Pseudorandom unitaries are neither real nor sparse nor noise-robust

Tobias Haug[1,2], Kishor Bharti[3,4], and Dax Enshan Koh[3,4,5]

[1]Quantum Research Center, Technology Innovation Institute, Abu Dhabi, UAE
[2]Blackett Laboratory, Imperial College London SW7 2AZ, UK
[3]Quantum Innovation Centre (Q.InC), Agency for Science, Technology and Research (A*STAR), 2 Fusionopolis Way, Innovis #08-03, Singapore 138634, Republic of Singapore
[4]Institute of High Performance Computing (IHPC), Agency for Science, Technology and Research (A*STAR), 1 Fusionopolis Way, #16-16 Connexis, Singapore 138632, Republic of Singapore
[5]Science, Mathematics and Technology Cluster, Singapore University of Technology and Design, 8 Somapah Road, Singapore 487372, Singapore

Pseudorandom quantum states (PRSs) and pseudorandom unitaries (PRUs) possess the dual nature of being efficiently constructible while appearing completely random to any efficient quantum algorithm. In this study, we establish fundamental bounds on pseudorandomness. We show that PRSs and PRUs exist only when the probability that an error occurs is negligible, ruling out their generation on noisy intermediate-scale and early fault-tolerant quantum computers. Further, we show that PRUs need imaginarity while PRS do not have this restriction. This implies that quantum randomness requires in general a complex-valued formalism of quantum mechanics, while for random quantum states real numbers suffice. Additionally, we derive lower bounds on the coherence of PRSs and PRUs, ruling out the existence of sparse PRUs and PRSs. We also show that the notions of PRS, PRUs and pseudorandom scramblers (PRSSs) are distinct in terms of resource requirements. We introduce the concept of pseudoresources, where states which contain a low amount of a given resource masquerade as high-resource states. We define pseudocoherence, pseudopurity and pseudoimaginarity, and identify three distinct types of pseudoresources in terms of their masquerading capabilities. Our work also establishes rigorous bounds on the efficiency of property testing, demonstrating the exponential complexity in distinguishing real quantum states from imaginary ones, in contrast to the efficient measurability of unitary imaginarity. Further, we show an exponential advantage in imaginarity testing when having access to the complex conjugate of the state. Lastly, we show that the transformation from a complex to a real model of quantum computation is inefficient, in contrast to the reverse process, which is efficient. Our results establish fundamental limits on property testing and provide valuable insights into quantum pseudorandomness.

Tobias Haug: tobias.haug@u.nus.edu
Kishor Bharti: kishor.bharti1@gmail.com
Dax Enshan Koh: dax_koh@ihpc.a-star.edu.sg

Randomness is a key resource for quantum information processing [1–11]. However, a simple counting argument reveals that preparing completely random quantum states is computationally intractable. Thus, a core challenge lies in identifying quantum states and unitaries that can be efficiently prepared while remaining indistinguishable from truly random ones.

To solve this problem, the concepts of pseudorandom quantum states (PRSs), pseudorandom unitaries (PRUs) [1, 12, 13] and pseudorandom scramblers (PRSSs) [14, 15] have been introduced. There is no efficient quantum algorithm that can distinguish Haar random states and unitaries from PRSs and PRUs, respectively, yet we can efficiently prepare them. Conveniently, PRSs can be generated with much shorter circuits compared to state designs [1, 16, 17] and

have been shown to be a weaker primitive than one-way functions [18]. They have also been used to design cryptographic functionalities such as commitment schemes [19–21], pseudo one-time pads [19–21] and pseudorandom strings [22]. There is an ongoing search to identify PRSs with as simple a structure as possible. Recent work showed that PRSs can have logarithmic entanglement [17] and require at least a linear number of non-Clifford gates [23]. However, for most other properties, the minimal requirements to generate PRSs, PRSSs and PRUs are unknown.

Imaginarity and coherence are key resources in quantum information processing, playing crucial roles in achieving a quantum advantage in various tasks. Imaginarity characterizes the degree to which states and operations require non-real numbers for their description. Surprising differences between real and complex descriptions of quantum mechanics can arise [24–26] and there are tasks that can be accomplished only with operations described by non-real numbers [27–29]. On the other hand, coherence, which measures the degree of being in a superposition, is a fundamental resource in quantum processing [30–35] that is intricately linked to entanglement [36, 37], circuit complexity [38] and serves as a vital ingredient in quantum algorithms [39–42].

Given their importance, can we verify whether coherence or imaginarity are actually present in a quantum state or unitary? For such tasks, the concept of property testing has been developed [43–45]. This concept has been studied extensively for other properties [17, 46–52].

