Magic hinders quantum certification

Lorenzo Leone,1,* Salvatore F.E. Oliviero,1 and Alioscia Hamma1
1Physics Department, University of Massachusetts Boston, 02125, USA

We show how the resource theory of magic quantifies the hardness of quantum certification protocols. In particular, the resources needed for a direct fidelity estimation grow exponentially with the stabilizer Rényi entropy[1]: the more the magic, the harder the certification. Remarkably, the verification turns out to be polynomially feasible only for those states which are shown to be useless to attain any quantum advantage. We then extend our results to quantum evolutions, showing that the resources needed to certify the quality of the application of a given unitary $U$ are governed by the magic in the Choi state associated with $U$, which is shown to possess a profound connection with out-of-time order correlators.

Introduction.— Quantum computers promise efficient solutions to problems which are otherwise intractable on classical computers[2–7]. 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[8–10]. Until reliable quantum technology can be realized, we must use classical resources to implement methods of quantum certification. In the last decade, there have been many attempts in tackling this problem, with a large landscape of different protocols, ranging from benchmarking[11–25], quantum state[26–41] and process[42–50] learning, to blind computation[51–58] and quantum supremacy[59–61]. For a panoramic overview of the approaches within the field of quantum certification see, e.g.[62–65].

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 by the apparatus; instead, the quality of quantum gates $U$ is commonly expressed in terms of average gate fidelity[18, 66–68].

The bottleneck of any quantum certification protocol is its efficiency in terms of the resources employed. These are conventionally quantified by the sample complexity[62, 63], i.e. the minimal number of experiments and resulting samples that need to be prepared for a protocol to be successful. In particular, a protocol is said to be efficient if its sample complexity scales polynomially in the number of qubits $n$; conversely, a protocol is inefficient if its sample complexity scales exponentially in $n$.

In this letter, we show that the sample complexity of a direct fidelity estimation protocol, conducted via Monte Carlo sampling, is exactly quantified by the amount of magic in the state. Magic is an expensive, but fundamental fuel for quantum computation[69–78]: without magic, a quantum computer can do nothing more than a classical computer. While simulations of stabilizer states (free resources) and Clifford circuits (free operations) are efficient on classical computers, the injection of $t$ non-Clifford gates makes the simulation exponentially harder in $t$, in fact unlocking quantum advantage. Resource theory of magic has been widely studied and found copious applications in the broad field of fault-tolerant quantum computation[79–85], as well as classical algorithms for simulations of quantum computing architectures[86–92]. Moreover, the interplay between magic and entanglement is at the root of the onset of entanglement complexity and quantum chaos[93–99].

We prove that sample complexity for state certification scales exponentially with magic, and thus exponentially in the number of non-Clifford gates needed for the state preparation: the certification protocol is efficient as long as the amount of non-Clifford gates used is $O(\log n)$. Remarkably, this is the same threshold for a quantum state to be efficiently simulated classically[89]. As a consequence, the quantum computation able to unlock a quantum speedup is the one for which the certification by classical means is not feasible. In other words, the same complexity that makes quantum technology powerful is the one that inhibits its certification.

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 multi-points 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[97, 100–102], 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 is the evolution[100] and the more inefficient is the quantum verification. Quantum chaos is quantum – it requires an extensive quantity $O(n)$ of non-Clifford resources – and therefore it hinders quantum certification. In what follows, we first introduce the resource theory of stabilizer Rényi entropy with its connection to unitary evolutions, and then we turn to show its deep connection to quantum fidelity estimation protocols.

**Stabilizer Rényi entropy of Choi states.** — The stabilizer Rényi entropy $M_{\alpha}$ introduced in[1] is a magic monotone that is particularly useful both computationally and experimentally measurable[103]. We now briefly review the definition and some useful properties of $M_{\alpha}$ and use it to characterize unitary operations $U$ through the Choi-Jamiołkowski isomorphism, establishing a non-trivial connection with OTOCs.

Consider the Pauli group on $n$ qubits $\mathbb{P}(n)$ with elements $P$. Any state $\rho$ in the $d = 2^n$-dimensional Hilbert space can be decomposed in the Pauli basis as $\rho = d^{-1} \sum_{P \in \mathbb{P}} \text{tr}(P \rho) P$. Define the purity functional $Pur(x) \equiv \text{tr} x^2$, and a probability distribution over the coefficients of such expansion by $\Xi_{\rho} := \{\text{Pur}^{-1}(\rho)d^{-1} \text{tr}^2(P\rho)\}_P$. Note that $\Xi_{\rho}(P) \geq 0$ and sum to one. The $\alpha$-Stabilizer Rényi entropy is defined as[1]:

$$M_{\alpha}(\rho) := S_{\alpha}(\Xi_{\rho}) + S_2(\rho) - \log d$$  \hspace{1cm} (1)

where $S_{\alpha}(\Xi_{\rho}) := (1 - \alpha)^{-1} \log \sum_{P} \Xi_{\alpha}^0(P)$ is the $\alpha$-Rényi entropy of the probability distribution $\Xi_{\rho}$, and $S_2(\rho) := - \log \text{Pur}(\rho)$ is the 2-Rényi entropy of $\rho$. $M_{\alpha}(\rho)$ 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 $\rho = d^{-1} \sum_{P \in G} \phi_P P$, where $G \subseteq \mathbb{P}(n)$ is a commuting subset of $\mathbb{P}(n)$ and $\phi_P = \pm 1$; (iii) 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 $M_{\alpha}(|\psi\rangle \langle \psi|) \leq \log d$. We denote the stabilizer Rényi entropy for a pure state $|\psi\rangle$ as $M_{\alpha}(|\psi\rangle)$; for pure states only, we have that $M_{\alpha}(|\psi\rangle) \leq \nu(|\psi\rangle)$[1], where $\nu(|\psi\rangle)$ is the stabilizer nullity[104] of $\psi$, defined as $\nu(|\psi\rangle) = \log d - \log s(|\psi\rangle)$ where $s(|\psi\rangle) := \{|P : \text{tr}(P |\psi\rangle \langle \psi|) = 1\}|$.

