $\Phi(\rho, \tilde{\rho})$ and $\text{Pur}(\tilde{\rho})$. Nonetheless, here we are only concerned with the overlap $\Phi(\rho, \tilde{\rho})$, because it is the only quantity involving a direct comparison between the theoretical state ρ and the actual state $\tilde{\rho}$. Note that the purity $\text{Pur}(\tilde{\rho})$ can be estimated efficiently by employing the standard technique of the *swap test* [7,8]. Writing $\Phi(\rho, \tilde{\rho})$

in the Pauli basis, one can recast it in terms of the expectation value, $\Phi(\rho, \tilde{\rho}) = \langle X_P(\rho) \rangle_{\Xi_\rho}$, of $X_P(\rho) := \frac{\text{tr}(P\tilde{\rho})}{\text{tr}(\rho\tilde{\rho})}$, on the probability distribution Ξ_ρ associated to the mixed state ρ , $\Xi_\rho = \{d^{-1} \text{Pur}^{-1}(\rho) \text{tr}^2(P\rho) | P \in \mathbb{P}(n)\}$. Thus, following the protocol described above, we can estimate the above average by an importance sampling of the probability distribution Ξ_ρ and construct an unbiased estimator $\hat{\Phi}(\rho, \tilde{\rho}) = \frac{1}{k} \sum_{P \in \mathbb{K}} \frac{1}{\text{tr}(P\rho)} \frac{1}{c_P(\rho)} \sum_{j=1}^{c_P(\rho)} \mathcal{P}_{Pj}(\tilde{\rho})$, where $c_P(\rho)$ are the number of copies of $\tilde{\rho}$ needed to estimate $\text{tr}(P\tilde{\rho})$ and $\mathcal{P}_{Pj}(\tilde{\rho})$ is the outcome of the measurement of P on the j th copy of $\tilde{\rho}$. The number of resources needed to access the overlap $\Phi(\rho, \tilde{\rho})$ is given again by the total number of copies of $\tilde{\rho}$, i.e., $N_{\tilde{\rho}} = \frac{1}{k} \sum_{P \in \mathbb{K}} c_P(\tilde{\rho})$. We are now ready to bound $N_{\tilde{\rho}}$ in terms of the stabilizer Rényi entropy for mixed states.

Corollary 2. The number of resources $N_{\tilde{\rho}}$ needed to measure the overlap $\Phi(\rho, \tilde{\rho})$ with an accuracy ϵ and success probability $\geq 1 - \delta$ is bounded by

$$\frac{2}{\epsilon^2} \ln(2/\delta) \exp[M_2(\rho)] \leq N_{\tilde{\rho}} \leq \frac{64}{\epsilon^4} \ln(2/\delta) \exp[M_0(\rho)]. \quad (16)$$

For mixed states also, the number of resources needed to measure the overlap between ρ and $\tilde{\rho}$ is exactly quantified by the stabilizer Rényi entropy $M_\alpha(\rho)$.

We remark once again that the Pauli fidelity estimation protocol described above is state-agnostic, i.e., it does not make any assumption on the nature of the state $|\psi\rangle$ and, consequently, it works for every state. Nevertheless, there is a rich literature of examples in which one can efficiently certify the preparation of a particular set of states. See, for example, hypergraph states [34,103–106], i.e., states built from $(|0\rangle + |1\rangle)^{\otimes n}$ with the application of CCZ gates, and bipartite pure states [33,35,107–110].

In what follows, we describe an extension of the Pauli fidelity estimation protocol for state-aware verifiers. Suppose one wants to prepare the state $|\psi\rangle$ and, besides knowing the quantum circuit able to prepare $|\psi\rangle$ from a reference state $|0^n\rangle$, one knows a complete set of stabilizer observables O_1, \dots, O_d , i.e., Hermitian operators, such that $O_i |\psi\rangle = \pm |\psi\rangle$ and $[O_i, O_j] = 0 \forall i, j = 1, \dots, d$. Note that every state $|\psi\rangle$ possesses one. Let \mathbb{O} be a complete basis of operators such that $O_1, \dots, O_d \in \mathbb{O}$ and define the state-dependent probability distribution $\Xi_\psi^\mathbb{O}$, in the same fashion of Ξ_ψ defined in Sec. III A, as

$$\Xi_\psi^\mathbb{O} := \{d^{-1} \text{tr}^2(O_i \psi), O_i \in \mathbb{O}\}. \quad (17)$$

Following the protocol described at the beginning of the section and replacing $\Xi_\psi \mapsto \Xi_\psi^\mathbb{O}$ and $P_i \mapsto O_i$, one can estimate the fidelity $\mathcal{F}(|\psi\rangle, \tilde{\psi})$ as $\mathcal{F}(|\psi\rangle, \tilde{\psi}) = \sum_{O_i \in \mathbb{O}} \frac{\text{tr}(\tilde{\psi} O_i)}{\text{tr}(\psi O_i)} \Xi_\psi^\mathbb{O}(O_i)$. At this point, one can define an entropy $S(\Xi_\psi^\mathbb{O})$ for the probability distribution $\Xi_\psi^\mathbb{O}$, similarly to the definition of stabilizer entropy in Sec. III A. Since $O_1, \dots, O_d \in \mathbb{O}$, it is straightforward to verify that $S(\Xi_\psi^\mathbb{O}) = n$. At this point, the following corollary readily descends from Theorem 2.

Corollary 3. Given the knowledge of a complete set of stabilizers O_1, \dots, O_d for a state $|\psi\rangle$ and the ability to perform measurements in the basis of operators $\mathbb{O} \ni O_1, \dots, O_d$, the number of resources \mathcal{N}_P to estimate the fidelity, via the generalized Pauli fidelity estimation protocol, between the state $|\psi\rangle$

and its noisy realization $\tilde{\psi}$ within an error ϵ and with failure probability δ is given by

$$\mathcal{N}_p^\circ = \Theta(\epsilon^{-2} \ln 2/\delta). \quad (18)$$

Before moving on to the next section, a couple of remarks are in order. The above corollary tells us that it is sufficient to know a set of stabilizer operators to certify any state $|\psi\rangle$ in the Hilbert space. However, the complete knowledge of a complete set of stabilizer observables is an assumption way stronger than one may think and, in practice, can be fulfilled for a restricted set of simple states. In general, a complete set of stabilizer observables requires exhaustive search in an exponentially large space to be found, as such operators are highly nonlocal. Moreover, even if, for some reason, a verifier knows a complete set of stabilizer observables, measurements in such a basis require, in general, an exponential space in classical memory to be performed. At least, the above corollary gives a simple recipe for direct fidelity estimation protocol for those states whose stabilizers can be easily found. Let us make a clarifying example: consider a single qubit state $|\phi\rangle$ and the n -fold tensor product $|\phi\rangle^{\otimes n}$. Let o_1, o_2 be two single qubit Hermitian operators such that $o_1 |\phi\rangle = o_2 |\phi\rangle = |\phi\rangle$. The set $\{o_1, o_2\}^n$ (i) is a complete set of stabilizer observables for $|\phi\rangle^{\otimes n}$, (ii) can be efficiently found by exhaustive search in the space of one qubit, and (iii) measurements in such basis can be easily performed being a tensor product basis of operators. The same conclusions can be reached for hypergraph states, whose stabilizers are well known and easily implemented being Hermitian Clifford operators (see [103,104]). In particular, for hypergraph states, Corollary 3 constitutes a simple and alternative proof of their efficient certification.

To conclude, one could argue about the validity of the main statement of the paper: is nonstabilizerness really playing a role in the efficiency of direct fidelity estimation? The answer is “yes” because, in general, for state-agnostic verifiers, the best thing that one can do is to perform measurements in the Pauli basis, i.e., the native logic basis of operators, which turns out to be much more feasible than an exhaustive search in an exponentially large space.

B. Shadow fidelity estimation

In this section, we prove that the resources needed to estimate the fidelity via the shadow estimation protocol scale with the number of non-Clifford gates used for the state preparation. Let $|\psi\rangle$ be the state to be prepared on a quantum computer and $\tilde{\psi}$ its noisy realization prepared by the hardware. The protocol proceeds in the following steps. (i) Draw $C_1, \dots, C_k \in \mathcal{C}(n)$ independent Clifford unitary operators. (ii) For each $C_i \in \mathcal{C}(n)$, apply $\tilde{\psi}_i \equiv C_i^\dagger \tilde{\psi} C_i$, measure $\tilde{\psi}_i$ in the computational basis $\{|x\rangle \mid x \in \{0, 1\}^n\}$, and record the outcome \bar{x}_i . (iii) Perform a classical estimation of the outcome probability $|\langle \bar{x}_i | C_i | \psi \rangle|^2$. An unbiased estimator for the fidelity is then given by

$$\tilde{\mathcal{F}} = \frac{1}{k} \sum_i [(d+1) |\langle \bar{x}_i | C_i | \psi \rangle|^2 - 1], \quad (19)$$

i.e., if $p_i[\bar{x}] \equiv \text{tr}[\tilde{\psi}_i |\bar{x}\rangle\langle\bar{x}|]$ is the probability that a measurement of $\tilde{\psi}_i$ gives the string \bar{x} , then $\sum_{\bar{x} \in \{0,1\}^n} \langle p_i[\bar{x}] \tilde{\mathcal{F}} \rangle_{C_i \in \mathcal{C}} =$

$\text{tr}(\psi \tilde{\psi})$. A complete and detailed derivation of Eq. (19) is to be found in [38,60]. Before stating the result of this section, let us focus on step (iii) of the protocol. Shadow fidelity estimation protocol explicitly asks for the demanding requirement of the classical estimation of the outcome probability $|\langle \bar{x}_i | C_i | \psi \rangle|^2$. Let us see how strong such a requirement is. Calling $p_{\epsilon_a}^{(i)}$ the classical estimation of $|\langle \bar{x}_i | C_i | \psi \rangle|^2$ within an additive error ϵ_a , then $|k^{-1} \sum_i [(d+1)p_{\epsilon_a}^{(i)} - 1] - \tilde{\mathcal{F}}| \leq \epsilon_a (d+1)$, i.e., to ensure a small additive error on the estimation of the unbiased estimator in Eq. (19), one should require $\epsilon_a \sim d^{-1}$, which rules out the sampling method used in Sec. IV A leading to an exponential scaling in n for any state. Instead, if $q_{\epsilon_r}^{(i)}$ is the classical estimation of $|\langle \bar{x}_i | C_i | \psi \rangle|^2$ with a small relative error ϵ_r , then $|k^{-1} \sum_i [(d+1)q_{\epsilon_r}^{(i)} - 1] - \tilde{\mathcal{F}}| \leq (\tilde{\mathcal{F}} + 1)\epsilon_r \leq 2\epsilon_r$ (almost surely). In other words, only if one is able to estimate the outcome probability within a small relative error is a shadow fidelity estimation protocol then possible. Note that the ability to compute all the outcome probabilities of $|\psi\rangle$, as well as the marginals, within a small relative error leads to the ability of sampling from the outcome distribution, see [89], for ψ and, therefore, quantum computation conducted by such states is entirely classical.