Here, we provide fundamental bounds on PRSs, PRSSs, PRUs, as well as testing for imaginarity and coherence as a function of the number of qubits n. We show that the number of copies needed to test the imaginarity of states scales as $\Omega(2^{n/2})$ with the number of qubits n, while for unitaries we require only $O(1)$ queries. Further, we show an exponential advantage in imaginarity testing with access to the complex conjugate of states. For coherence, we provide bounds on the number of copies needed for testing as a function of coherence of the state and unitary. This lower bounds the coherence of PRUs as $\omega(\log(n))$ and their imaginarity as $1 - \mathrm{negl}(n)$. With our results, we rule out the existence of real and sparse PRUs. Further, we show that PRSs and PRUs are not robust to noise, with a maximal depolarizing noise probability $p = \mathrm{negl}(n)$. We introduce pseudoresource ensembles that mimic states with high resource value using states with a only a low amount of the given resource, and identify three classes of pseudoresources. We also show that unitaries that prepare PRS, PRSS and PRUs are separated in resource complexity, proving a clear separation between the three notions of pseudorandomness. Finally, we apply our results to show that there is no efficient way to transform from a complex mode of quantum computing to a real one. Our work establishes rigorous limits on property testing and the generation of pseudorandomness.

1 Preliminaries

Pseudorandom state (PRS): An ensemble of quantum states indexed by a key (commonly referred to as a keyed family of states [1]) is considered pseudorandom if it can be generated efficiently and appears statistically indistinguishable from Haar random states to an observer with limited computational resources. More precisely, a family of PRSs is a set of pure states $\{|\phi_k\rangle\}_{k\in\mathcal{K}}$ of some key space $\mathcal{K}$ which satisfies two conditions: First, they can be efficiently prepared on quantum computers. Second, given $t = \mathrm{poly}(n)$ copies of the state, they are indistinguishable from Haar random quantum states $S(\mathcal{H})$ of an n-qubit Hilbert space $\mathcal{H}$, for any efficient quantum algorithm [1]. The notion of pseudorandom states was recently generalized to mixed states [53], which we do not address in this work.

Pseudorandom unitary (PRU): Similarly, one can also define PRUs [1, 12, 13]. A family of unitary operators is considered pseudorandom if it is both efficiently computable and indistinguishable from Haar random unitaries for an observer with bounded computational power. Moreover, variants of PRUs with restricted security have been proposed [54–57].

Pseudorandom scrambler (PRSS): Recently, the notion of PRSS was introduced, which lies in between PRS and PRU: PRSS are an ensemble of unitaries that applied to an arbitrary, fixed state generate PRSs [14, 15]. It is straightforward to see that any PRU must also be a PRSS, though it had hitherto been unclear whether all PRSSs are also PRU [14, 15]. In this work, we provide an explicit counterexample of a PRSS that is not

a PRU.

Quantum resources: In quantum information, quantum resources can be regarded as the expensive fuel needed to carry out quantum processing tasks [58]. For example, a key resource is entanglement, which characterizes the non-local correlations in quantum systems. In fault-tolerant quantum computing, the resource theory of magic plays a significant role [59]. Furthermore, quantum information processing often requires coherence, which describes the degree to which a state exists as a superposition of computational basis states [30, 31]. Finally, the degree to which complex numbers are needed to describe states is quantified by the resource theory of imaginarity [24].

Given a state ρ, one characterizes the resource content via quantum resource monotones $Q(\rho)$, which satisfy $Q(\rho) \geq 0$ [58]. These resource monotones are defined by free operations F_Q that cannot increase the resource, i.e. $Q(F_Q(\rho)) \leq Q(\rho)$, and free states with $Q(\rho) = 0$. While free operations are easy to implement, performing non-trivial tasks within the resource theory typically requires resource states with $Q(\rho) > 0$.

Property Testing: Property testing checks whether a given state has a particular property or resource Q. In particular, given t copies of $|\psi\rangle$, we want to determine whether $|\psi\rangle$ has $Q(|\psi\rangle) \leq \beta$, where β is the threshold for the property and $Q(|\psi\rangle)$ is a resource measure with $Q(|\psi\rangle) \geq 0$. The property tester accepts when $Q(|\psi\rangle) \leq \beta$, and rejects when $Q(|\psi\rangle) \geq \delta$, where δ is the rejection threshold, which is chosen as $\delta > \beta$.

For further details and formal definitions on cryptography and property testing, refer to the Appendix A and B.