We can naturally associate a stabilizer Rényi entropy to unitary operators $U$ through the Choi state $|U\rangle := (\mathbb{I} \otimes U)|I\rangle$, where $|I\rangle := d^{-1/2} \sum_i |i\rangle \otimes |i\rangle$. Let $\Xi_U$ be the probability distribution whose elements are $\Xi_U(P, P') := d^{-2} \text{tr}^2(P U P' U^\dagger)$ for $P, P' \in \mathbb{P}(n)$. Note that $d^2 \Xi_U(P, P')$ is a double stochastic matrix, i.e. $d^2 \sum_P \Xi_U(P, P') = d^2 \sum_P \Xi_U(P, P') = 1$. The following lemma holds:

**Lemma 1.** The stabilizer Rényi entropy for $|U\rangle$ reads[105]:

$$M_{\alpha}(|U\rangle) = S_{\alpha}(\Xi_U) - 2 \log d$$ \hspace{1cm} (2)

Now we are ready to state one of the main results of the paper, which builds a tight connection between the magic of the Choi state $|U\rangle$ and OTOCs[105]:

**Lemma 2.** The $\alpha$-stabilizer Rényi entropy of $|U\rangle$, for $\alpha > 1$, equals the 4α-points out-of-time order correlator

$$M_{\alpha}(|U\rangle) = \frac{1}{1 - \alpha} \log \text{OTOCT}_{4\alpha}(U)$$ \hspace{1cm} (3)

where $\text{OTOCT}_{2\alpha} := d^{-2} \sum_{P, P'} \text{otoct}_{2\alpha}(P, P')$, and $d \times \text{otoct}_{4\alpha}(P, P') := \text{tr}(P_0 \prod_{i=1}^n P(U P_{2i-1} P_{2i} P_{2i+1}))$ with $P_0 \equiv \mathbb{I}$, $\langle \rangle$ the average over $P_1, \ldots, P_{4\alpha}$ and $P(U) \equiv UP U^\dagger$.

The above lemma gives the meaning to the magic of the Choi state $|U\rangle$ associated to a unitary evolution $U$: the more the magic $M_{\alpha}(|U\rangle)$, the more chaotic is the evolution[100]. Lastly, we show a bound on a new magic monotone defined on unitary operators, useful in proving the main results of the paper. Let $\nu(U)$ be the unitary stabilizer nullity defined in[106] as $\nu(U) := 2 \log d - \log s(U)$, 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

$$M_{\alpha}(|U\rangle) \leq \nu(U)$$ \hspace{1cm} (4)

The lemma easily follows from Lemma 1 and the bound proven in[1], i.e. $M_{\alpha}(|\psi\rangle) \leq \nu(|\psi\rangle)$ for any $\alpha$. 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. $\nu(U) = \nu(U)$. Now we are ready to present the main results of the paper, showing that the efficiency of direct fidelity estimation protocols is governed by the stabilizer Rényi entropy.

**Magic and quantum certification.** — In this section, we show that the stabilizer Rényi entropy quantify the number of resources required for quantum
We quantify the resources needed for the estimation of measurable numbers \( X \) of pure states \( \tilde{\psi} \) and \( \psi \), i.e., \( \mathcal{F}(\tilde{\psi}, \psi) := \text{tr}(\tilde{\psi} \psi) \) where \( \psi := |\psi \rangle \langle \psi| \). One can rewrite above equation in the Pauli basis \( \mathcal{P}(n) \) as \( \mathcal{F}(\tilde{\psi}, \psi) = d^{-1} \sum_{P} \text{tr}(P \tilde{\psi}) \text{tr}(P \psi) \), where \( \Xi_{\psi} := \{ \Xi_{\psi}(P) \equiv d^{-1} \text{tr}^{2}(P \psi) | P \in \mathcal{P}(n) \} \) is the probability distribution introduced above for \( \psi \) being a pure state. We can then write the fidelity as an expectation value over \( \Xi_{\psi} \), that is, \( \mathcal{F}(\tilde{\psi}, \psi) = \sum_{P} X_{P} \Xi_{\psi}(P) \equiv \langle X_{P} \rangle_{\Xi_{\psi}} \); i.e., the fidelity between the theoretical pure state \( \psi \) and the prepared state \( \tilde{\psi} \) can be recast as an average of measurable numbers \( X_{P} \) on the probability distribution \( \Xi_{\psi} \). Following[30, 62], we use the following protocol to estimate the average \( \langle X_{P} \rangle_{\Xi_{\psi}} \): (i) extract \( k \) Pauli operators \( P_{1}, \ldots, P_{k} \in \mathbb{K} \) according to the state-dependent probability distribution \( \Xi_{\psi} \); (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 \( \mathcal{F}(\tilde{\psi}, \psi) \) given by \( \hat{\mathcal{F}} = k^{-1} \sum_{P \in \mathbb{K}} \hat{X}_{P} \) where \( \hat{X}_{P} = \text{tr}^{-1}(P \tilde{\psi}) c_{P}(\tilde{\psi})^{-1} \sum_{j=1}^{c_{P}(\tilde{\psi})} P_{P_{j}}(\tilde{\psi}) \) and \( P_{P_{j}}(\tilde{\psi}) \) 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 \( \epsilon \) and failure probability \( \delta \) – as the number of copies of \( \tilde{\psi} \) to be prepared on the apparatus:

\[
N_{\tilde{\psi}} := \sum_{P \in \mathbb{K}} c_{P}(\tilde{\psi})
\]  
(5)

Surprisingly, the total resources \( N_{\tilde{\psi}} \) are exactly quantified by the magic of \( |\tilde{\psi} \rangle \), measured via the stabilizer Rényi entropy \( M_{n}(|\tilde{\psi} \rangle) \) as the next theorem states[105].

**Theorem 1.** The number of resources \( N_{\tilde{\psi}} \) needed to measure the fidelity \( \mathcal{F} \) with accuracy \( \epsilon \) and success probability \( 1 - \delta \) is bounded:

\[
\frac{2}{\epsilon^{2}} \ln \frac{2}{\delta} \exp[M_{2}(|\psi \rangle)] \leq N_{\tilde{\psi}} \leq \frac{64}{\delta} \ln \frac{2}{\delta} \exp[M_{0}(|\psi \rangle)]
\]  
(6)

where \( M_{2}(|\psi \rangle) \) and \( M_{0}(|\psi \rangle) \) are the 2 and the 0 stabilizer Rényi entropy respectively.

The above theorem tells us that the more magic a state contains, the harder the verification through a direct fidelity estimation protocol is. As an example, consider the \( t \)-doped stabilizer states \( |\psi_t \rangle \) defined as the output of a circuit composed by Clifford gates doped with a finite amount \( t \) of non-Clifford resources. The best classical algorithm able to simulate general such states scales as \( O(\text{poly}(n) \exp[\epsilon]) \)[89], providing an insightful threshold for the onset of quantum advantage: as long as \( t = O(\log n) \), 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 \( \psi_t \) grows exponentially in \( t \):

\[
\Omega(\exp[t \log 4/3]) \leq \langle N_{\psi_t} \rangle \leq \Omega(\exp[t]) \leq \Omega(d)
\]  
(7)

Two comments are in order here: first, the hardness of the verification of \( t \)-doped stabilizer states quickly saturates the bound, growing exponentially in \( t \), and, second, for this reason the certification protocol is only efficient for those states - with \( t = O(\log n) \) - that are useless for quantum computation.