In what follows, we use the classical simulation method introduced in Sec. III A that is able to estimate $|\langle \bar{x}_i | C_i | \psi \rangle|^2$ with no error. As explained below, this choice does not feature a loss of generality for the purpose of the paper.

Repeating steps (i), (ii), and (iii) for l times, and defining $\bar{\mathcal{F}} := \text{median}\{\mathcal{F}_s \mid s = 1, \dots, l\}$, we have the following theorem.

Theorem 3. Let $|\psi\rangle$ be a state prepared by a circuit containing a number t of T gates. Let $N_{\tilde{\psi}}$ be the number of times one needs to prepare $\tilde{\psi}$ on a quantum hardware and let N_{cl} be the number of classical resources for the classical estimation of the output probabilities. The number of resources necessary to estimate $\mathcal{F}(|\psi\rangle, \tilde{\psi})$ within an error ϵ , given by $\mathcal{N}_S = N_{\tilde{\psi}} \times N_{cl}$, is

$$\mathcal{N}_S = \Theta[2^t \epsilon^{-2} \ln \delta^{-1} (n+t)^3]. \quad (20)$$

In particular, the sample complexity is $N_{\tilde{\psi}} \equiv k \times l = \Theta(\epsilon^{-2} \ln \delta^{-1})$, where $l = 8 \ln 2 \delta^{-1}$, while the number of classical resources $N_{cl} = \Theta[2^t (n+t)^3]$.

Proof. The sample complexity bounded as $N_{\tilde{\psi}} \equiv k \times l = \Theta(\epsilon^{-2} \ln \delta^{-1})$ is to be found in [60], while the scaling of the classical postprocessing complexity is derived in Sec. III B and then the total complexity \mathcal{N}_S is given by the product; cf. Eq. (2).

Let us make a couple of remarks about the theorem.

Remark 1. One could argue about the existence of other simulation methods beyond the stabilizer formalism as matrix product decompositions (tensor network) or match-gates circuits. The question is can these methods provide better scalings for the resources in Theorem 3? The answer is “no” because the entire protocol relies on the extraction of a random Clifford circuit drawn uniformly at random according to the Haar measure over the Clifford group $\mathcal{C}(n)$ [see step (i)]; a state evolved by a random Clifford circuit C is, with overwhelming probability, far beyond being easily encodable via tensor network decomposition; in other words, $C |0^n\rangle$ features a large bond dimension. On the other hand, a random Clifford

circuit is far beyond being a match-gate circuit, because CX gates are not matchgates. We conclude that shadow fidelity estimation protocol implicitly requires a simulation method within the stabilizer formalism that, as shown in Sec. III B, scales exponentially in the number of non-Clifford gates in the circuit.

Remark 2. As anticipated, we used the simulation method for Clifford+T circuits described in Sec. III A, which is definitely not a *state of the art* method. We opted for this pedagogical choice for the sake of simplicity. Indeed, the best-known simulations method approximates outcome probabilities within a small relative error gaining only a square root advantage with respect to the exponential scaling in t . The best known simulation algorithms are able to estimate $|\langle \bar{x}_i | C_i | \psi \rangle|^2$ within a relative error ϵ_r and a failure probability p_f in time $\Theta(2^{\beta t} t^3 \epsilon_r^{-2} \ln p_f^{-1})$, where $0 < \beta \leq 1/2$ (see [89]). In other words, we have no loss of generality in concluding that Theorem 3 tells us that a shadow fidelity protocol is possible as long as the number of T gates is $t = O(\log_2 n)$, i.e., the same threshold that makes quantum computation by $|\psi\rangle$ entirely classical.

In the next section, we are going to make some comparison between the above introduced protocols.

C. Pauli fidelity estimation versus shadow fidelity estimation

In this section, we compare the two protocols discussed in this paper and highlight their differences in resource utilization. It is important to note that both protocols are inefficient and this inefficiency is governed by nonstabilizerlessness. However, they differ in the way they use resources. One key difference is that the sampling complexity of shadow fidelity estimation is independent of the size of the Hilbert space, unlike Pauli fidelity estimation. However, it should be noted that in order to achieve efficient classical postprocessing, shadow fidelity estimation requires strong classical simulation for states to be certified. Additionally, it is worth noting that shadow fidelity estimation and Pauli fidelity estimation use different types of measurement data; while shadow fidelity estimation uses randomly selected bases for measurement, Pauli fidelity estimation uses the expectation values of observables. Correspondingly, they differ in their setups for experimental implementations. Let us conclude the section with the following remark. We recall that the (bound on) number of resources for the two protocols, to certify a given state $\psi \equiv |\psi\rangle\langle\psi|$, to ensure a small error and a high success probability are

$$\begin{aligned} \mathcal{N}_P &= O(\exp M_0(\psi)), & \text{Pauli fidelity estimation,} \\ \mathcal{N}_S &= O(\exp t), & \text{shadow fidelity estimation,} \end{aligned} \quad (21)$$

where we neglected the dependency from ϵ and δ displayed in Eqs. (16) and (20), respectively. By a closer look to the scaling of the resources, one realize that, for generic states, Pauli fidelity estimation performs better than shadow fidelity estimation. Indeed, as shown in Sec. III A, one has $M_0(\psi) \leq v(\psi)$, for $v(\psi)$ being the stabilizer nullity, and thus

$$M_0(\psi) \leq t, \quad (22)$$

for t being the number of non-Clifford gates used to prepare ψ . Note that the above inequality becomes strict in many cases. One trivial example is provided by the sequential

application of T gates, because $T^2 = S$: while the zero-stabilizer entropy does not change, being invariant under Clifford operations, the number of T gates does; only using a compilation procedure aimed to reduce the T count, as the one employed in [111], one can get rid of additional useless T gates.

Let us conclude the paper with the extensions of the above results to the certification of quantum processes.

D. Quantum processes

In this section, we show that the stabilizer Rényi entropy of the Choi state $|U\rangle$ bounds the resources needed to perform a quantum process verification. Suppose one wants to characterize the quality of the application of a given unitary operator U . This task occurs in many quantum algorithms and the quantum Fourier transform provides a nice example. Let \mathcal{U} be the quantum map (in general nonunitary) applied by the quantum processor. One way to certify the quality of \mathcal{U} is through the average gate fidelity [18,29,60,112]:

$$F_{\text{avg}}(U) := \int d\psi \mathcal{F}(U|\psi\rangle, \mathcal{U}(\psi)), \quad (23)$$

i.e., the average fidelity between the application of the target unitary on $|\psi\rangle$ and the quantum map on $\psi \equiv |\psi\rangle\langle\psi|$, according to the Haar measure $d\psi$. One can easily show, via a Kraus operator expansion, see Appendix C, that $F_{\text{avg}}(U) = \mathcal{F}_U + O(d^{-1})$, where

$$\mathcal{F}_U := \frac{1}{d^4} \sum_{\mu\nu} \text{tr}(P_\mu U P_\nu U^\dagger) \text{tr}[P_\mu \mathcal{U}(P_\nu)] \quad (24)$$

is the *entanglement fidelity* between U and the quantum map $\mathcal{U}(\cdot)$ [60]. Let us use the same trick as before: define a probability distribution $\Xi_U := \{\text{tr}^2(P_\mu U P_\nu U^\dagger)/d^4 \mid \mu, \nu = 1, \dots, d^2\}$ and rewrite \mathcal{F}_U as the average of $\mathcal{X}_{\mu\nu} := \text{tr}[P_\mu \mathcal{U}(P_\nu)]/\text{tr}(P_\mu U P_\nu U^\dagger)$ on the probability distribution Ξ_U , i.e., $\mathcal{F}_U = \langle \mathcal{X}_{\mu\nu} \rangle_{\Xi_U}$. \mathcal{F}_U can thus be estimated via Monte Carlo methods by sampling k pairs of Pauli operators $(P_1, P'_1), \dots, (P_k, P'_k)$ according to the probability distribution Ξ_U . We quantify the resources as the number of uses N_U of the channel \mathcal{U} . Note that, from Lemma 1, the probability distribution Ξ_U coincides with the probability distribution associated with the Choi state $|U\rangle$. The following theorem provides bounds for the number of resources needed to estimate \mathcal{F}_U in terms of the stabilizer Rényi entropy $M_\alpha(|U\rangle)$.

Theorem 4. The number of resources N_U to estimate \mathcal{F}_U with accuracy ϵ and success probability $1 - \delta$ is bounded by

$$\frac{2}{\epsilon^2} \ln(2/\delta) \exp[M_2(|U\rangle)] \leq N_U \leq \frac{64}{\epsilon^4} \ln(2/\delta) \exp[M_0(|U\rangle)]. \quad (25)$$

See Appendix C for the proof. We found that the nonstabilizerlessness of the Choi state $|U\rangle$ is a direct quantifier of the hardness in verifying the correct application of a target unitary U . The result presented in Lemma 2 tells the meaning of the stabilizer Rényi entropy $M_\alpha(|U\rangle)$.

Corollary 4. The resources N_U are bounded:

$$\Theta[OTOC_8(U)^{-1}] \leq N_U \leq \Theta(\exp[v(U)]), \quad (26)$$

where $OTOC_8(U)$ is defined in Lemma 2 and $v(U)$ is the unitary stabilizer nullity.