2 Noise

PRSs and PRUs physically prepared on quantum computers are subject to noise originating from the environment or imperfect experimental control. One can characterize the amount of noise via the property of purity $\gamma(\rho) = \mathrm{tr}(\rho^2)$ of a state ρ [63], where $\gamma = 1$ for any pure state and $\gamma = 2^{-n}$ for maximally mixed states. It has been shown that PRSs must have maximal purity up to a negligible perturbation [20]. As we now show, PRSs and PRUs are very fragile with respect to noise channels:

Resource Q	Pure states	Unitaries
Purity	$O(1)$ [60]	$O(1)$
Entanglement	$O(1)$ [61]	$O(1)$ [47]
Magic	$O(1)$ [48]	$O(1)$ [48]
Coherence	$O(1)$ [Prop. 1]	$O(1)$ [33]
Imaginarity	$\Omega(2^{n/2})$ [Thm. 2]	$O(1)$ [62]

Table 1: Copies M needed for property tester $\mathcal{A}_Q$ for the resources of imaginarity, entanglement, magic, coherence and purity, where we regard pure states and unitaries (except for purity where we regard mixed states and channels). Here, we assume $\beta = 0$, $\delta = \Omega(1)$ for the tester and choose a representative measure with the best known protocol for each property. Further details in Appendix L.

Theorem 1 (PRSs and PRUs are not robust to noise (Appendix C))**.** *Any ensemble of unitaries or states subject to a single-qubit depolarizing noise channel* $\Lambda(X) = (1-p)X + p\mathrm{tr}(X)I_1/2$ *can be PRSs and PRUs only with at most* $p = \mathrm{negl}(n)$ *depolarizing probability.*

Theorem 1 is proven via the SWAP test [60]. In particular, any state or unitary subject to a local depolarizing channel with $p = \Omega(1/\mathrm{poly}(n))$ noise probability can be efficiently distinguished from Haar random states or unitaries.

3 Imaginarity of states

Next, we discuss the property of imaginarity. An n-qubit quantum state ρ is non-imaginary or real when all the coefficients in the expansion

$$\rho = \sum_{k,\ell} \rho_{k,\ell} |k\rangle\langle\ell| \tag{1}$$

are real, i.e. $\rho_{k,\ell} \in \mathbb{R}$ for all k, ℓ. Note that here we do not allow for flag qubits that serve as an indicator of imaginarity as used in the rebit model of quantum computation [64]. Further note that imaginarity depends on the chosen canonical basis of the system. For example, redefining the computational basis from $|0\rangle, |1\rangle$ to $|+y\rangle, |-y\rangle$, where $|\pm y\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)$, changes a real state into an imaginary one. Here, we make the usual choice to define imaginarity with respect to the canonical computational basis $|0\rangle$ and $|1\rangle$.

The degree to which a state ρ requires complex numbers can be quantified using measures

of imaginarity such as the robustness of imaginarity [24, 65]

$$R(\rho) = \min_{\tau} \left\{ s \geq 0 : \frac{\rho + s\tau}{1+s} \text{ real} \right\} = \frac{1}{2}\|\rho - \rho^T\|_1 \tag{2}$$

where the minimization is taken over all quantum states τ and $\|A\|_1 = \mathrm{tr}(\sqrt{AA^\dagger})$ denotes the trace norm. We now consider the imaginarity of pure states $\rho = |\psi\rangle\langle\psi|$

$$\mathcal{I}(|\psi\rangle) \equiv R(|\psi\rangle)^2 = 1 - |\langle\psi|\psi^*\rangle|^2 \tag{3}$$

where $\mathcal{I} = 0$ only for real states and $0 \leq \mathcal{I} \leq 1$. Here, $|\psi^*\rangle$ indicates the complex conjugate of $|\psi\rangle$ and we used $\frac{1}{2}\||\psi\rangle\langle\psi| - |\phi\rangle\langle\phi|\|_1 = \sqrt{1 - |\langle\psi|\phi\rangle|^2}$.

When given a polynomial number of copies of a state $|\psi\rangle$ which is promised to be either a non-imaginary state or a state with high imaginarity, can we tell those two cases apart? The answer to this question is negative, i.e. testing the imaginarity of states requires in general exponentially many copies.

Theorem 2 (Imaginarity cannot be efficiently tested for states (Appendix D))**.** *Any tester $\mathcal{A}_\mathcal{I}$ for imaginarity according to Def. 10 for an arbitrary n-qubit state $|\psi\rangle$ requires $t = \Omega(2^{n/2})$ copies of $|\psi\rangle$ for $\delta < 1 - n^2 2^{-n/2}$ and any $\beta < \delta$.*

The proof idea is that Haar random states are highly imaginary, while being indistinguishable from an ensemble of real states.

For the real states, we use the recently introduced K-subset phase states [17]

$$|\psi_{S,f}\rangle = \frac{1}{\sqrt{K}} \sum_{x \in S} (-1)^{f(x)} |x\rangle \tag{4}$$

where S is a set of binary strings $\{0,1\}^n$ with $K = |S|$ elements and $f : \{0,1\}^n \to \{0,1\}$ a binary phase function. The ensemble of Eq. (4) over all f has been shown to be pseudorandom [16, 17]. The ensemble of Haar random states and the ensemble of phase states of all binary phase functions with $K = \omega(\log(n))$ are indistinguishable with polynomial copies [17], which we apply to prove Theorem 2.