Let us now extend the above results to mixed states. Suppose one aims to prepare a mixed state \( \rho \) on a quantum processor and be \( \tilde{\rho} \) the actual prepared state. One way to check whether the preparation is faithful is to evaluate the difference in 2-norm between \( \rho \) and \( \tilde{\rho} \)[109]:

\[
\| \rho - \tilde{\rho} \|_{2} = \sqrt{\text{Pur}(\rho) \left[ 1 + \frac{\text{Pur}(\tilde{\rho})}{\text{Pur}(\rho)} - 2\Phi(\rho, \tilde{\rho}) \right]}
\]  
(8)

where we defined \( \Phi(\rho, \tilde{\rho}) := \frac{\text{tr}(\rho \tilde{\rho})}{\text{Pur}(\rho)} \) as the overlap between \( \rho \) 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 \( \rho \) 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[8, 110].
can estimate the above average by an importance sampling\cite{111,112} of the probability distribution \( \Xi_\mu \), and construct an unbiased estimator \( \tilde{F}(\rho, \tilde{\rho}) = k^{-1} \sum_{P \in \mathcal{P}} \text{tr}^{-1}(P) P^{-1}(\rho) \sum_{j=1}^{c_P(\rho)} \mathcal{P}_j(\tilde{\rho}) \), where \( c_P(\rho) \) are the number of copies of \( \rho \) needed to estimate \( \text{tr}(P\rho) \), and \( \mathcal{P}_j(\tilde{\rho}) \) is the 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. \( N_\tilde{\rho} = \sum_{P \in \mathcal{P}} c_P(\rho) \). We are now ready to bound \( N_\tilde{\rho} \) in terms of the stabilizer Rényi entropy for mixed states, in a similar fashion of Theorem 1:

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

\[
\frac{2}{\epsilon^2} \ln \frac{2}{\delta} \exp[\mathcal{M}_2(\rho)] \leq N_\tilde{\rho} \leq \frac{64}{\epsilon^2} \ln \frac{2}{\delta} \exp[\mathcal{M}_0(\rho)]
\]

(9)

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

**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 \( \tilde{U} \) be the quantum map (in general non-unitary) effectively applied by the quantum processor. One way to certify the quality of \( \tilde{U} \) is through the average gate fidelity\cite{18,30,62,113}:

\[
\mathcal{F}_{\text{avg}}(U) := \int d\psi \mathcal{F}(U |\psi\rangle \langle \psi| \tilde{U}) = \langle \psi| \tilde{U} \rho \tilde{U}^\dagger |\psi\rangle,
\]

i.e. the average fidelity between the application of the target unitary on \(|\psi\rangle\) and the quantum map on \(|\psi\rangle\), according to the Haar measure \( d\psi \). One can easily show, via a Kraus operator expansion, see \cite{105}, that \( \mathcal{F}_{\text{avg}}(U) = \mathcal{F}_U + O(d^{-1}) \), where \( \mathcal{F}_U := d^{-2} \sum_{\mu} \text{tr}(P_\mu U P_\mu U^\dagger) \text{tr}(P_\mu \tilde{U} P_\mu) \) is the entanglement fidelity between \( U \) and the quantum map \( \tilde{U}(\cdot) \)\cite{62}. Let us use the same trick as before: define a probability distribution \( \Xi_U := \{ d^{-2} \text{tr}^2(P_\mu U P_\mu U^\dagger) | \mu, \nu = 1, \ldots, d^2 \} \), and rewrite \( \mathcal{F}_U \) as the average of \( X_{\mu \nu} := \text{tr}(P_\mu \tilde{U} P_\nu)/\text{tr}(P_\mu U P_\nu U^\dagger) \) on the probability distribution \( \Xi_U \), i.e. \( \mathcal{F}_U = (X_{\mu \nu})_{\Xi_U} \). \( \mathcal{F}_U \) can thus be estimated via Monte Carlo methods by sampling \( k \) pairs of Pauli operators \( (P_\mu, P_\nu), \ldots, (P_k, P_k) \) according to the probability distribution \( \Xi_U \). We quantify the resources as the number of uses \( N_{\mathcal{F}_U} \) of the channel \( \tilde{U} \). Note that, from Lemma 1, the probability distribution \( \Xi_U \) coincides with the probability distribution associated to 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 \( \mathcal{M}_\alpha(\langle U\rangle) \), see\cite{105}.

**Theorem 2.** The number of resources \( N_{\mathcal{F}_U} \) to estimate \( \mathcal{F}_U \) with accuracy \( \epsilon \) and success probability \( 1 - \delta \) is bounded

\[
\frac{2}{\epsilon^2} \ln \frac{2}{\delta} \exp[m_2(|U\rangle)] \leq N_{\mathcal{F}_U} \leq \frac{64}{\epsilon^2} \ln \frac{2}{\delta} \exp[m_0(|U\rangle)]
\]

(10)

We find that the magic of the Choi state \(|U\rangle\) is a direct quantifier of the hardness in verifying the correct application of a target unitary. Now, by using Lemmas 2 and 3, we also see how quantum certification is related to quantum chaos:

**Corollary 3.** The resources \( N_{\mathcal{F}_U} \) are bounded:

\[
\Omega(\text{OTOC}_k(|U\rangle)^{-1}) \leq N_{\mathcal{F}_U} \leq \Omega(\exp[\nu(|U\rangle)])
\]

(11)

As small value for the OTOCs is a measure of quantum chaos\cite{100}, we see that the more chaotic is \( U \), the harder is certification via direct fidelity estimation.

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 circuits\cite{97,114} consists of global layers of Clifford gates interleaved by single qubit \( T \)-gates. In\cite{89} it was proved that classical simulations of such circuits scale exponentially with \( t \), while in\cite{97} we proved that, to mimic quantum chaotic evolution, it is both necessary and sufficient that \( t = O(n) \), 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. We can already suspect that the answer is no, since quantum chaos has to contain an extensive amount of magic. Formally:

**Corollary 4.** The \( \langle N_{\mathcal{F}_U} \rangle \) average number of resources to certify a \( t \)-doped Clifford circuit \( C_t \) increases exponentially with \( t \)\cite{105}:

\[
\Omega(\exp[t \log \frac{4}{3}]) \leq \langle N_{\mathcal{F}_U} \rangle \leq \Omega(\exp[t]) \leq \Omega(d^2)
\]

(12)

Let us now briefly comment on the scalings of the bounds in Eq.(12). First note that such scalings are the same of those in Corollary 1: while for states the resources are upper bounded by \( \Omega(d^2) \) 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.