Therefore, the more chaotic the evolution generated by U is, the smaller the out-of-time-order correlators are [91] and the harder the certification via direct fidelity estimation is.

In the same fashion of doped stabilizer states, the doped Clifford circuits provide an important class of circuits to look at. A t -doped Clifford circuit [94, 113] consists of global layers of Clifford gates interleaved by single qubit T gates. Bravyi and Gosset [89] proved that the classical simulations of such circuits scale exponentially with the number of T gates, while in [94] we proved that to mimic quantum chaotic evolution, a quantum circuit should contain at least $O(n)$ T gates, showing the impossibility to simulate quantum chaos classically. In this scenario, we ask the question of whether quantum chaos can be effectively certified by the above fidelity estimation protocol. The following theorem determines the scaling of N_U with the number t of T gates.

Corollary 5. Let $\langle N_{C_t} \rangle$ be the average number of resources to verify a t -doped Clifford circuit C_t ; then it increases exponentially with t :

$$\Theta(\exp[t \log_2 4/3]) \leq \langle N_{C_t} \rangle \leq \Theta(\exp[t]) \leq \Theta(d^2). \quad (27)$$

The answer is no: quantum chaos cannot be efficiently certified, as the protocol is efficient up to $O(\log_2 n)$ T gates injected in a Clifford circuit. See Appendix C for the proof. Let us now briefly comment on the scalings of the bounds in Eq. (27). First, note that such scalings are the same as those in Corollary 1: while for states the resources are upper bounded by $\Theta(d)$ and the bound is saturated after the injection of “only” n non-Clifford gates, for unitary operators the injection of more than n non-Clifford resources makes the verification even harder.

V. SUMMARY AND DISCUSSION

In this paper, we showed the tight connection underlying quantum certification via direct fidelity estimation, nonstabilizerness, and chaos. We showed that the complexity of Pauli fidelity estimation and shadow fidelity estimation scales exponentially with the number of non-Clifford gates and thus with the nonstabilizerness $M(|\psi\rangle)$. This fact implies the impossibility of such protocols to certify all the states $|\psi\rangle$ beyond the efficiency threshold $M(|\psi\rangle) = O(\log_2 n)$. Remarkably, the protocol fails to certify all those states which turn out to be useful to achieve quantum speedups. In other words, there is no free lunch: any quantum certification protocol aimed to directly estimate the fidelity between the theoretical state and the actual state becomes inefficient, and this inefficiency is governed by nonstabilizerness, the resource which makes quantum technology truly quantum. However, we note that the inefficiency is due to the wide applicability of such protocols: there exist other protocols aimed to certify particular sets of states that, although possessing a high amount of nonstabilizerness, can be efficiently certified. One prominent example is the set of hypergraph states. Such states feature an extensive amount of nonstabilizerness, making both Pauli fidelity estimation and shadow fidelity estimation unfeasible, but possess efficiently encodable stabilizer operators that make their certification possible, as shown in Sec. IV A (see Corollary 3). The scope of this work is to rule out the use of general and widely applicable protocols for direct fidelity estimation and, at the

same time, to leave the window open for state-aware protocols aimed to certify certain specific classes of states. After all, the class of quantum states that are truly useful for a quantum computational speedup is of measure zero in the Hilbert space [114] and, therefore, there is no need for a general protocol able to certify every quantum state.

ACKNOWLEDGMENTS

L.L. and S.F.E.O. thank Sarah True for helpful comments. The authors acknowledge support from NSF Award No. 2014000. The work of L.L. and S.F.E.O. was supported in part by College of Science and Mathematics Dean’s Doctoral Research Fellowship through fellowship support from Oracle, Project ID R20000000025727. A.H. acknowledges financial support from PNRR MUR project PE0000023-NQSTI and PNRR MUR project CN_00000013-ICSC.

APPENDIX A: STABILIZER RÉNYI ENTROPY

1. Proof of Lemma 1

In this section, we prove that the nonstabilizerness of the Choi-Jamiołkowski isomorphism can be measured as the Rényi entropy of the probability distribution Ξ_U whose elements are

$$\Xi_U(P, P') = \frac{\text{tr}^2(PUP'U^\dagger)}{d^4}. \quad (A1)$$

Recall that the Choi isomorphism is a map from the space of operator $\mathcal{B}(\mathcal{H})$ to state vectors in $\mathcal{H}^{\otimes 2}$. Let U be a unitary operator; its Choi isomorphism $|U\rangle \in \mathcal{H}^{\otimes 2}$ is defined as

$$|U\rangle := (\mathbb{1} \otimes U) |I\rangle, \quad |I\rangle = \frac{1}{\sqrt{d}} \sum_i |i\rangle \otimes |i\rangle. \quad (A2)$$

Let us compute the stabilizer Rényi entropy of $|U\rangle$. Since now we are working with states of $\mathcal{H}^{\otimes 2}$, the Pauli group is $\mathbb{P}(2n) = \mathbb{P}(n) \otimes \mathbb{P}(n)$, and the coefficients of the probability distribution for $|U\rangle$ read

$$\Xi_U(P \otimes P') = \frac{1}{d^2} \text{tr}^2(P \otimes P' |U\rangle\langle U|), \quad P, P' \in \mathbb{P}(n), \quad (A3)$$

the stabilizer Rényi entropy reads

$$M_\alpha(|U\rangle) = \frac{1}{1-\alpha} \log_2 \sum_{P, P'} |\Xi_U(P \otimes P')|^\alpha - 2 \log_2 d. \quad (A4)$$

Let us prove that the coefficients $\text{tr}(P \otimes P' |U\rangle\langle U|) \propto \frac{1}{d} \text{tr}(PUP'U^\dagger)$ up to a global phase ± 1 . First, it is well known that the trace is invariant under partial transpose: let $A, B \in \mathcal{B}(\mathcal{H})$ two operators on \mathcal{H} ; then the partial transpose is defined as $(A \otimes B)^{T_2} := A \otimes B^T$, where B^T is the transpose of B ,

$$\begin{aligned} \text{tr}(P \otimes P' |U\rangle\langle U|) &= \text{tr}(P \otimes P' |U\rangle\langle U|)^{T_2} \\ &= \pm \text{tr}(P \otimes P' |U\rangle\langle U|^{T_2}), \end{aligned} \quad (A5)$$

where the \pm comes from the fact that $P^T \propto P'$ up to a sign (because $Y^T = -Y$, $X^T = X$, and $Z^T = Z$). Now

$$\begin{aligned} |U\rangle\langle U|^{T_2} &= (\mathbb{1} \otimes U^T) |I\rangle\langle I|^{T_2} (\mathbb{1} \otimes U^*) \\ &= (\mathbb{1} \otimes U^T) \frac{\hat{S}}{d} (\mathbb{1} \otimes U^*) = \frac{\hat{S}}{d} (U^T \otimes U^*), \end{aligned} \quad (A6)$$

where \hat{S} is the swap operator. The fact that $|I\rangle\langle I|^{T_2} = \frac{\hat{S}}{d}$ can be checked straightforwardly; then

$$\text{tr}(P \otimes P' |U\rangle\langle U|) = \frac{\pm 1}{d} \text{tr}(PU^T P' U^*) = \frac{\pm 1}{d} \text{tr}(P' U P U^\dagger). \quad (\text{A7})$$

Thus we obtain that the elements of the probability distribution Ξ_U read

$$\Xi_U(P, P') = \frac{1}{d^2} \text{tr}^2(P \otimes P' |U\rangle\langle U|) = \frac{1}{d^4} \text{tr}^2(P' U P U^\dagger) \quad (\text{A8})$$

and the lemma follows straightforwardly.

2. Proof of Lemma 2

From Lemma 1, we have that

$$\begin{aligned} M_\alpha(|U\rangle) &= \frac{1}{1-\alpha} \log_2 \sum_{P, P'} \frac{\text{tr}^{2\alpha}(P U P' U^\dagger)}{d^{4\alpha}} - \log_2 d^2 \\ &= \frac{1}{1-\alpha} \log_2 \frac{1}{d^2} \sum_{P, P'} \frac{\text{tr}^{2\alpha}(P U P' U^\dagger)}{d^{2\alpha}}. \end{aligned} \quad (\text{A9})$$

To prove the Lemma, we recall the following identity:

$$\hat{S} = \frac{1}{d} \sum_P P^{\otimes 2}, \quad (\text{A10})$$

where \hat{S} is the swap operator. Note that

$$\begin{aligned} &\frac{\text{tr}(P U P' U^\dagger)}{d} \frac{\text{tr}(P U P' U^\dagger)}{d} \\ &= \frac{1}{d^2} \sum_{P_1} \frac{\text{tr}(P U P' U^\dagger P_1 P U P' U^\dagger P_1)}{d} \\ &\equiv \frac{\text{tr}(\langle P U P' U^\dagger P_1 P U P' U^\dagger P_1 \rangle_{P_1})}{d}. \end{aligned} \quad (\text{A11})$$

We thus can recursively use the above identity and arrive to

$$\begin{aligned} \frac{\text{tr}^{2\alpha}(P U P' U^\dagger)}{d^{2\alpha}} &= d^{-1} \text{tr} \left[\left\langle P_{2\alpha} \prod_{i=1}^{2\alpha} U P U^\dagger P' P_{i-1} P_i \right\rangle \right] \\ &= \text{otoc}_{4\alpha}(P, P'), \end{aligned} \quad (\text{A12})$$

where $\langle \cdot \rangle \equiv d^{-2} \sum_{P_i \in \mathbb{P}(n)}$ for all $i = 1, \dots, 2\alpha$, while $P_0 \equiv \mathbb{I}$. Let us write the above explicitly for $\alpha = 2$:

$$\begin{aligned} \frac{\text{tr}^4(P U P' U^\dagger)}{d^4} &= d^{-1} \text{tr}(\langle P_4 P^{(U)} P' P_1 P^{(U)} P' P_1 P_2 P^{(U)} \\ &\quad \times P' P_2 P_3 P^{(U)} P' P_3 P_4 \rangle_{P_1, \dots, P_4}) \\ &= d^{-1} \text{tr}(\langle P^{(U)} P' P_1 P^{(U)} P' P_1 P_2 P^{(U)} \\ &\quad \times P' P_2 P_3 P^{(U)} P' P_3 \rangle_{P_1, \dots, P_4}) = \text{otoc}_8(P, P'). \end{aligned} \quad (\text{A13})$$

Note that the above holds for any integer $\alpha > 1$.