Thus, PRSs can assume any value of imaginarity as it cannot be tested efficiently, which is evidenced by the existence of both real [16] and imaginary PRSs [1]. Note that alternative constructions of real-valued PRSs exist, which do not require negative amplitudes [66, 67].

While testing imaginarity is inefficient in general, the scaling is indeed better than tomography as we show with an explicit algorithm in Appendix E.

Also note that when we have access to both $|\psi\rangle$ and its complex conjugate $|\psi^*\rangle$, we can simply use the SWAP test to efficiently evaluate Eq. (3) using $O(1)$ samples. Thus, access to the complex conjugate gives an exponential advantage in imaginarity testing.

Corollary 1 (Exponential separation in testing imaginarity with conjugate states)**.** *Testing the imaginarity of arbitrary state $|\psi\rangle$ with access to its complex conjugate $|\psi^*\rangle$ requires $O(1)$ copies, while without $|\psi^*\rangle$ one requires $t = \Omega(2^{n/2})$ copies.*

Now, let us assume that we are not given arbitrary states, but states drawn from a restricted class of states. In this case, efficient algorithms to test imaginarity can exist. In particular, we can efficiently test the imaginarity of pure stabilizer states, i.e. states that are generated by compositions of the CNOT, Hadamard, and S gates applied to computational basis states [68]:

Claim 1 (Efficient measurement of imaginarity for stabilizer states (Appendix F))**.** *For an n-qubit stabilizer state $|\chi\rangle \in \mathrm{STAB}$, imaginarity is given by*

$$\mathcal{I}_{\mathrm{STAB}}(|\chi\rangle) = 1 - 2^{-n} \sum_{\sigma \in \mathcal{P}} |\langle\chi|\sigma|\chi^*\rangle|^2 |\langle\chi|\sigma|\chi\rangle|^2 \tag{5}$$

where $\mathcal{P}$ is the set of all n-qubit Pauli strings with phase $+1$. $\mathcal{I}_{\mathrm{STAB}}(|\chi\rangle)$ can be efficiently measured within additive precision δ with a failure probability ν using at most $t = O(\delta^{-2}\log(1/\nu))$ copies.

4 Imaginarity of unitaries

A channel is real if and only if its associated Choi-state is a real state [65]. Using this fact, we define imaginarity for an n-qubit unitary U via its Choi-state $U \otimes I|\Phi\rangle$ where $|\Phi\rangle = 2^{-n/2}\sum_{k=0}^{2^n-1} |k\rangle|k\rangle$ is the maximally entangled state

$$\mathcal{I}_{\mathrm{p}}(U) \equiv \mathcal{I}(U \otimes I|\Phi\rangle) = 1 - 4^{-n} \left|\mathrm{tr}(U^\dagger U^*)\right|^2 . \tag{6}$$

In contrast to states, imaginarity of unitaries can be efficiently tested:

Claim 2 (Imaginarity of unitaries can be measured efficiently (Appendix G or [62]))**.** *Measuring $\mathcal{I}_p(U)$ within additive precision δ with a failure probability ν requires at most $t = O(\delta^{-2}\log(1/\nu))$ queries to U.*

The efficient algorithm to measure $\mathcal{I}_\mathrm{p}$ is found in Appendix G or [62]. An earlier quantum interactive proof to distinguish Haar random complex and orthogonal unitaries is given in Ref. [69]. This surprising difference between unitaries and states can be intuitively understood with the following argument: Efficient measurement of imaginarity for a state $|\psi\rangle$ requires the complex conjugate $|\psi^*\rangle$ which cannot be efficiently prepared when having only access to copies of $|\psi\rangle$ (see also Corollary 6). In contrast, for unitary U one can use the ricochet property $(U\otimes I_n)|\Phi\rangle = (I_n\otimes(U^*)^\dagger)|\Phi\rangle$ to gain indirect access to the complex conjugate U^*.

Theorem 3 (Appendix H)**.** *PRUs require imaginarity $\mathcal{I}_p = 1 - \mathrm{negl}(n)$.*

Theorem 3 is proven using Claim 2. In particular, one can efficiently distinguish Haar random unitaries from low-imaginarity unitaries, which excludes them from being PRUs.

Corollary 2. *Real unitaries are not pseudorandom.*

Corollary 2 follows from Theorem 3 by considering the special case when U satisfies $\mathcal{I}_\mathrm{p}(U) = 0$. In particular, pseudorandom permutations, which were proposed as candidates for PRUs in Ref. [1], cannot be PRUs due to Corollary 2. Additionally, we note that Corollary 2 does not apply to pseudorandom isometries, which can be implemented using only real operations [15, 57]. Moreover, we note that by assuming a weaker notion of security where the unitary is applied on non-entangled input states, one can achieve somewhat secure PRUs that are real-valued [56].