Summary and discussion—In this letter, we showed the tight connection underlying quantum certification, magic, and chaos. We proved our results in the setting of direct fidelity estimation protocols via Monte Carlo sampling, showing that the complexity of the quantum certification scales exponentially with the magic $M(\langle \psi \rangle)$. This fact implies the impossibility for such a protocol to certify all the states $\langle \psi \rangle$ beyond the efficiency threshold $M(\langle \psi \rangle) = O(\log n)$. Remarkably, the protocol fails to certify all those states which turn out to be useful to achieve quantum speedups.

However, another quantum certification protocol based on direct fidelity estimation has been recently introduced: shadow fidelity estimation, e.g. the Clifford group $\mu_{CI}$ – e.g. the Clifford group $\mu_{CI}$ – is possible to estimate the fidelity with a sample complexity not scaling with the number of qubits. Nonetheless, to ensure an efficient classical postprocessing algorithm, shadow fidelity estimation also deals with magic. Indeed, to post-process the data in a shadow fidelity protocol, one has to classically estimate the outcome probabilities of the state $U U^\dagger$, where $U$ is any unitary uniformly drawn from a unitary 2-design. For each $U \sim \mu_{CI}$, the complexity of such an operation scale exponentially with the magic of $U$, see e.g. [85, 89]. 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 magic, the resource which makes quantum technology truly quantum.

Acknowledgments.—The authors thank Sarah True and Oliver Hahn 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 R2000000025727.

* lorenzo.leone001@umb.edu

---

[1] L. Leone, S. F. E. Oliviero and A. Hamma, Stabilizer Renyi entropy, Physical Review Letters 128, 050402 (2022), doi:10.1103/PhysRevLett.128.050402

[2] R. D. Somma, S. Boixo et al., Quantum simulations of classical annealing processes, Physical Review Letters 101, 130504 (2008), doi:10.1103/PhysRevLett.101.130504

[3] H. J. Kimble, The quantum internet, Nature 453(7198), 1023 (2008), doi:10.1038/nature07127

[4] J. I. Cirac and P. Zoller, Goals and opportunities in quantum simulation, Nature Physics 8(4), 264 (2012), doi:10.1038/nphys2273

[5] S. Bravyi, D. Gosset and R. König, Quantum advantage with shallow circuits, Science 362(6412), 308 (2018), doi:10.1126/science.aar3606

[6] A. Acín, I. Bloch et al., The quantum technologies roadmap: a european community view, New Journal of Physics 20(8), 080201 (2018), doi:10.1088/1367-2630/aae1ea

[7] F. Arute, K. Arya et al., Quantum supremacy using a programmable superconducting processor, Nature 574(7779), 505 (2019), doi:10.1038/s41586-019-1666-5

[8] H. Buhrman, R. Cleve et al., Quantum fingerprinting, Physical Review Letters 87, 167902 (2001), doi:10.1103/PhysRevLett.87.167902

[9] A. Gilànyi and A. Poremba, Improved quantum algorithms for fidelity estimation, 10.48550/ARXIV.2203.15993 (2022).

[10] L. Cincio, Y. Subaşı et al., Learning the quantum algorithm for state overlap, New Journal of Physics 20(11), 113022 (2018), doi:10.1088/1367-2630/aae94a

[11] E. Knill, D. Leibfried et al., Randomized benchmarking of quantum gates, Physical Review A 77, 012307 (2008), doi:10.1103/PhysRevA.77.012307

[12] E. Magesan, J. M. Gambetta and J. Emerson, Scalable and robust randomized benchmarking of quantum processes, Physical Review Letters 106, 180504 (2011), doi:10.1103/PhysRevLett.106.180504

[13] J. M. Gambetta, A. D. Corcoles et al., Characterization of addressability by simultaneous randomized benchmarking, Physical Review Letters 109, 240504 (2012), doi:10.1103/PhysRevLett.109.240504

[14] E. Magesan, J. M. Gambetta et al., Efficient measurement of quantum gate error by interleaved randomized benchmarking, Physical Review Letters 109, 080505 (2012), doi:10.1103/PhysRevLett.109.080505

[15] S. Kimmel, M. P. da Silva et al., Robust extraction of tomographic information via randomized benchmarking, Physical Review X 4, 011059 (2014), doi:10.1103/PhysRevX.4.011059

[16] J. J. Wallman and S. T. Flammia, Randomized benchmarking with confidence, New Journal of Physics 16(10), 103032 (2014), doi:10.1088/1367-2630/16/10/103032

[17] K. Kueng, D. M. Long et al., Comparing experiments to the fault-tolerance threshold, Physical Review Letters 117, 170502 (2016), doi:10.1103/PhysRevLett.117.170502

[18] I. Roth, K. Kueng et al., Quantum gates from few average gate fidelities, Physical Review Letters 121, 170502 (2018), doi:10.1103/PhysRevLett.121.170502

[19] J. J. Wallman, Randomized benchmarking with gate-dependent noise, Quantum 2, 47 (2018), doi:10.22331/q-2018-01-29-47

[20] A. Erhard, J. J. Wallman et al., Characterizing the resource which makes quantum technology truly quantum, Physical Review A 108, 032431 (2023), doi:10.1103/PhysRevA.108.032431
Physical Review Letters 116, 250501 (2016), doi:10.1103/PhysRevLett.116.250501.

S. Bravyi, G. Smith and J. A. Smolin, Trading classical and quantum computational resources, Physical Review X 6, 021043 (2016), doi:10.1103/PhysRevX.6.021043.

S. Bravyi, D. Browne et al., Simulation of quantum circuits by low-rank stabilizer decompositions, Quantum 3, 181 (2019), doi:10.22331/q-2019-09-02-181.

J. R. Seddon, B. Regula et al., Quantifying quantum speedups: Improved classical simulation of tightly magic monotones, PRX Quantum 2, 010345 (2021), doi:10.1103/PRXQuantum.2.010345.

C. Chamon, A. Hamma and E. R. Mucciolo, Emergent irreversible and entanglement spectrum statistics, Physical Review Letters 112, 240501 (2014), doi:10.1103/PhysRevLett.112.240501.

D. Shaffer, C. Chamon et al., Irreversibility and entanglement spectrum statistics in quantum circuits, Journal of Statistical Mechanics: Theory and Experiment 2014(12), P12007 (2014), doi:10.1088/1742-5468/2014/12/p12007.

Z.-C. Yang, A. Hamma et al., Entanglement complexity in quantum many-body dynamics, thermalization, and localization, Physical Review B 96, 020408(R) (2017), doi:10.1103/PhysRevB.96.020408.

S. Zhou, Z.-C. Yang et al., Single T gate in a Clifford circuit drives transition to universal entanglement spectrum statistics, SciPost Physics 9, 87 (2020), doi:10.21468/SciPostPhys.9.6.087.

L. Leone, S. F. E. Oliviero et al., Quantum Chaos is Quantum, Quantum 5, 453 (2021), doi:10.22331/q-2021-05-04-45.

S. F. Oliviero, L. Leone and A. Hamma, Transitions in entanglement complexity in random quantum circuits by measurements, Physics Letters A 418, 127721 (2021), doi:10.1016/j.physleta.2021.127721.