APPENDIX B: QUANTUM STATES CERTIFICATION

1. Proof of Theorem 2

In this section, we give proof of the main theorem in the manuscript. Some parts of the proof are inspired by the work of Flammia *et al.* [29]; see also [60]. We prove the two bounds separately.

(i) *Lower bound.* Here we need to lower bound the necessary resources such that the estimator $\tilde{\mathcal{F}} = \frac{1}{k} \sum_{P \in \mathbb{K}} \tilde{X}_P$, defined in the main text, obeys to

$$\Pr(|\mathcal{F} - \tilde{\mathcal{F}}| \leq \epsilon) \geq 1 - \delta. \quad (\text{B1})$$

To prove it, define $m := \min_P |\text{tr}(P\psi)|$ and note that $|\tilde{X}_P| \leq m^{-1}$. Using Hoeffding's inequality [115], one can bound the probability

$$\Pr(|\mathcal{F} - \tilde{\mathcal{F}}| \leq \epsilon) \geq 1 - 2 \exp \left[-\frac{k\epsilon^2}{2m^{-2}} \right]. \quad (\text{B2})$$

To have the probability lower bounded by $1 - \delta$, the number of samples k must be

$$k = \frac{2}{\epsilon^2 m^2} \ln(2/\delta). \quad (\text{B3})$$

Setting the number of copies $c_P(\tilde{\psi})$ of the state $\tilde{\psi}$ to determine each sampled P to be one (one-shot measurements), i.e., $c_P(\tilde{\psi}) = 1 \forall P$, one has that $N_{\tilde{\psi}} \equiv k$. Let us lower bound the number of resources $N_{\tilde{\psi}}$. Let $P \in \mathbb{P}(n)$; then the average of $|\text{tr}(P\psi)|$ over the state dependent probability distribution Ξ_ψ is upper bounded by

$$\langle |\text{tr}(P\psi)| \rangle_{\Xi_\psi} \leq \sqrt{\langle \text{tr}^2(P\psi) \rangle_{\Xi_\psi}} = \sqrt{\exp[-M_2(|\psi\rangle)]}. \quad (\text{B4})$$

Then since $m = \min_P |\text{tr}(P\psi)|$, one trivially has $m \leq \langle |\text{tr}(P\psi)| \rangle_{\Xi_\psi}$ and thus $m \leq \sqrt{\exp[-M_2(|\psi\rangle)]}$. Thus the number of resources $N_{\tilde{\psi}}$ is lower bounded:

$$N_{\tilde{\psi}} \geq \frac{2}{\epsilon^2} \ln(2/\delta) \exp[M_2(|\psi\rangle)]. \quad (\text{B5})$$

(ii) *Upper bound.* Let $\psi = |\psi\rangle\langle\psi|$ be the state we want to verify. Let us define the following operator (in the Pauli basis fashion):

$$\text{tr}(P\psi_{\text{cut}}) := \begin{cases} \text{tr}(P\psi), & \text{if } |\text{tr}(P\psi)| \geq \frac{\epsilon}{2\sqrt{2}} \sqrt{\exp[-M_0(\psi)]}, \\ 0, & \text{otherwise} \end{cases} \quad (\text{B6})$$

and its normalized version $\psi' := \psi_{\text{cut}} / \|\psi_{\text{cut}}\|_2$. Define $\mathbb{Q} := \{P \in \mathbb{P}(n) \mid |\text{tr}(P\psi)| \geq \epsilon/2\sqrt{2} \sqrt{\exp[-M_0(\psi)]}\}$ so that ψ' in the Pauli basis reads

$$\psi' = \frac{1}{\sqrt{\frac{1}{d} \sum_{P \in \mathbb{Q}} \text{tr}^2(P\psi)}} \frac{1}{d} \sum_{P \in \mathbb{Q}} \text{tr}(P\psi) P. \quad (\text{B7})$$

Let us evaluate the difference between $\mathcal{F}'(\psi', \tilde{\psi}) := \text{tr}(\psi' \tilde{\psi})$ and the true fidelity $\mathcal{F}(|\psi\rangle, \tilde{\psi})$:

$$|\mathcal{F}' - \mathcal{F}| \leq \|\psi' - \psi\|_2 = \sqrt{2[1 - \text{tr}(\psi\psi')]} \quad (\text{B8})$$

In the above we used $\text{tr}(\psi'^2) = 1$. Let us evaluate $\text{tr}(\psi\psi')$ by writing it in the Pauli basis:

$$\begin{aligned} \text{tr}(\psi\psi') &= \frac{1}{\|\psi_{\text{cut}}\|_2} \frac{1}{d} \sum_{P \in \mathbb{Q}} \text{tr}^2(P\psi) = \sqrt{\frac{1}{d} \sum_{P \in \mathbb{Q}} \text{tr}^2(P\psi)} \\ &= \sqrt{1 - \frac{1}{d} \sum_{P \in \mathbb{Q}} \text{tr}^2(P\psi)} \\ &\geq \sqrt{1 - \frac{\epsilon^2 \exp[-M_0(\psi)] |\mathbb{Q}|}{8d}}, \end{aligned} \quad (\text{B9})$$

where $\bar{\mathbb{Q}}$ is the complement set of \mathbb{Q} . Note that $|\bar{\mathbb{Q}}| = \text{card}(\psi) - |\mathbb{Q}|$ —where $\text{card}(\psi) := |\{P \mid \text{tr}(P\psi) \neq 0\}|$ —and that $\text{card}(\psi)/d = \exp[M_0(\psi)]$. We obtain $\text{tr}(\psi\psi') \geq \sqrt{1 - \epsilon^2/8} \geq 1 - \epsilon^2/8$ and thus

$$|\mathcal{F}' - \mathcal{F}| \leq \frac{\epsilon}{2}. \quad (\text{B10})$$

Note that \mathcal{F}' can be estimated in the same fashion as \mathcal{F} :

$$\mathcal{F}' = \frac{1}{d} \sum_P \text{tr}(P\tilde{\psi}) \text{tr}(P\psi') = \langle X'_P \rangle_{\Xi_{\psi'}}, \quad (\text{B11})$$

where the average is taken over the probability distribution $\Xi_{\psi'}$ whose elements are

$$\Xi_{\psi'}(P) = \begin{cases} \frac{\text{tr}^2(\psi P)}{\sum_{P \in \mathbb{Q}} \text{tr}^2(P\psi)}, & P \in \mathbb{Q}, \\ 0, & \text{otherwise} \end{cases} \quad (\text{B12})$$

and $X'_P := \frac{\text{tr}(P\tilde{\psi})}{\text{tr}(P\psi')}$. Thus we define $\tilde{\mathcal{F}}'$ the estimator of \mathcal{F}' obtained by sampling the probability distribution $\Xi_{\psi'}$ and by experimentally measuring $X'_P \in \mathbb{K}'$:

$$\tilde{\mathcal{F}}' = \frac{1}{k} \sum_{P \in \mathbb{K}'} \tilde{X}'_P, \quad (\text{B13})$$

where $\tilde{X}'_P = \frac{1}{\text{tr}(P\psi')} \frac{1}{c_P(\tilde{\psi})} \sum_{j=1}^{c_P(\tilde{\psi})} \mathcal{P}_{P_j}(\tilde{\psi})$, $c_P(\tilde{\psi})$ is the number of copies $\tilde{\psi}$ used to estimate $P \in \mathbb{K}$, and $\mathcal{P}_{P_j}(\tilde{\psi})$ is the outcome of a one-shot measurement of P .

Let us prove that, setting $N_{\tilde{\psi}} \leq \frac{64}{\epsilon^4} \ln(2/\delta) \exp[M_0(\psi)]$, we have

$$\Pr(|\mathcal{F} - \tilde{\mathcal{F}}| \leq \epsilon) \geq 1 - \delta. \quad (\text{B14})$$

First

$$|\mathcal{F} - \tilde{\mathcal{F}}| \leq |\mathcal{F} - \mathcal{F}'| + |\mathcal{F}' - \tilde{\mathcal{F}}| \leq \frac{\epsilon}{2} + |\mathcal{F}' - \tilde{\mathcal{F}}|. \quad (\text{B15})$$

Then note that $\Pr(|\mathcal{F} - \tilde{\mathcal{F}}| \leq \epsilon) = \Pr(|\mathcal{F}' - \tilde{\mathcal{F}}| \leq \epsilon/2)$. Since $\mathbb{E}(\tilde{\mathcal{F}}') = \mathcal{F}'$, i.e., $\tilde{\mathcal{F}}'$ is an unbiased estimator for \mathcal{F}' , we can use Hoeffding's inequality:

$$\Pr(|\mathcal{F}' - \tilde{\mathcal{F}}'| \leq \epsilon/2) = 1 - 2 \exp\left[-\frac{km'^2\epsilon^2}{8}\right], \quad (\text{B16})$$

where $m' := \min_P |\text{tr}(\psi'P)|$ and thus $|\tilde{X}'_P| \leq m^{-1}$. To have that the probability is lower bounded by $1 - \delta$, we impose that $c_P(\tilde{\psi}) = 1$ for any $P \in \mathbb{Q}$ and

$$N_{\tilde{\psi}} = k = \frac{8}{\epsilon^2 m^2} \ln(2/\delta). \quad (\text{B17})$$

To prove the upper bound to the number of resources $N_{\tilde{\psi}}$ it is sufficient to note that

$$\begin{aligned} m' &= \min_{P \in \mathbb{Q}} \frac{|\text{tr}(P\psi)|}{\sqrt{\frac{1}{d} \sum_{P \in \mathbb{Q}} \text{tr}^2(P\psi)}} \geq \min_{P \in \mathbb{Q}} |\text{tr}(P\psi)| \\ &\geq \frac{\epsilon}{2\sqrt{2}} \sqrt{\exp[-M_0(\psi)]}, \end{aligned} \quad (\text{B18})$$

where we exploited once again the fact that $\sqrt{\frac{1}{d} \sum_{P \in \mathbb{Q}} \text{tr}^2(P\psi)} \leq 1$. We finally obtain

$$N_{\tilde{\psi}} \leq \frac{64}{\epsilon^4} \ln(2/\delta) \exp[M_0(\psi)], \quad (\text{B19})$$

which concludes the proof.