5 Coherence of states

Coherence measures the "amount" of off-diagonal coefficients of a state ρ. One measure of coherence is the relative entropy of coherence, which is defined as [30, 31]

$$\mathcal{C}(\rho) = \mathrm{tr}(\rho\ln(\rho)) - \mathrm{tr}(\rho_\mathrm{d}\ln(\rho_\mathrm{d})) = -\sum_k |c_k|^2\ln(|c_k|^2)\,, \tag{7}$$

where $\rho_\mathrm{d} = \sum_k \langle k|\rho|k\rangle |k\rangle\langle k|$ is obtained by ρ by keeping only the diagonal coefficients and setting all other entries to zero, and c_k are the amplitudes of $|\psi\rangle = \sum_k c_k|k\rangle$ in the computational basis. Coherence is minimal for computational basis states $\mathcal{C}(|k\rangle) = 0$ and maximal for $|+\rangle^{\otimes n}$, $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ with $\mathcal{C}(|+\rangle^{\otimes n}) = n\ln(2)$. We now test for the property of coherence:

Theorem 4 (Lower bound on coherence testing for states (Appendix I))**.** *Any tester $\mathcal{A}_\mathcal{C}$ for relative entropy of coherence $\mathcal{C}$ according to Def. 10 for an arbitrary n-qubit state $|\psi\rangle$ requires $t = \Omega(2^{\beta/2})$ for $\delta < n\ln(2) - 1$ and any $\beta < \delta$.*

The proof idea for Theorem 4 is similar to the one for imaginarity testing. First, we construct an ensemble of low coherence states via the ensemble of K-subset phase states with $\beta = \ln(K)$. Next, we build the ensemble of highly coherent states $|\psi\rangle \in \mathcal{E}_{\mathcal{C}\geq\delta}$ with coherence $\mathcal{C}(|\psi\rangle) \geq \delta$ which cannot be efficiently distinguished from Haar random states [70]. We then use the closeness between Haar random states and subset phase states [17] to prove Theorem 4.

Claim 3 (Appendix I)**.** *PRSs require $\mathcal{C} = \omega(\log(n))$ relative entropy of coherence.*

To prove Claim 3, we provide an efficient measurement scheme for the coherence measure based on the Hilbert-Schmidt norm $\sum_k |c_k|^4$ [30]. Together with Jensen's inequality, this implies that one can efficiently distinguish Haar random states from states with $\mathcal{C} = O(\log(n))$.

Corollary 3. *States with polynomial support on the computational basis, i.e. $|\psi\rangle = \sum_{k\in|S|} c_k|k\rangle$ with $|S| = \mathrm{poly}(n)$, are not pseudorandom.*

To show Corollary 3, assume a state $|\psi\rangle = \sum_{k\in|S|} c_k|k\rangle$ with $|S| = O(n^c)$ with $c > 0$. Then, we have for the max relative entropy $\ln(\mathrm{card}(|\psi\rangle)) = O(\log(n))$, where card(.) counts the non-zero coefficients of $|\psi\rangle$ in the computational basis. The state cannot be a PRS due to $\ln(\mathrm{card}(|\psi\rangle)) \geq \mathcal{C}(|\psi\rangle)$ and Claim 3.

6 Coherence power of unitaries

Similar to the relative entropy of coherence for states, one can define the coherence power of unitaries [33]. We introduce the relative entropy of

coherence power as

$$\mathcal{C}_{\mathrm{p}}(U) = -\sum_{k,\ell} 2^{-n} |\langle k|U|\ell\rangle|^2 \ln(|\langle k|U|\ell\rangle|^2) \quad (8)$$

with $0 \leq \mathcal{C}_{\mathrm{p}} \leq n\ln(2)$. It measures the amount of off-diagonal coefficients of unitaries, where diagonal unitaries have $\mathcal{C}_{\mathrm{p}}(U_{\mathrm{diag}}) = 0$ and for the Hadamard gate H we have $\mathcal{C}_{\mathrm{p}}(H^{\otimes n}) = n\ln(2)$.

Theorem 5 (PRUs need coherence (Appendix J))**.** *PRUs require $\mathcal{C}_p = \omega(\log(n))$ relative entropy of coherence power.*

The proof idea is to efficiently measure $\sum_{kl} 2^{-n} |\langle k|U|\ell\rangle|^4$ (see Appendix J or [33]). Using Jensen's inequality, this implies that one can efficiently distinguish unitaries with $\mathcal{C}_{\mathrm{p}} = O(\log(n))$ from Haar random unitaries.