S. True and A. Hamma, Transitions in entanglement complexity in random circuits, doi:10.48550/ARXIV.2202.02648 (2022).

D. A. Roberts and B. Yoshida, Chaos and complexity by design, Journal of High Energy Physics 2017(4), doi:10.1007/JHEP04(2017)121.

S. F. E. Oliviero, L. Leone et al., Random Matrix Theory of the Isospectral Twirling, SciPost Physics 10, 76 (2021), doi:10.21468/SciPostPhys.10.3.076.

L. Leone, S. F. E. Oliviero and A. Hamma, Isospectral twirling and quantum chaos, Entropy 23(8), doi:10.3390/e23081073.

S. F. E. Oliviero, L. Leone et al., Measuring magic on a quantum processor, doi:10.48550/ARXIV.2204.00015 (2022).

M. Beverland, E. Campbell et al., Lower bounds on the non-clifford resources for quantum computations, Quantum Science and Technology 5(3), 035009 (2020), doi:10.1088/2058-9565/ab896c.

See Supplemental Material for formal proofs, which includes[121,122].

J. Jiang and X. Wang, Lower bound the t-count via unitary stabilizer nullity, doi:10.48550/ARXIV.2110.02962 (2021).

B. P. Lanyon, C. Maier et al., Efficient tomography of a quantum many-body system, Nature Physics 13(12), 1158 (2017), doi:10.1038/nphys4244.

A. Fedorov, L. Steffen et al., Implementation of a toffoli gate with superconducting circuits, Nature 481(7380), 170 (2012), doi:10.1038/nature10713.

R. O’Donnell and J. Wright, Efficient quantum tomography, In Proceedings of the Forty-Eighth Annual ACM Symposium on Theory of Computing, STOC ’16, p. 899–912. Association for Computing Machinery, New York, NY, USA, ISBN 9781450341325, doi:10.1145/2897518.2897534 (2016).

D. Gottesman and I. Chuang, Quantum digital signatures, PH/0105033 (2001).

J. M. Hammersley and K. W. Morton, Poor man’s monte carlo, Journal of the Royal Statistical Society: Series B (Methodological) 16(1), 23 (1954), https://doi.org/10.1111/j.1467-9868.1954.tb00145.x.

M. N. Rosenbluth and A. W. Rosenbluth, Monte carlo calculation of the average extension of molecular chains, The Journal of Chemical Physics 23(2), 356 (1955), doi:10.1063/1.174196.

D. M. Reich, G. Guarnieri and C. P. Koch, Optimal strategies for estimating the average fidelity of quantum gates, Physical Review Letters 111, 200401 (2013), doi:10.1103/PhysRevLett.111.200401.

J. Haferkamp, F. Montanaro-Mora et al., Quantum homeopathy works: Efficient unitary designs with a system-size independent number of non-Clifford gates, doi:10.48550/ARXIV.2002.09524 (2020).

S. Aaronson, Shadow tomography of quantum states, In Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2018, p. 325–338. Association for Computing Machinery, New York, NY, USA, ISBN 9781450355599, doi:10.1145/3188745.3188805 (2018).

S. Chen, W. Yu et al., Robust shadow estimation, PRX Quantum 2, 03048 (2021), doi:10.1103/PRXQuantum.2.03048.

D. E. Koh and S. Grewal, Classical shadows with noise, doi:10.48550/ARXIV.2011.11589 (2020).

R. J. Garcia, Y. Zhou and A. Jaffe, Quantum scrambling with classical shadows, Physical Review Research 3, 033155 (2021), doi:10.1103/PhysRevResearch.3.033155.

R. Levy, D. Luo and B. K. Clark, Classical shadows for quantum process tomography on near-term quantum computers, doi:10.48550/ARXIV.2110.02962 (2021).

H.-Y. Hu, S. Choi and Y.-Z. You, Classical shadow tomography with locally scrambled quantum dynamics, doi:10.48550/ARXIV.2107.04017 (2021).

W. Hoefding, Probability inequalities for sums of bounded random variables, Journal of the American Statistical Association 53(283), 13 (1958), doi:10.1080/01621459.1963.1050115.

L. Zhang, Matrix integrals over unitary groups: An application of schur-ory duality, doi:10.48550/ARXIV.1408.3782 (2014).
SUPPLEMENTAL MATERIAL

Appendix A: Stabilizer Rényi entropy

Proof of Lemma 1

In this section, we prove that the magic of the Choi–Jamiołkowski isomorphism $U \mapsto |U\rangle$ can be measured as the Rényi entropy of the probability distribution $\Xi_U$ whose elements are:

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

Before moving into the proof, note that $d^2\Xi_U(P, P')$ is a double stochastic matrix with entries labeled by $P$ and $P'$. Indeed, using the identity \[\text{tr}(\hat{S}U^\otimes 2 PP'U^\dagger U^\otimes 2) = \frac{\text{tr}(PP')}{d} \quad \text{(A2)}\]

where we used the fact that $[U^\otimes 2, \hat{S}]=0$ and $\text{tr}(\hat{S} A \otimes B) = \text{tr}(AB)$.

First, recall that the Choi isomorphism is a map from the space of operator $B(\mathcal{H})$ 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

$$|U\rangle := (\mathbb{1} \otimes U) |I\rangle, \quad |I\rangle = \frac{1}{\sqrt{d}} \sum_i |i\rangle \otimes |i\rangle \quad \text{(A3)}$$

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

$$\Xi_U(P \otimes P') = \frac{1}{d^2} \text{tr}^2(P \otimes P' |U\rangle \langle U|) \quad P, P' \in \mathbb{P}(n) \quad \text{(A4)}$$

by definition \[1\], the stabilizer Rényi entropy reads:

$$M_\alpha(|U\rangle) = \frac{1}{1-\alpha} \log \sum_{P, P'} |\Xi_U(P \otimes P')|^\alpha - 2 \log d \quad \text{(A5)}$$

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

$$\text{tr}(P \otimes P' |U\rangle \langle U|) = \text{tr}(P \otimes P' |U\rangle \langle U|)^{T_z} = \pm \text{tr}(P \otimes P' |U\rangle \langle U|)^{T_z} \quad \text{(A6)}$$

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

Now:

$$|U\rangle \langle U|^{T_z} = (\mathbb{1} \otimes U^T) |I\rangle \langle I|^T_z (\mathbb{1} \otimes U^*) = (\mathbb{1} \otimes U^T) \frac{\hat{S}}{d^2} (\mathbb{1} \otimes U^*) = \frac{\hat{S}}{d} (U^T \otimes U^*) \quad \text{(A7)}$$