2. Proof of Corollary 1

From the main theorem, we have that

$$\begin{aligned} &\frac{2}{\epsilon^2} \ln(2/\delta) \langle \exp[M_2(\psi_t)] \rangle \\ &\leq \langle N_{\tilde{\psi}_t} \rangle \leq \frac{64}{\epsilon^4} \ln(2/\delta) \langle \exp[M_0(\psi_t)] \rangle. \end{aligned} \quad (\text{B20})$$

The average of the left-hand side for states can be lower bounded through the Jensen inequality and we obtain

$$\langle N_{\tilde{\psi}_t} \rangle \geq \frac{2}{\epsilon^2} \ln(2/\delta) \langle \exp[M_2(\psi_t)] \rangle \geq \frac{2}{\epsilon^2} \ln(2/\delta) \frac{1}{\langle \text{tr}(Q\psi_t^{\otimes 4}) \rangle}, \quad (\text{B21})$$

where $Q = \frac{1}{d^2} \sum_{P \in \mathcal{P}_n} P^{\otimes 4}$. Then the average over t -doped stabilizer states $|\psi_t\rangle$ can be computed using the techniques in [68,116]. The result is shown in Eq. (13) of [68]:

$$\langle \exp[M_2(\psi_t)] \rangle \geq \frac{d+3}{4+(d-1)f_+^t} = \Theta(\exp[t \log_2 4/3]), \quad (\text{B22})$$

where $f_+ = \frac{3d^2-3d-4}{4(d^2-1)}$ and this concludes the proof.

The right-hand side can be upper bounded using the stabilizer nullity. Recall that

$$\exp[M_0(\psi_t)] \leq \exp[\nu(|\psi_t\rangle)], \quad (\text{B23})$$

where $\nu(|\psi_t\rangle)$ is the stabilizer nullity of the t -doped stabilizer state. We can write such a state as $|\psi_t\rangle = C_t |0\rangle^{\otimes n}$, where C_t is a doped Clifford circuit, i.e., layers of Clifford operators interleaved by the action of single qubit T gates. Then [96] we have the following chain of inequality:

$$\nu(|\psi_t\rangle) = \nu(C_t |0\rangle^{\otimes n}) \leq \nu(C_t) \leq t, \quad (\text{B24})$$

where $\nu(C_t)$ is the unitary stabilizer nullity, introduced in [96], which lower bounds the number of non-Clifford resources injected in a Clifford unitary operator. Therefore, we obtain

$$\exp[M_0(\psi_t)] \leq \exp[t]. \quad (\text{B25})$$

Lastly note that, since $M_0(\psi_t) \leq \log_2 d$, we have $\langle N_{\tilde{\psi}_t} \rangle \leq d$.

APPENDIX C: UNITARY OPERATORS

1. Entanglement fidelity

In this section we prove that $F_{\text{avg}} = \mathcal{F}_U + O(d^{-1})$, i.e., the average gate fidelity F_{avg} is the entanglement fidelity \mathcal{F}_U up to an error scaling as $O(d^{-1})$. Let us start with the definition of average gate fidelity given in the main text:

$$F_{\text{avg}}(U) := \int d\psi \text{tr}[U\psi U^\dagger \mathcal{U}(\psi)]. \quad (\text{C1})$$

By expanding \mathcal{U} in terms of Kraus operator A_α one can write the above as

$$F_{\text{avg}} = \sum_\alpha \int d\psi \text{tr}(U\psi U^\dagger A_\alpha \psi A_\alpha^\dagger). \quad (\text{C2})$$

By the well-known identity [117] $\int d\psi \psi^{\otimes 2} = [d(d+1)]^{-1} (\mathbb{I} + \hat{S})$, one has

$$F_{\text{avg}} = \frac{\frac{1}{d} \sum_\alpha \text{tr}(U^\dagger \otimes U A_\alpha \otimes A_\alpha^\dagger) + 1}{d+1}. \quad (\text{C3})$$

Multiplying by $\mathbb{I}^{\otimes 2} \equiv \hat{S}\hat{S}$ and by expanding both $\hat{S}U \otimes U^\dagger$ and $\hat{S}A_i \otimes A_i^\dagger$ in terms of the Pauli operators on $\mathcal{H}^{\otimes 2}$, we have

$$\text{tr}(U^\dagger \otimes UA_\alpha \otimes A_\alpha^\dagger) = \frac{1}{d^2} \sum_{\mu\nu} \text{tr}(P_\mu U P_\nu U^\dagger) \text{tr}(P_\mu A_\alpha P_\nu A_\alpha^\dagger). \quad (\text{C4})$$

Finally $F_{\text{avg}} = \mathcal{F}_U + O(d^{-1})$, where we defined

$$\mathcal{F}_U := \frac{1}{d^4} \sum_{\mu\nu} \text{tr}(P_\mu U P_\nu U^\dagger) \text{tr}[P_\mu \mathcal{U}(P_\nu)]. \quad (\text{C5})$$

2. Proof of Theorem 4

In this section, we prove Theorem 4. We give the proof for the lower and the upper bound separately.

(i) *Lower bound.* Let $(P_1, P'_1), \dots, (P_k, P'_k)$ be k pairs of Pauli operators sampled at random according to the probability distribution Ξ_U and labeled by $i = 1, \dots, k$. Let $\tilde{\mathcal{F}}_U =$

$\frac{1}{k} \sum_{i=1}^k \tilde{\mathcal{X}}_i$ be an estimator for \mathcal{F}_U , i.e., $\mathbb{E}[\tilde{\mathcal{F}}_U] = \mathcal{F}_U$, where

$$\mathcal{X}_i = \frac{1}{\text{tr}(U P_i U^\dagger P'_i)} \frac{1}{c_i(\mathcal{U})} \sum_{j=1}^{c_i(\mathcal{U})} \mathcal{P}_{ij}(\mathcal{U}), \quad (\text{C6})$$

where $\mathcal{P}_{ij}(\mathcal{U})$ is the j th measurement of $\text{tr}[\mathcal{U}(P_i P'_i)]$ and $c_i(\mathcal{U})$ are the number of copies needed to estimate a given pair (P_i, P'_i) for $i = 1, \dots, k$. Following the proof of Theorem 2, define $m_U := \min_{P, P'} |\text{tr}(U^\dagger P U P')|/d$ and note that $|\tilde{\mathcal{X}}_i| \leq m_U^{-1}$. Using Hoeffding's inequality we have that

$$\Pr(|\tilde{\mathcal{F}}_U - \mathcal{F}_U| \leq \epsilon) \geq 1 - 2 \exp \left[-\frac{k\epsilon^2}{2m_U^{-2}} \right]. \quad (\text{C7})$$

Thus, by imposing the probability to be lower bounded by $1 - \delta$ and by setting $c_i(\mathcal{U}) = 1$ for any i (i.e., one-shot measurements) one gets

$$\mathcal{N}_U = \frac{2}{\epsilon^2 m_U^2} \ln(2/\delta) \quad (\text{C8})$$

to prove the lower bound is sufficient to note that

$$m_U := \min_{P, P'} |\text{tr}(U^\dagger P U P')|/d \leq \langle d^{-1} |\text{tr}(U^\dagger P U P')| \rangle_{\Xi_U} \leq d^{-1} \sqrt{\sum_{P, P'} \frac{\text{tr}^4(U^\dagger P U P')}{d^4}} \equiv \sqrt{\exp[-M_2(|U\rangle)]}, \quad (\text{C9})$$

where $M_2(|U\rangle)$ is the stabilizer Rényi entropy of the Choi state $|U\rangle$; cf. Lemma 1.

(ii) *Upper bound.* To prove the upper bound let us define an auxiliary operator U_{cut} with a similar technique of the one used for pure states. Define the following coefficients:

$$\text{tr}(U_{\text{cut}}^\dagger P U_{\text{cut}} P') := \begin{cases} \text{tr}(U^\dagger P U P'), & \text{if } |\text{tr}(U^\dagger P U P')|/d \geq \theta \sqrt{\exp[-M_0(|U\rangle)]}, \\ 0, & \text{otherwise} \end{cases} \quad (\text{C10})$$

and $\mathbb{Q}_U := \{P, P' \mid \text{tr}(U_{\text{cut}}^\dagger P U_{\text{cut}} P') \neq 0\}$. Now define the operator U' such that

$$\hat{S}U'^\dagger \otimes U' = \frac{1}{\sqrt{\sum_{P, P' \in \mathbb{Q}_U} \text{tr}^2(U^\dagger P U P')}} \sum_{P, P' \in \mathbb{Q}_U} \text{tr}(U^\dagger P U P') P \otimes P'. \quad (\text{C11})$$

Let us evaluate the difference between $\mathcal{F}_{U'} := \frac{1}{d^2} \sum_\alpha \text{tr}(U'^\dagger \otimes U' A_\alpha \otimes A_\alpha^\dagger)$ and \mathcal{F}_U defined in the main text:

$$|\mathcal{F}_{U'} - \mathcal{F}_U| \leq \frac{1}{d^2} \left\| \sum_\alpha A_\alpha \otimes A_\alpha^\dagger \right\|_2 \|U'^\dagger \otimes U' - U^\dagger \otimes U\|_2 \leq \frac{1}{d} \|U'^\dagger \otimes U' - U^\dagger \otimes U\|_2. \quad (\text{C12})$$

Now evaluate $\|U'^\dagger \otimes U' - U^\dagger \otimes U\|_2$ recalling that $\text{tr}(U'^\dagger \otimes U' U^\dagger \otimes U) = d^2$:

$$\frac{1}{d} \|U'^\dagger \otimes U' - U^\dagger \otimes U\|_2 = \sqrt{2 \left(1 - \frac{1}{d^2} \text{tr}(U'^\dagger \otimes U' U^\dagger \otimes U) \right)}, \quad (\text{C13})$$

$$\frac{1}{d^2} \text{tr}(U'^\dagger \otimes U' U^\dagger \otimes U) = \frac{1}{d^2} \text{tr}[\hat{S}(U'^\dagger \otimes U') \hat{S}(U^\dagger \otimes U)] = \frac{1}{d^2} \frac{1}{\sqrt{\sum_{P, P' \in \mathbb{Q}_U} \text{tr}^2(U^\dagger P U P')}} \sum_{P, P' \in \mathbb{Q}_U} \text{tr}^2(U^\dagger P U P'). \quad (\text{C14})$$