Corollary 4. *Sparse unitaries, i.e. unitaries where rows or columns have at most poly(n) non-zero entries, cannot be pseudorandom.*

To prove Corollary 4, we assume sparse unitaries U_{sp} with $O(n^c)$ non-zero entries per column and $c > 0$. Thus, the max relative entropy is given by $\ln(2^{-n}\mathrm{card}(U_{\mathrm{sp}})) = O(\log(n))$ where $\mathrm{card}(\cdot)$ counts the number of non-zero coefficients. From the inequalities between Rényi entropies, we have $\ln(2^{-n}\mathrm{card}(U_{\mathrm{sp}})) \geq \mathcal{C}_{\mathrm{p}}(U_{\mathrm{sp}})$, which according to Theorem 5 precludes PRUs.

7 Pseudoresource

Quantum resources such as entanglement or coherence are essential ingredients to run quantum computers and devices. We ask now whether 'high'-resource state ensembles can be mimicked using another 'low´-resource ensemble? This concept was first introduced for the resource of entanglement as pseudoentanglement in Ref. [17]. Pseudoentanglement describes ensembles of states which are computationally indistinguishable, yet have widely different entanglement.

We generalise this concept to *pseudoresources* for arbitrary resource measures $Q(|\psi\rangle)$ with $0 \leq Q \leq Q_{\max}(n)$, where $Q_{\max}(n)$ is the maximal value of Q. For formal definition see Def. 9 A pseudoresource ensemble consists of two state ensembles: The first ensemble $|\psi_k\rangle$ has a high amount of the resource $Q(|\psi_k\rangle) = f(n)$. The second ensemble $|\phi_k\rangle$ has a lower amount of the resource $Q(|\psi_k\rangle) = g(n)$ while being computationally indistinguishable from the first ensemble, where $f(n) \geq g(n)$ are two functions. Thus, a pseudoresource ensemble can masquerade as having $f(n)$ of the resource, while actually containing only $g(n)$. The difference in resource between the two ensembles is called the pseudoresource gap $f(n)$ vs $g(n)$. We summarize results for various pseudoresources in Table 2.

Next, we introduce three new types of pseudoresources: Pseudocoherence, pseudoimaginarity and pseudopurity.

We find pseudocoherent ensembles with a pseuodcoherence gap of $f(n) = \Theta(n)$ vs $g(n) = \log(n)$, by tuning the rank of the subset phase states. This shows that one can mimic extensive coherence with only logarithmic coherent states. As coherence can be enhanced independently of entanglement and magic via LOCC and Clifford operations, pseudocoherence can be tuned independently of pseudoentanglement and pseudomagic.

In contrast, for purity $\mathrm{tr}(\rho^2)$, the pseudopurity gap is exponentially small with $g(n) = 1 - O(2^{-n})$ vs $f(n) = 1$ as any state with non-negligible noise is not pseudorandom.

For imaginarity, we find that the pseudoimaginarity gap is maximal with $f(n) = 1 - O(2^{-n})$ vs $g(n) = 0$. In particular, subset phase states have zero imaginarity, while a class of imaginary pseudorandom states [1] have asymptotically maximal imaginarity.

We categorize three classes of pseudoresources using the pseudoresource gap ratio $\Delta = (f(n) - g(n))/Q_{\max}$, where $0 \leq \Delta \leq 1$. Δ indicates the degree to which a resource can be masqueraded using pseudorandom states. First, pseudopurity has $\Delta = O(2^{-n})$, indicating that only maximally pure states can be pseudorandom. Second, for pseudoentanglement, pseudomagic and pseudocoherence we find $\Delta = 1 - \omega(\log(n)/n)$. For this class of resources a low, but non-negligible amount of the resource is needed such that pseudorandom states can masquerade as high-resource states. The third class, which consists of pseudoimaginarity, any amount of imaginarity can be mimicked by pseudorandom states. Thus, this resource can be freely chosen for pseudorandom states.

Resource Q	$f(n)$	$g(n)$	Δ
Purity	1	$1-O(2^{-n})$	$O(2^{-n})$
Entanglement [17]	$\Theta(n)$	$\omega(\log(n))$	$1-\omega(\log(n)/n)$
Magic [71]	$\Theta(n)$	$\omega(\log(n))$	$1-\omega(\log(n)/n)$
Coherence	$\Theta(n)$	$\omega(\log(n))$	$1-\omega(\log(n)/n)$
Imaginarity	$1-O(2^{-n})$	0	$1-O(2^{-n})$

Table 2: Maximal pseudoresource gap $f(n)$ vs $g(n)$ of pure states (except for purity) for different resources Q. We also show the pseudoresource gap ratio $\Delta = (f(n)-g(n))/Q_{\max}$ with respect to the maximal value of the resource $Q_{\max}$.