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

$$\text{tr}(P \otimes P' |U\rangle \langle U|) = \pm \frac{1}{d} \text{tr}(PU^T P'U^*) = \pm \frac{1}{d} \text{tr}(P'U^T U^\dagger) \quad \text{(A8)}$$

Thus we obtain that the elements of the probability distribution $\Xi_U$ read

$$\Xi_U(P, P') = \frac{1}{d^2} \text{tr}^2(P \otimes P' |U\rangle \langle U|) = \frac{1}{d^2} \text{tr}^2(P'U^T U^\dagger) \quad \text{(A9)}$$

and the lemma follows straightforwardly.
Proof of Lemma 2

From Lemma 1, we have that:
\[
M_\alpha(|U\rangle) = \frac{1}{1 - \alpha} \log \sum_{P,P'} \frac{tr^{2\alpha}(PUPU'^\dagger)}{d^{2\alpha}} - \log d = \frac{1}{1 - \alpha} \log \frac{1}{d^2} \sum_{P,P'} \frac{tr^{2\alpha}(PUPU'^\dagger)}{d^{2\alpha}} \tag{A10}
\]

To prove the Lemma, we recall the swap identity \(\hat{S} = d^{-1} \sum_P P^\otimes 2\), and note that:
\[
\frac{tr(PP'U^\dagger)}{d} \frac{tr(PP'U'^\dagger)}{d} = \frac{1}{d^2} \sum_{P_1} \frac{tr(PP'U^\dagger_1 PPU'^\dagger P_1 U')}{d} \equiv \frac{tr((PP'U^\dagger_1 PPU'^\dagger_1 P_1 U')_1)}{d} \tag{A11}
\]

We thus can recursively use the above identity and arrive to
\[
\frac{tr^{2\alpha}(PP'U'^\dagger)}{d^{2\alpha}} = d^{-1} \text{tr}[\{P_{2\alpha} \prod_{i=1}^{2\alpha} UPU^\dagger P_{i-1} P_i\}] = oto_{2\alpha}(P, P') \tag{A12}
\]
where \(\langle \cdot \rangle \equiv d^{-2} \sum_{P_i \in \mathcal{P}(n)} \) for all \(i = 1, \ldots, 2\alpha\), while \(P_0 \equiv \mathbb{I}\). Let us write the above explicitly for \(\alpha = 2\):
\[
\frac{tr^4(PP'U'^\dagger)}{d^4} = d^{-1} \text{tr}\{P(U^\dagger P' P' P' P' P' P'' P_1 P_2 P'' P_3 P'' P'' P'' P_4 P_5 \ldots P_i)\}
\]
\[
= d^{-1} \text{tr}\{P(U) P' P' P' P'' P_1 P'' P'' P_3 P'' P'' P'' P_5 P_{i+1} P_{i+2} \ldots P_i\} = oto_{8}(P, P') \tag{A13}
\]
where \(P(U) \equiv UPU^\dagger\). Note that the above holds for for any integer \(\alpha > 1\).

Appendix B: Quantum states certification

1. Proof of Theorem 1

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 [30], see also [62]. We prove the two bounds separately.

- **Lower bound**: Here we need to lower bound the necessary resources such that the estimator \(\hat{F} = \frac{1}{k} \sum_{P \in \mathcal{P}} \hat{X}_P\), defined in the main text, obeys to:
\[
\Pr(|F - \hat{F}| \leq \epsilon) \geq 1 - \delta \tag{B1}
\]
To prove it, define \(m := \min_P |\text{tr}(P\psi)|\) and note that \(|\hat{X}_P| \leq m^{-1}\). Using Hoeffding’s inequality[121], one can bound the probability:
\[
\Pr(|F - \hat{F}| \leq \epsilon) \geq 1 - 2 \exp \left[-\frac{k \epsilon^2}{2m^2}\right] \tag{B2}
\]
to have the probability lower bounded by \(1 - \delta\), the number of samples \(k\) must be:
\[
k = \frac{2 \epsilon^2}{m^2} \ln(2/\delta) \tag{B3}
\]
setting the number of copies \(c_P(\hat{\psi})\) of the state \(\hat{\psi}\) to determine each sampled \(P\) to be one (one-shot measurements), i.e. \(c_P(\hat{\psi}) = 1 \forall P\), one has that \(N_{\hat{\psi}} \equiv k\). Let us lower bound the number of resources \(N_{\hat{\psi}}\). Let \(P \in \mathcal{P}(n)\), then the average of \(|\text{tr}(P\psi)|\) over the state dependent probability distribution \(\Xi_\psi\) is upper bounded by
\[
\langle |\text{tr}(P\psi)| \rangle_{\Xi_\psi} \leq \sqrt{\langle tr^2(P\psi) \rangle_{\Xi_\psi}} = \sqrt{\exp[-M_2(||\psi||)]} \tag{B4}
\]
then since \(m = \min_P |\text{tr}(P\psi)|\), then one trivially has \(m \leq \langle |\text{tr}(P\psi)| \rangle_{\Xi_\psi}\) and thus \(m \leq \sqrt{\exp[-M_2(||\psi||)]}\). Thus, the number of resources \(N_{\hat{\psi}}\) is lower bounded
\[
N_{\hat{\psi}} \geq \frac{2 \epsilon^2}{\sqrt{m}} \ln(2/\delta) \exp[M_2(||\psi||)] \tag{B5}
\]
• 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):

\[
\text{tr}(P\psi_{\text{cut}}) := \begin{cases} \text{tr}(P\psi), & \text{if } |\text{tr}(P\psi)| \geq \frac{1}{\sqrt{2}} \sqrt{\exp[-M_0(\psi)]} \\ 0, & \text{otherwise} \end{cases}
\]

(B6)

and its normalized version \( \psi' := \psi_{\text{cut}}/\|\psi_{\text{cut}}\|_2 \). Note that \( \|\psi_{\text{cut}}\|_2 = \sqrt{\frac{1}{d} \sum_{P \in Q} \text{tr}^2(P\psi)} \), where \( Q := \{ P \in F(n) | |\text{tr}(P\psi)| \geq \epsilon/(2\sqrt{2}) \sqrt{\exp[-M_0(\psi)]} \} \). \( \psi' \) in the Pauli basis reads:

\[
\psi' = \frac{1}{\sqrt{\frac{1}{d} \sum_{P \in Q} \text{tr}^2(P\psi)}} \frac{1}{d} \sum_{P \in Q} \text{tr}(P\psi) P
\]

(B7)

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

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

(B8)