We are just left to the following series of inequalities:

$$\sum_{P, P' \in \mathbb{Q}_U} \text{tr}^2(U^\dagger P U P') = d^4 - \sum_{P, P' \in \bar{\mathbb{Q}}_U} \text{tr}^2(U^\dagger P U P') > d^4 - \frac{\theta^2 d^4 |\bar{\mathbb{Q}}_U|}{\text{card}(U)} > d^4 (1 - \theta^2), \quad (\text{C15})$$

where we used the fact that $\text{tr}^2(U^\dagger P U P') < \theta \sqrt{\exp[M_0(|U\rangle)]}$ iff $P \in \bar{\mathbb{Q}}_U$, where $\bar{\mathbb{Q}}_U$ is the complement set of \mathbb{Q}_U . Moreover, note that $|\bar{\mathbb{Q}}_U| = \text{card}(U) - |\mathbb{Q}_U| < \text{card}(U)$, where $\text{card}(U) := |\{P, P' \mid \text{tr}(P U P' U^\dagger) \neq 0\}|$ and $M_0(|U\rangle) = \log_2 \frac{\text{card}(U)}{d^2}$. We finally obtain that

$$|\mathcal{F}_{U'} - \mathcal{F}_U| \leq \frac{1}{d} \|U'^\dagger \otimes U' - U^\dagger \otimes U\|_2 \leq \sqrt{2}\theta. \quad (\text{C16})$$

Now, $\mathcal{F}_{U'}$ can be estimated in a similar fashion to \mathcal{F}_U via Monte Carlo sampling; indeed,

$$\mathcal{F}_{U'} = \frac{1}{d^2} \sum_{\alpha} \text{tr}(U'^{\dagger} \otimes U' A_{\alpha} \otimes A_{\alpha}^{\dagger}) = \frac{1}{d^4} \sum_{\mu, \nu} \text{tr}[P_{\mu} \mathcal{U}(P_{\nu})] \text{tr}(P_{\mu} U' P_{\nu} U'^{\dagger}) = \langle \mathcal{X}'_{\mu\nu} \rangle_{\Xi_{U'}}, \quad (\text{C17})$$

where $\mathcal{X}'_{\mu\nu} := \text{tr}[P_{\mu} \mathcal{U}(P_{\nu})] / \text{tr}(P_{\mu} U' P_{\nu} U'^{\dagger})$ and $\Xi_{U'}$ is a probability distribution whose elements are

$$\Xi_{U'}(P_{\mu}, P_{\nu}) = \begin{cases} \frac{\text{tr}^2(P_{\mu} U' P_{\nu} U'^{\dagger})}{\sum_{P, P' \in \mathbb{Q}_U} \text{tr}^2(P U' P' U'^{\dagger})}, & P_{\mu}, P_{\nu} \in \mathbb{Q}_U, \\ 0, & \text{otherwise.} \end{cases} \quad (\text{C18})$$

We can now define the estimator $\tilde{\mathcal{F}}_{U'}$ of $\mathcal{F}_{U'}$ in the usual way:

$$\tilde{\mathcal{F}}_{U'} = \frac{1}{k} \sum_i \tilde{\mathcal{X}}'_i, \quad (\text{C19})$$

where $\tilde{\mathcal{X}}'_i = \frac{1}{\text{tr}(P_i U' P_i U'^{\dagger})} \frac{1}{c_i(\mathcal{U})} \sum_{j=1}^{c_i(\mathcal{U})} P_{ij}(\mathcal{U})$. We are ready to bound the probability to measure \mathcal{F}_U with accuracy ϵ and find an upper bound to the resources $N_{\mathcal{U}}$:

$$\Pr(|\mathcal{F}_U - \tilde{\mathcal{F}}_{U'}| \leq \epsilon) \geq 1 - \delta. \quad (\text{C20})$$

First $|\mathcal{F}_U - \tilde{\mathcal{F}}_{U'}| \leq |\mathcal{F}_U - \mathcal{F}_{U'}| + |\mathcal{F}_{U'} - \tilde{\mathcal{F}}_{U'}| \leq \sqrt{2}\theta + |\mathcal{F}_{U'} - \tilde{\mathcal{F}}_{U'}|$. Then, defining $m'_U := \min_P |\text{tr}(P_i U' P_j U'^{\dagger})|/d$, since $\mathbb{E}\tilde{\mathcal{F}}_{U'} = \mathcal{F}_{U'}$ we can use Hoeffding's inequality to

bound the probability as

$$\Pr(|\mathcal{F}_{U'} - \tilde{\mathcal{F}}_{U'}| \leq \epsilon/2) \leq 1 - 2 \exp\left[-\frac{k\epsilon^2 m_U'^2}{8}\right]. \quad (\text{C21})$$

Setting the probability to be greater than $1 - \delta$, we find the necessary resources to be

$$N_{\mathcal{U}} = \frac{8}{\epsilon^2 m_U'^2} \ln(2/\delta). \quad (\text{C22})$$

Setting $\theta\sqrt{2} = \epsilon/2$, we find $\Pr(|\mathcal{F}_U - \tilde{\mathcal{F}}_{U'}| \leq \epsilon) \geq 1 - \delta$. To complete the proof, it is necessary to lower bound m'_U :

$$m'_U \geq \frac{\epsilon}{2\sqrt{2}} \sqrt{\exp[-M_0(|U\rangle)]}, \quad (\text{C23})$$

which follows from Eq. (C10). This concludes the proof.

3. Proof of Corollary 5

In this section, we prove Corollary 5. Let us start with the lower bound of the number of resources needed for a doped Clifford circuit C_t —with associated Choi state $|C_t\rangle$ —to be certified. From Theorem 4 we have

$$N_{C_t} \geq \frac{2}{\epsilon^2} \ln(2/\delta) \exp[M_2(|C_t\rangle)]. \quad (\text{C24})$$

To proceed we look at the average behavior of $\exp[M_2(|C_t\rangle)]$:

$$\langle (\exp[M_2(|C_t\rangle)]) \rangle_{C_t} = \left\langle \left(\frac{d^6}{\sum_{P_1, P_2} \text{tr}^4(P_1 U P_2 U^{\dagger})} \right) \right\rangle_{C_t} \geq \frac{d^2}{\langle [\text{tr}(QU^{\otimes 4}QU^{\dagger \otimes 4})] \rangle_{C_t}}, \quad (\text{C25})$$

where $Q := \frac{1}{d^2} \sum_{P \in \mathcal{P}_n} P^{\otimes 4}$, and we used the Jensen inequality to bound the average of $\langle (\exp[M_2(|C_t\rangle)]) \rangle_{C_t}$. To compute the average over doped Clifford circuits we use the techniques introduced in [94, 116] and obtain

$$\langle [\text{tr}(QU^{\otimes 4}QU^{\dagger \otimes 4})] \rangle_{C_t} = \left[\frac{4(6 - d^2 + d^4)}{d^2(d^2 - 9)} + (d^2 - 1) \left(\frac{(d+2)(d+4)f_+^t}{6d(d+3)} + \frac{(d-2)(d-4)f_-^t}{6d(d-3)} + \frac{(d^2-4)\left(\frac{f_++f_-}{2}\right)^t}{3d^2} \right) \right]^{-1}, \quad (\text{C26})$$

where $f_{\pm} = \frac{3d^2 \mp 3d - 4}{4(d^2 - 1)}$. One easily shows that $\langle [\text{tr}(QU^{\otimes 4}QU^{\dagger \otimes 4})] \rangle_{C_t} = \Theta(\exp[t \log_2 4/3])$, and thus the number of resources is lower bounded by

$$N_{C_t} \geq \Theta(\exp[t \log_2 4/3]). \quad (\text{C27})$$

To prove the upper bound to the number of resources we use the upper bound in Theorem 4:

$$N_{C_t} \leq \frac{64}{\epsilon^4} \ln(2/\delta) \exp[v(U)]. \quad (\text{C28})$$

As proven in [96] the unitary stabilizer nullity can be upper bounded with the T -count $t(U)$, which corresponds to the minimum number of T gates required to implement the unitary U .

Equation (C28) can be upper bounded via the T count as

$$N_{C_t} \leq \frac{64}{\epsilon^4} \ln(2/\delta) \exp[v(U)] \leq \frac{64}{\epsilon^4} \ln(2/\delta) \exp[t] \simeq \Theta(\exp[t]), \quad (\text{C29})$$

where we used that for doped Clifford circuits $t(U) = t$. This concludes the proof.

APPENDIX D: SHADOW FIDELITY ESTIMATION

Let $N_{\tilde{\rho}}$ be the number of physical preparation of ρ . Let $N_{\tilde{\psi}} = k \times l$, where k is the number of Clifford circuits drawn uniformly at random from the Clifford group and l is the number of realizations of the experiment. For a single experiment,

we have

$$\mathcal{F}_s = \frac{1}{k} \sum_{C_i \in \mathbb{C}_s} [(d+1) \langle \bar{x}_i | C_i^\dagger \rho C_i | \bar{x}_i \rangle - 1]. \quad (\text{D1})$$

Defining $\bar{\mathcal{F}} = \text{median}\{\mathcal{F}_s | s = 1, \dots, l\}$, we already know that [60]

$$\Pr[|\mathcal{F}(\rho, \tilde{\rho}) - \bar{\mathcal{F}}| \leq \epsilon] \geq 1 - \delta \quad (\text{D2})$$

for $N_{\tilde{\rho}} \geq \frac{160}{\epsilon^2} \ln \delta^{-1}$ and $k = 8 \ln 8 \delta^{-1}$. Now, let $\rho_{\bar{x}_i}$ be the classical estimation of the outcome probability $\langle \bar{x}_i | C_i^\dagger \rho C_i | \bar{x}_i \rangle$.