8 Separation between PRSS and PRUs

Any PRU is also a PRSS [14, 15]. However, the reverse question whether any PRSS is also a PRU has been left as an open question [14, 15], which we will proceed to answer negatively:

Theorem 6 (Separation between PRSS and PRU)**.** *PRSS are strictly weaker than PRSS. In particular, there are PRSS which are not PRUs.*

In Ref. [14] (Def. 5.4), a class of real-valued PRSS based on Kac's walk is proposed. It uses the permutation $\sigma \in S_{2^n}$ over n qubits, and real-valued rotations with discretized rotation angles. This PRSS is not a PRU due to a lack of imaginarity, which follows directly from Thm. 3.

9 Transformation limits

Universal quantum computation with qubits usually requires complex-valued operations and states. However, one can also realize the same universal quantum computations using $n+1$ rebits, i.e. qubits with only real coefficients which support only real states and real unitaries [64, 72–74]. For rebits, the role of imaginarity is mimicked by adding an ancilla rebit which acts as a flag that records the real and imaginary parts of the amplitudes of the quantum states separately. In particular, while a complex n-qubit state with coefficients $a_k, b_k \in \mathbb{R}$ is written as

$$|\psi\rangle = \sum_{k=0}^{2^n-1} (a_k + ib_k)|k\rangle \tag{9}$$

the corresponding $(n+1)$-rebit state is given by

$$|\psi_{\mathrm{R}}\rangle = \sum_{k=0}^{2^n-1} (a_k|k\rangle|R\rangle + b_k|k\rangle|I\rangle) \tag{10}$$

where $|R\rangle$, $|I\rangle$ are the computational flag states for real and imaginary value respectively. The rebit representation can naturally perform additional non-linear operations not commonly associated with the usual qubit quantum computing model, and thus it would be highly interesting to transform between the qubit and rebit representations [72]. However, as we show below, qubit-to-rebit transformations are inefficient, in contrast to the reverse process, for which we give an efficient protocol.

Corollary 5. *There is no algorithm $\mathcal{T}(|\psi\rangle^{\otimes t}) \to |\psi_R\rangle$ using $t = \mathrm{poly}(n)$ copies of n-qubit state Eq. (9) that returns the $(n+1)$-rebit state Eq. (10) with non-negligible probability.*

Corollary 5 can be easily seen from the following: In the rebit representation $|\psi_{\mathrm{R}}\rangle$, we can efficiently measure the corresponding imaginarity of the qubit representation $|\psi\rangle$ via the purity of the flag rebit (Appendix K)

$$\mathcal{I}(|\psi\rangle) \equiv 2(1-\mathrm{tr}(\mathrm{tr}_{1:n}(|\psi_{\mathrm{R}}\rangle\langle\psi_{\mathrm{R}}|)^2))\,, \tag{11}$$

where $\mathrm{tr}_{1:n}(\cdot)$ is the partial trace over all rebits except the $(n+1)$-th rebit. Now, suppose for the sake of contradiction that $\mathcal{T}$ is efficient. Then, we could efficiently transform $|\psi\rangle$ into $|\psi_{\mathrm{R}}\rangle$ and efficiently measure the imaginarity of $|\psi\rangle$ via $|\psi_{\mathrm{R}}\rangle$. However, the efficient measurement of imaginarity contradicts Theorem 2. Therefore, $\mathcal{T}$ must be inefficient.

Claim 4. *There is an efficient algorithm $\mathcal{T}_R(|\psi_R\rangle^{\otimes t}) \to |\psi\rangle$ t copies of $(n+1)$-rebit state Eq. (10) that returns n-qubit state Eq. (9) with exponentially small failure probability $O(2^{-t})$.*

Algorithm $\mathcal{T}_{\mathrm{R}}$ uses the operator $\Pi = I_n \otimes \frac{1}{\sqrt{2}}(\langle R| + i\langle I|)$ via $|\psi\rangle = \sqrt{2}\Pi|\psi_{\mathrm{R}}\rangle$, where I_n is

the n-qubit identity operator [72]. Π is implemented efficiently by measuring the flag rebit in the $\{\frac{1}{\sqrt{2}}(|R\rangle+i|I\rangle), \frac{1}{\sqrt{2}}(|R\rangle-i|I\rangle)\}$ basis and post-selecting $\frac{1}{\sqrt{2}}(|R\rangle + i|I\rangle)$ with success probability $\|\Pi|\psi_{\mathrm{R}}\rangle\| = \frac{1}{2}$. By repeating the above algorithm with t copies, one succeeds at least once with failure probability 2^{-t}.