Let us prove that, setting \( N = \frac{1}{\epsilon} \ln(2/\delta) \exp[M_0(\psi)] \), we used \( \text{tr}(\psi\psi'') = 1 \). Let us evaluate \( \text{tr}(\psi\psi') \), writing it in the Pauli basis:

\[
\text{tr}(\psi\psi') = \frac{1}{\|\psi_{\text{cut}}\|_2} \frac{1}{d} \sum_{P \in Q} \text{tr}^2(P\psi) = \frac{1}{d} \sum_{P \in Q} \text{tr}^2(P\psi) = \frac{1 - 1/d \sum_{P \in Q} \text{tr}^2(P\psi) \geq 1 - \epsilon^2 \exp[-M_0(\psi)] / 8d}
\]

where \( \tilde{Q} \) is the complement set of \( Q \). Note that \( |\tilde{Q}| = \text{card}(\psi) - |Q| \) where \( \text{card}(\psi) := |\{ P | \text{tr}(P\psi) \neq 0 \}| \) 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:

\[
|F' - F| \leq \frac{\epsilon}{2}
\]

(B10)

Note that \( F' \) can be estimated in a same fashion of \( F \):

\[
F' = \frac{1}{d} \sum_{P} \text{tr}(P\tilde{\psi}) \text{tr}(P\psi') = \langle X'_{P} \rangle_{\Xi_{\psi'}}
\]

(B11)

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

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

(B12)

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

\[
\hat{F}' = \frac{1}{k} \sum_{P \in K'} X'_{P}
\]

(B13)

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

Let us prove that, setting \( N_{\tilde{\psi}} \leq \frac{1}{\epsilon} \ln(2/\delta) \exp[M_0(\psi)] \), we have:

\[
\text{Pr}(|F' - \hat{F}'| \leq \epsilon) \geq 1 - \delta
\]

(B14)

First:

\[
|F - \hat{F}'| \leq |F - F'| + |F' - \hat{F}'| \leq \frac{\epsilon}{2} + |F' - \hat{F}'|
\]

(B15)
then note that \( \Pr(|\mathcal{F} - \tilde{\mathcal{F}}| \leq \epsilon) = \Pr(|\mathcal{F}' - \tilde{\mathcal{F}}'| \leq \epsilon/2) \). Since \( \mathbb{E}(\hat{\mathcal{F}}') = \mathcal{F}' \), i.e. \( \hat{\mathcal{F}}' \) is an unbiased estimator for \( \mathcal{F}' \), we can use the Hoeffding’s inequality once again:

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

(B16)

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

\[
N_{\tilde{\psi}} = k = \frac{8}{\epsilon^2 m'^2} \ln(2/\delta)
\]  

(B17)

To prove the upper bound to the number of resources \( N_{\tilde{\psi}} \) is sufficient to note that:

\[
m' = \min_{P \in \mathcal{Q}} \frac{|\text{tr}(\psi|P))|}{\sqrt{1/4 \sum_{P \in \mathcal{Q}} \text{tr}^2(\psi|P))}} \geq \min_{P \in \mathcal{Q}} \text{tr}(\psi|P)) \geq \frac{\epsilon}{2\sqrt{2}} \sqrt{\exp[-M_0(\psi)]} \text{ok}
\]  

(B18)

where we exploited once again the fact that \( \sqrt{1/4 \sum_{P \in \mathcal{Q}} \text{tr}^2(\psi|P))} \leq 1 \). We finally obtain:

\[
N_{\tilde{\psi}} \leq \frac{64}{\epsilon^2} \ln(2/\delta) \exp[M_0(\psi)]
\]  

(B19)

which concludes the proof.

2. Proof of Corollary 1

From Theorem 1, we have that the average of \( N_{\tilde{\psi}} \) over the \( t \)-doped stabilizer states \( \psi_t \) (in the following denoted as \( \langle \cdot \rangle \)), is bounded:

\[
\langle N_{\tilde{\psi}} \rangle \leq \frac{64}{\epsilon^2} \ln(2/\delta) \exp[M_0(\psi_t)]
\]  

(B20)

the average of the left-hand side for states can be lower bounded through the Jensen inequality:

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

(B21)

where \( Q = \frac{1}{d} \sum_{P \in \mathcal{P}} P_{\psi_t}^{\otimes 4}[1] \). Then the average over \( t \)-doped stabilizer states \( \langle \psi_t \rangle \) can be computed using the techniques in[1, 98]. The result is shown in Eq. (13) of [1]:

\[
\langle \exp[M_2(\psi_t)] \rangle \geq \frac{d + 3}{4 + (d - 1)f_+^t} = \Omega(\exp(t \log 4/3))
\]  

(B22)

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

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

\[
\exp[M_0(\psi_t)] \leq \exp[\nu(|\psi_t\rangle)]
\]  

(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[106] we have the following chain of inequality:

\[
\nu(|\psi_t\rangle) = \nu(C_t |0\rangle^{\otimes n}) \leq \nu(C_t) \leq t
\]  

(B24)

where \( \nu(C_t) \) is the unitary stabilizer nullity, introduced in[106], which lower bounds the number of non-Clifford resources injected in a Clifford unitary operator. Therefore we obtain:

\[
\exp[M_0(\psi_t)] \leq \exp[t]
\]  

(B25)

lastly note that since \( M_0(\psi_t) \leq \log d \), we have \( \langle N_{\tilde{\psi}} \rangle \leq O(d) \).
Appendix C: Unitary operators

Entanglement fidelity

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

\[
F_{\text{avg}}(U) := \int d\psi \, \text{tr}(U\psi U^\dagger \tilde{U}(\psi)) \tag{C1}
\]

By expanding \( \tilde{U} \) in terms of Kraus operator \( A_\alpha \) one can write the above as

\[
F_{\text{avg}} = \sum_\alpha \int d\psi \, \text{tr}(U\psi U^\dagger A_\alpha \psi A_\alpha^\dagger) \tag{C2}
\]

by the well-known identity\[122\] \( \int d\psi \psi \otimes 2 = [d(d+1)]^{-1}(\mathbb{I} + \hat{S}) \), one has:

\[
F_{\text{avg}} = \frac{1}{d} \sum_\alpha \text{tr}(U^\dagger \otimes U A_\alpha \otimes A_\alpha^\dagger) + 1 \tag{C3}
\]

multiplying by \( \mathbb{I} \otimes 2 = \hat{S} \hat{S} \) 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 \( P_\mu \otimes P_\nu \) on \( H \otimes 2 \), we have:

\[
\text{tr}(U^\dagger \otimes U A_\alpha \otimes A_\alpha^\dagger) = \frac{1}{d^2} \sum_{\mu\nu} \text{tr}(P_\mu U P_\nu U^\dagger) \text{tr}(P_\mu A_\alpha P_\nu A_\alpha^\dagger) \tag{C4}
\]

Finally \( F_{\text{avg}} = F_U + O(d^{-1}) \), where we defined:

\[
F_U := \frac{1}{d} \sum_{\mu\nu} \text{tr}(P_\mu U P_\nu U^\dagger) \text{tr}(P_\mu \tilde{U}(P_\nu)). \tag{C5}
\]

**Proof of Theorem 2**

In this section, we prove Theorem 2. We give the proof for the lower and the upper bound separately.