Let N_{cl} be the classical resources necessary for ensuring

$$\Pr[|\rho_{\bar{x}_i} - \langle \bar{x}_i | C_i^\dagger \rho C_i | \bar{x}_i \rangle| \leq \epsilon] \geq 1 - \delta. \quad (\text{D3})$$

Then, defining

$$\tilde{\mathcal{F}}_s = \frac{1}{k} \sum_{C_i \in \mathbb{C}_s} [(d+1) \rho_{\bar{x}_i} - 1], \quad (\text{D4})$$

one has

$$\Pr[|\tilde{\mathcal{F}}_s - \mathcal{F}_s| \leq (d+1)\epsilon] \geq 1 - \delta. \quad (\text{D5})$$

-
- [1] R. D. Somma, S. Boixo, H. Barnum, and E. Knill, Quantum Simulations of Classical Annealing Processes, *Phys. Rev. Lett.* **101**, 130504 (2008).
 - [2] H. J. Kimble, The quantum internet, *Nature (London)* **453**, 1023 (2008).
 - [3] J. I. Cirac and P. Zoller, Goals and opportunities in quantum simulation, *Nat. Phys.* **8**, 264 (2012).
 - [4] S. Bravyi, D. Gosset, and R. König, Quantum advantage with shallow circuits, *Science* **362**, 308 (2018).
 - [5] A. Acín *et al.*, The quantum technologies roadmap: A European community view, *New J. Phys.* **20**, 080201 (2018).
 - [6] F. Arute *et al.*, Quantum supremacy using a programmable superconducting processor, *Nature (London)* **574**, 505 (2019).
 - [7] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, Quantum Fingerprinting, *Phys. Rev. Lett.* **87**, 167902 (2001).
 - [8] D. Gottesman and I. Chuang, Quantum digital signatures, [arXiv:quant-ph/0105032](https://arxiv.org/abs/quant-ph/0105032).
 - [9] A. Gilyén and A. Poremba, Improved quantum algorithms for fidelity estimation, [arXiv:2203.15993](https://arxiv.org/abs/2203.15993).
 - [10] L. Cincio *et al.*, Learning the quantum algorithm for state overlap, *New J. Phys.* **20**, 113022 (2018).
 - [11] E. Knill *et al.*, Randomized benchmarking of quantum gates, *Phys. Rev. A* **77**, 012307 (2008).
 - [12] E. Magesan, J. M. Gambetta, and J. Emerson, Scalable and Robust Randomized Benchmarking of Quantum Processes, *Phys. Rev. Lett.* **106**, 180504 (2011).
 - [13] J. M. Gambetta *et al.*, Characterization of Addressability by Simultaneous Randomized Benchmarking, *Phys. Rev. Lett.* **109**, 240504 (2012).
 - [14] E. Magesan, J. M. Gambetta, and J. Emerson, Characterizing quantum gates via randomized benchmarking, *Phys. Rev. A* **85**, 042311 (2012).
 - [15] S. Kimmel, M. P. da Silva, C. A. Ryan, B. R. Johnson, and T. Ohki, Robust Extraction of Tomographic Information via Randomized Benchmarking, *Phys. Rev. X* **4**, 011050 (2014).
 - [16] J. J. Wallman and S. T. Flammia, Randomized benchmarking with confidence, *New J. Phys.* **16**, 103032 (2014).
 - [17] R. Kueng, D. M. Long, A. C. Doherty, and S. T. Flammia, Comparing Experiments to the Fault-Tolerance Threshold, *Phys. Rev. Lett.* **117**, 170502 (2016).
 - [18] I. Roth, R. Kueng *et al.*, Recovering Quantum Gates from Few Average Gate Fidelities, *Phys. Rev. Lett.* **121**, 170502 (2018).
 - [19] J. J. Wallman, Randomized benchmarking with gate-dependent noise, *Quantum* **2**, 47 (2018).
 - [20] A. Erhard *et al.*, Characterizing large-scale quantum computers via cycle benchmarking, *Nat. Commun.* **10**, 5347 (2019).
 - [21] E. Onorati, A. H. Werner, and J. Eisert, Randomized Benchmarking for Individual Quantum Gates, *Phys. Rev. Lett.* **123**, 060501 (2019).
 - [22] J. Helsen *et al.*, A new class of efficient randomized benchmarking protocols, *npj Quantum Inf.* **5**, 71 (2019).
 - [23] J. Helsen, J. J. Wallman *et al.*, Multiqubit randomized benchmarking using few samples, *Phys. Rev. A* **100**, 032304 (2019).
 - [24] D. S. Phillips, M. Walschaers *et al.*, Benchmarking of Gaussian boson sampling using two-point correlators, *Phys. Rev. A* **99**, 023836 (2019).
 - [25] S. Aaronson, The learnability of quantum states, *Proc. R. Soc. A* **463**, 3089 (2007).
 - [26] M. Cramer *et al.*, Efficient quantum state tomography, *Nat. Commun.* **1**, 149 (2010).
 - [27] A. Mari, K. Kieling *et al.*, Directly Estimating Nonclassicality, *Phys. Rev. Lett.* **106**, 010403 (2011).
 - [28] D. Gross, Y.-K. Liu *et al.*, Quantum State Tomography via Compressed Sensing, *Phys. Rev. Lett.* **105**, 150401 (2010).
 - [29] S. T. Flammia and Y.-K. Liu, Direct Fidelity Estimation from Few Pauli Measurements, *Phys. Rev. Lett.* **106**, 230501 (2011).
 - [30] M. P. da Silva, O. Landon-Cardinal, and D. Poulin, Practical Characterization of Quantum Devices without Tomography, *Phys. Rev. Lett.* **107**, 210404 (2011).
 - [31] M. Guta, J. Kahn, R. Kueng, and J. A. Tropp, Fast state tomography with optimal error bounds, [arXiv:1809.11162](https://arxiv.org/abs/1809.11162).
 - [32] S. Aaronson, Shadow tomography of quantum states, in *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing* (ACM Press, New York, 2018), pp. 325–338.
 - [33] Y. Takeuchi and T. Morimae, Verification of Many-Qubit States, *Phys. Rev. X* **8**, 021060 (2018).
 - [34] D. Markham and A. Krause, A simple protocol for certifying graph states and applications in quantum networks, *Cryptography* **4**, 3 (2020).
 - [35] S. Pallister, N. Linden, and A. Montanaro, Optimal Verification of Entangled States with Local Measurements, *Phys. Rev. Lett.* **120**, 170502 (2018).
 - [36] Y. Takeuchi *et al.*, Resource-efficient verification of quantum computing using Serfling's bound, *npj Quantum Inf.* **5**, 27 (2019).
 - [37] A. Elben *et al.*, Cross-Platform Verification of Intermediate Scale Quantum Devices, *Phys. Rev. Lett.* **124**, 010504 (2020).