- **Lower bound:**

  Following\[30\], let \( (P_1, P_1') \ldots (P_k, P_k') \) be \( k \) pairs of Pauli operators sampled at random according to the probability distribution \( \Xi_U \) and labeled by \( i = 1, \ldots, k \). Let \( \tilde{F}_U = \frac{1}{k} \sum_{i=1}^k \bar{X}_i \) be an estimator for \( F_U \), i.e. \( E[\tilde{F}_U] = F_{\bar{U}} \), where

  \[
  \bar{X}_i = \frac{1}{\text{tr}(U P_i U^\dagger P_i')} \frac{c_i(\tilde{U})}{\sum_{j=1}^{c_i(\tilde{U})} P_{ij}(\tilde{U})} \tag{C6}
  \]

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

  \[
  \Pr(|\tilde{F}_U - F_U| \leq \epsilon) \geq 1 - 2 \exp \left[ - \frac{k \epsilon^2}{2m_U^2} \right] \tag{C7}
  \]

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

  \[
  N_{\tilde{U}} = \frac{2}{\epsilon^2 m_U^2} \ln(2/\delta) \tag{C8}
  \]
to prove the lower bound is sufficient to note that:

\[
m_U := \min_{P,P'} |\text{tr}(U^\dagger PU'P')|/d \leq \langle d^{-1} |\text{tr}(U^\dagger PU'P')\rangle \leq d^{-1} \sqrt{\sum_{P,P'} \text{tr}^2(U^\dagger PU'P')/d^2} = \sqrt{\exp[-M_2(|U|)]}
\]

where \(M_2(|U|)\) is the Stabilizer Rényi entropy of the Choi state \(|U\rangle\), cfr. Lemma 1.

\* Upper bound:

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

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

and \(Q_U := \{P,P' | \text{tr}(U_{\text{cut}}^\dagger PU_{\text{cut}}P') \neq 0\}\). Now define the operator \(U'\) such that:

\[
\mathcal{S}U^\dagger \otimes U' = \frac{1}{\sqrt{\sum_{P,P' \in Q_U} \text{tr}^2(U^\dagger PU'P')}} \sum_{P,P' \in Q_U} \text{tr}(U^\dagger PU'P') P \otimes P'
\]

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

\[
|\mathcal{F}_{U'} - \mathcal{F}_U| \leq \frac{1}{d^2} \| \sum_\alpha A_{\alpha} \otimes A_{\alpha}^\dagger \|_2 \|U^\dagger \otimes U' - U^\dagger \otimes U\|_2 \leq \frac{1}{d} \|U^\dagger \otimes U' - U^\dagger \otimes U\|_2
\]

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

\[
\frac{1}{d^2} \|U^\dagger \otimes U' - U^\dagger \otimes U\|_2^2 = \sqrt{2} \left(1 - \frac{1}{d^2} \text{tr}(U^\dagger \otimes U'U'U' \otimes U')\right)
\]

we are just left to the following series of inequalites:

\[
\sum_{P,P' \in Q_U} \text{tr}^2(U^\dagger PU'P') = d^4 - \sum_{P,P' \in \bar{Q}_U} \text{tr}^2(U^\dagger PU'P') > d^4 - \frac{\theta^2 d^4 |\bar{Q}_U|}{\text{card}(U)} > d^4(1 - \theta^2)
\]

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

\[
|\mathcal{F}_{U'} - \mathcal{F}_U| \leq \frac{1}{d} \|U^\dagger \otimes U' - U^\dagger \otimes U\|_2 \leq \sqrt{2} \theta
\]

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

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

where \(\mathcal{X}_{\mu,\nu} := \text{tr}(P_{\mu} \bar{U}(P_{\nu})) / \text{tr}(P_{\mu} U'P_{\nu}U')\) and \(\Xi_U\) is a probability distribution whose elements are:

\[
\Xi_U(P_{\mu},P_{\nu}) = \begin{cases} 
\frac{\text{tr}^2(P_{\mu} U'P_{\nu}U')}{\sum_{P,P' \in \bar{Q}_U} \text{tr}^2(U^\dagger PU'P')}, & P_{\mu},P_{\nu} \in Q_U \\
0, & \text{otherwise}
\end{cases}
\]
To proceed we look at the average denoted as $\langle \cdot \rangle_q$ introduced in Eq. (C2). The number of resources is lower bounded by:

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

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 $m_U' := \min_P \{\text{tr}(P_i U' P_j U' d)\}$, since $\mathbb{E}\tilde{\mathcal{F}}_{U'} = \mathcal{F}_{U'}$ we can use Hoeffding’s inequality to bound the probability as:

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

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

$$N_U = \frac{8}{\epsilon^2 m_U'^2} \ln(2/\delta)$$

Setting $\theta = \epsilon/2$, 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 $m_U'$:

$$m_U' \geq \frac{\epsilon}{2\sqrt{2}} \sqrt{\exp[-M_0(|\mathcal{U}|)]}$$

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

**Proof of Corollary 4**

In this section, we prove Corollary 4. 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 2 we have:

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

To proceed we look at the average denoted as $\langle \cdot \rangle_{C_t}$:

$$\langle (\exp[M_2(|C_t|)]) \rangle_{C_t} \geq \frac{d^2}{\langle \text{tr}(QU^{\otimes 4}QU^{\dagger \otimes 4}) \rangle_{C_t}}$$

where $Q := \frac{1}{d^2} \sum_{P \in \mathcal{P}_d} P^{\otimes 4}$, and we used the Jensen inequality to bound the average of $\langle (\exp[M_2(|C_t|)]) \rangle_{C_t}$. To compute the average over Doped Clifford circuits we use the techniques introduced in [97, 98], and obtain:

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

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

$$N_{C_t} \geq \Omega(\exp[t \log 4/3])$$
To prove the upper bound to the number of resources we use the upper bound in Theorem 2.

\[ N_{C_t} \leq \frac{64}{e^4} \ln(2/\delta) \exp[\nu(U)] \]  \hspace{1cm} (C28)

As proven in [106] the unitary stabilizer nullity can be upper bounded by the T-count \( t(U) \), which corresponds to the minimum number of T gates required to implement the unitary \( U \). Eq. (C28) can be upper-bounded via the T-count as:

\[ N_{C_t} \leq \frac{64}{e^4} \ln(2/\delta) \exp[\nu(U)] \leq \frac{64}{e^4} \ln(2/\delta) \exp[t] = \Omega(\exp[t]) \]  \hspace{1cm} (C29)

where \( t(C_t) = t \) by definition. This concludes the proof.