- [38] H.-Y. Huang, R. Kueng, and J. Preskill, Predicting many properties of a quantum system from very few measurements, *Nat. Phys.* **16**, 1050 (2020).
- [39] H.-Y. Huang *et al.*, Provably efficient machine learning for quantum many-body problems, *Science* **377**, eabk3333 (2022).
- [40] M. Holzäpfel, T. Baumgratz *et al.*, Scalable reconstruction of unitary processes and Hamiltonians, *Phys. Rev. A* **91**, 042129 (2015).
- [41] P. Sekatski, J.-D. Bancal *et al.*, Certifying the Building Blocks of Quantum Computers from Bell's Theorem, *Phys. Rev. Lett.* **121**, 180505 (2018).
- [42] A. Bouland *et al.*, On the complexity and verification of quantum random circuit sampling, *Nat. Phys.* **15**, 159 (2019).
- [43] Y.-C. Liu, J. Shang *et al.*, Efficient verification of quantum processes, *Phys. Rev. A* **101**, 042315 (2020).
- [44] H. Zhu and H. Zhang, Efficient verification of quantum gates with local operations, *Phys. Rev. A* **101**, 042316 (2020).
- [45] C. Dankert, R. Cleve *et al.*, Exact and approximate unitary 2-designs and their application to fidelity estimation, *Phys. Rev. A* **80**, 012304 (2009).
- [46] S. T. Flammia and J. J. Wallman, Efficient Estimation of Pauli Channels, *ACM Trans. Quantum Comput.* **1**, 1 (2020).
- [47] R. Harper, S. T. Flammia, and J. J. Wallman, Efficient learning of quantum noise, *Nat. Phys.* **16**, 1184 (2020).
- [48] M. Kliesch *et al.*, Guaranteed recovery of quantum processes from few measurements, *Quantum* **3**, 171 (2019).
- [49] A. K. Hashagen *et al.*, Real Randomized Benchmarking, *Quantum* **2**, 85 (2018).
- [50] B. W. Reichardt, F. Unger, and U. Vazirani, Classical command of quantum systems, *Nature (London)* **496**, 456 (2013).
- [51] D. Mills, A. Pappa, T. Kapourniotis, and E. Kashefi, Information theoretically secure hypothesis test for temporally unstructured quantum computation, *arXiv:1704.01998*.
- [52] J. F. Fitzsimons, Private quantum computation: An introduction to blind quantum computing and related protocols, *npj Quantum Inf.* **3**, 23 (2017).
- [53] J. F. Fitzsimons and E. Kashefi, Unconditionally verifiable blind quantum computation, *Phys. Rev. A* **96**, 012303 (2017).
- [54] A. Coladangelo *et al.*, Verifier-on-a-leash: New schemes for verifiable delegated quantum computation, with quasilinear resources, in *Advances in Cryptology—EUROCRYPT 2019*, edited by Y. Ishai and V. Rijmen, Lecture Notes in Computer Science (Springer International Publishing, Cham, 2019), pp. 247–277.
- [55] U. Mahadev, Classical verification of quantum computations, in *Proceedings of the 2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE, New York, 2018), pp. 259–267.
- [56] A. Gheorghiu and T. Vidick, Computationally-secure and composable remote state preparation, in *Proceedings of the 2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE, New York, 2019), pp. 1024–1033.
- [57] I. Šupić and J. Bowles, Self-testing of quantum systems: A review, *Quantum* **4**, 337 (2020).
- [58] S. Aaronson and L. Chen, Complexity-theoretic foundations of quantum supremacy experiments, in *Proceedings of the 32nd Computational Complexity Conference (CCC 2017)*, edited by R. O'Donnell (Schloss Dagstuhl—Leibniz-Zentrum fuer Informatik, Wadern, 2017), Vol. 79, pp. 22:1–22:67.
- [59] C. Neill *et al.*, A blueprint for demonstrating quantum supremacy with superconducting qubits, *Science* **360**, 195 (2018).
- [60] M. Kliesch and I. Roth, Theory of quantum system certification, *PRX Quantum* **2**, 010201 (2021).
- [61] J. Eisert *et al.*, Quantum certification and benchmarking, *Nat. Rev. Phys.* **2**, 382 (2020).
- [62] A. Gheorghiu, T. Kapourniotis, and E. Kashefi, Verification of quantum computation: An overview of existing approaches, *Theory Comput. Syst.* **63**, 715 (2019).
- [63] A. Elben *et al.*, The randomized measurement toolbox, *Nat. Rev. Phys.* **5**, 9 (2023).
- [64] D. Hangleiter and J. Eisert, Computational advantage of quantum random sampling, *arXiv:2206.04079*.
- [65] B. Schumacher, Sending entanglement through noisy quantum channels, *Phys. Rev. A* **54**, 2614 (1996).
- [66] M. A. Nielsen, A simple formula for the average gate fidelity of a quantum dynamical operation, *Phys. Lett. A* **303**, 249 (2002).
- [67] A. Carignan-Dugas, J. J. Wallman, and J. Emerson, Bounding the average gate fidelity of composite channels using the unitarity, *New J. Phys.* **21**, 053016 (2019).
- [68] L. Leone, S. F. E. Oliviero, and A. Hamma, Stabilizer Rényi Entropy, *Phys. Rev. Lett.* **128**, 050402 (2022).
- [69] E. T. Campbell and D. E. Browne, Bound States for Magic State Distillation in Fault-Tolerant Quantum Computation, *Phys. Rev. Lett.* **104**, 030503 (2010).
- [70] E. T. Campbell, Catalysis and activation of magic states in fault-tolerant architectures, *Phys. Rev. A* **83**, 032317 (2011).
- [71] V. Veitch *et al.*, The resource theory of stabilizer quantum computation, *New J. Phys.* **16**, 013009 (2014).
- [72] M. Howard and E. Campbell, Application of a Resource Theory for Magic States to Fault-Tolerant Quantum Computing, *Phys. Rev. Lett.* **118**, 090501 (2017).
- [73] M. Ahmadi, H. B. Dang *et al.*, Quantification and manipulation of magic states, *Phys. Rev. A* **97**, 062332 (2018).
- [74] X. Wang, M. M. Wilde, and Y. Su, Quantifying the magic of quantum channels, *New J. Phys.* **21**, 103002 (2019).
- [75] J. R. Seddon and E. T. Campbell, Quantifying magic for multi-qubit operations, *Proc. R. Soc. A* **475**, 20190251 (2019).
- [76] J. R. Seddon, B. Regula *et al.*, Quantifying quantum speedups: Improved classical simulation from tighter magic monotones, *PRX Quantum* **2**, 010345 (2021).
- [77] C. D. White, C. Cao, and B. Swingle, Conformal field theories are magical, *Phys. Rev. B* **103**, 075145 (2021).
- [78] H. Qassim, H. Pashayan, and D. Gosset, Improved upper bounds on the stabilizer rank of magic states, *Quantum* **5**, 606 (2021).
- [79] O. Hahn, A. Ferraro *et al.*, Quantifying Qubit Magic Resource with Gottesman-Kitaev-Preskill Encoding, *Phys. Rev. Lett.* **128**, 210502 (2022).
- [80] S. F. E. Oliviero *et al.*, Measuring magic on a quantum processor, *npj Quantum Inf.* **8**, 148 (2022).
- [81] T. Haug and M. Kim, Scalable measures of magic resource for quantum computers, *PRX Quantum* **4**, 010301 (2023).
- [82] P. W. Shor, Fault-tolerant quantum computation, in *Proceedings of the 37th Conference on Foundations of Computer Science* (IEEE, New York, 1996), pp. 56–65.

- [83] D. Gottesman, Theory of fault-tolerant quantum computation, *Phys. Rev. A* **57**, 127 (1998).
- [84] A. Y. Kitaev, Fault-tolerant quantum computation by anyons, *Ann. Phys. (NY)* **303**, 2 (2003).
- [85] E. T. Campbell, B. M. Terhal, and C. Vuillot, Roads towards fault-tolerant universal quantum computation, *Nature (London)* **549**, 172 (2017).
- [86] D. Gottesman, The Heisenberg representation of quantum computers, talk at, in *International Conference on Group Theoretic Methods in Physics* (Springer, Berlin, 1998).
- [87] S. Aaronson and D. Gottesman, Improved simulation of stabilizer circuits, *Phys. Rev. A* **70**, 052328 (2004).
- [88] S. Bravyi and J. Haah, Magic-state distillation with low overhead, *Phys. Rev. A* **86**, 052329 (2012).
- [89] S. Bravyi and D. Gosset, Improved Classical Simulation of Quantum Circuits Dominated by Clifford Gates, *Phys. Rev. Lett.* **116**, 250501 (2016).
- [90] S. Bravyi, G. Smith, and J. A. Smolin, Trading Classical and Quantum Computational Resources, *Phys. Rev. X* **6**, 021043 (2016).
- [91] S. Bravyi *et al.*, Simulation of quantum circuits by low-rank stabilizer decompositions, *Quantum* **3**, 181 (2019).
- [92] S. F. E. Oliviero *et al.*, Random matrix theory of the isospectral twirling, *SciPost Phys.* **10**, 76 (2021).
- [93] L. Leone, S. F. E. Oliviero, and A. Hamma, Isospectral twirling and quantum chaos, *Entropy* **23**, 1073 (2021).
- [94] L. Leone *et al.*, Quantum chaos is quantum, *Quantum* **5**, 453 (2021).
- [95] M. Beverland and E. Campbell, *et al.*, Lower bounds on the non-Clifford resources for quantum computations, *Quantum Sci. Technol.* **5**, 035009 (2020).
- [96] J. Jiang and X. Wang, Lower bound the T-count via unitary stabilizer nullity, [arXiv:2103.09999](https://arxiv.org/abs/2103.09999).
- [97] L. Kocia and G. Tulloch, More optimal simulation of universal quantum computers, [arXiv:2202.01233](https://arxiv.org/abs/2202.01233).
- [98] A. Kissinger, J. van de Wetering, and R. Vilmart, Classical simulation of quantum circuits with partial and graphical stabiliser decompositions, in *Proceedings of the 17th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2022)*, edited by F. Le Gall and T. Morimae, Leibniz International Proceedings in Informatics (LIPIcs) Vol. 232 (Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 2022), pp. 5:1–5:13.
- [99] A. Kissinger and J. van de Wetering, Simulating quantum circuits with ZX-calculus reduced stabiliser decompositions, *Quantum Sci. Technol.* **7**, 044001 (2022).
- [100] B. P. Lanyon *et al.*, Efficient tomography of a quantum many-body system, *Nat. Phys.* **13**, 1158 (2017).
- [101] A. Fedorov *et al.*, Implementation of a Toffoli gate with superconducting circuits, *Nature (London)* **481**, 170 (2012).
- [102] R. O'Donnell and J. Wright, Efficient quantum tomography, in *Proceedings of the Forty-Eighth Annual ACM Symposium on Theory of Computing* (ACM Press, New York, 2016), pp. 899–912.
- [103] T. Morimae, Y. Takeuchi, and M. Hayashi, Verification of hypergraph states, *Phys. Rev. A* **96**, 062321 (2017).
- [104] H. Zhu and M. Hayashi, Efficient Verification of Hypergraph States, *Phys. Rev. Appl.* **12**, 054047 (2019).
- [105] N. Dangniam, Y.-G. Han, and H. Zhu, Optimal verification of stabilizer states, *Phys. Rev. Res.* **2**, 043323 (2020).
- [106] Y. Zhou and A. Hamma, Entanglement of random hypergraph states, *Phys. Rev. A* **106**, 012410 (2022).
- [107] Z. Li, Y.-G. Han, and H. Zhu, Efficient verification of bipartite pure states, *Phys. Rev. A* **100**, 032316 (2019).
- [108] H. Zhu and M. Hayashi, Efficient Verification of Pure Quantum States in the Adversarial Scenario, *Phys. Rev. Lett.* **123**, 260504 (2019).
- [109] Y.-C. Liu, X.-D. Yu *et al.*, Efficient Verification of Dicke States, *Phys. Rev. Appl.* **12**, 044020 (2019).
- [110] Z. Li, Y.-G. Han *et al.*, Verification of phased Dicke states, *Phys. Rev. A* **103**, 022601 (2021).
- [111] L. E. Heyfron and E. T. Campbell, An efficient quantum compiler that reduces T count, *Quantum Sci. Technol.* **4**, 015004 (2018).
- [112] D. M. Reich, G. Gualdi, and C. P. Koch, Optimal Strategies for Estimating the Average Fidelity of Quantum Gates, *Phys. Rev. Lett.* **111**, 200401 (2013).
- [113] J. Haferkamp, F. Montealegre-Mora, M. Heinrich, J. Eisert, D. Gross, and I. Roth, Efficient unitary designs with a system-size independent number of non-Clifford gates, *Commun. Math. Phys.* **397**, 995 (2023).
- [114] D. Gross, S. T. Flammia, and J. Eisert, Most Quantum States Are Too Entangled To Be Useful As Computational Resources, *Phys. Rev. Lett.* **102**, 190501 (2009).
- [115] W. Hoeffding, Probability inequalities for sums of bounded random variables, *J. Am. Stat. Assoc.* **58**, 13 (1963).
- [116] S. F. E. Oliviero, L. Leone, and A. Hamma, Transitions in entanglement complexity in random quantum circuits by measurements, *Phys. Lett. A* **418**, 127721 (2021).
- [117] D. N. Page, Average Entropy of a Subsystem, *Phys. Rev. Lett.* **71**, 1291 (1993).