Finally, we give a short proof that the complex conjugation of states is inefficient. This was previously proven using more involved techniques [75, 76]:

Corollary 6. *There is no efficient quantum algorithm with access to* $\mathrm{poly}(n)$ *copies of* $|\psi\rangle$ *that returns the complex conjugate* $|\psi^*\rangle$ *with non-negligible probability.*

One can show this as follows: When given t copies of $|\psi\rangle$ and $|\psi^*\rangle$, one can efficiently test imaginarity $\mathcal{I}(|\psi\rangle)$ up to additive accuracy $O(1/\sqrt{t})$ via the SWAP test. This scheme can be used as a property tester for imaginarity, i.e. one can test with high probability whether any given state has zero imaginarity or high imaginarity. Thus, efficient access to the complex conjugate state contradicts Theorem 2, implying that $|\psi^*\rangle$ cannot be efficiently prepared from $|\psi\rangle$.

10 Conclusion

We have studied the limits of testing purity, imaginarity and coherence. This, in turn, places fundamental limits on the properties of PRSs and PRUs as a function of qubit number n. Our work builds upon the fundamental and widely acknowledged principle that a pseudorandom object possesses all the efficiently verifiable properties inherent in its random counterpart [77].

PRSs and PRUs are not robust to noise, and can tolerate depolarizing noise with at most negligible probability. Thus, it is not possible to generate PRSs on noisy intermediate-scale quantum computers [78]. Further, early fault-tolerant quantum computers [79, 80], i.e. quantum computers with limited error correction where not all errors are exponentially suppressed, are expected to be unable to generate PRSs.

We further show that PRSs and PRUs must have a $\mathcal{C} = \omega(\log(n))$ relative entropy of coherence (power), which implies that PRUs are not sparse, requiring $\omega(\log(n))$ coherent operations such as the Hadamard gates to be generated.

Does the description of quantum mechanics require complex numbers, or does it suffice to only use real numbers to achieve arbitrary tasks? For quantum communication tasks, it has been shown that complex numbers are indeed necessary [24–26]. We now show that quantum randomness also requires complex numbers, however with a subtle catch. In particular, we show that PRUs must not be real and require $\mathcal{I}_{\mathrm{p}} = 1 - \mathrm{negl}(n)$ imaginarity. This implies that a real-valued description of quantum information is unable to generate quantum randomness for unitaries, and complex numbers are indeed necessary. In contrast, PRSs (and PRSSs) have no restrictions on imaginarity. Thus, randomness on the level of quantum states does not need complex numbers, and a real-valued quantum theory suffices to generate states which look completely random. This reveals a fundamental difference of the role of complex numbers for operations and states. Given recent efficient constructions of real PRSs [16], some-what secure real PRUs [56], and complex PRUs [12, 13], the relationship of randomness and complex numbers can be directly probed in experiment.

We introduce pseudoresource as the ability of a pseudorandom state ensemble with a low amount of a given resource to masquerade as a high-resource ensemble. We observe that pseudoresource behaves fundamentally different depending on the resource: For pseudocoherence (as well as pseudoentanglement and pseudomagic), we find a large, but non-maximal pseudoresource gap between low and high coherence ensembles. For pseudoimaginarity, the gap is maximal, while for pseudopurity the gap is exponentially small. Thus, not all resources can be effectively masqueraded using low-resource states. It would be interesting to draw a fundamental connection between resource theories and the pseudoresource gap. Further, it would be interesting to relate pseudoresources to state preparation complexity [81].

Various notions of pseudorandomness exist, and their relative relationships is not well understood. Here, we establish two new results: First, we show that creating PRUs is more demanding than generating PRSs, which was conjectured in Ref. [1]. In particular, while real and diagonal unitaries applied to a product state can create the PRSs of Eq. (4) [1], we show that these unitaries

cannot be pseudorandom themselves, providing a separation in the generation complexity of PRSs and PRUs. Second, we show that PRSS are not always PRUs, proving that there is indeed a clear gap between the two notions of pseudorandomness which was alluded in Refs. [14, 15].

We show that access to the complex conjugate of a state gives an exponential advantage in imaginarity testing. Thus, the ability to conjugate (which in general is exponentially difficult) poses a powerful resource in property testing, which similarly has been shown for learning problems [82, 83].

Our work also sheds light on the relationship between rebit and qubit models of quantum computing. In particular, we show that one can efficiently transform from rebit to a qubit model of quantum computing, while the inverse transformation is not efficient.

Finally, we note that for pure states and unitaries, one can efficiently test quantum properties such as entanglement [47, 61, 84], magic [48, 85], coherence [33], purity [60] and imaginarity [62], with the sole exception being the imaginarity of states (see Appendix L). This curious outlier highlights the special character of the resource theory of imaginarity, which warrants further studies.

Acknowledgments

D.E.K. acknowledges funding support from the National Research Foundation, Singapore, and the Agency for Science, Technology and Research (A*STAR), Singapore, under its Quantum Engineering Programme (NRF2021-QEP2-02-P03); A*STAR C230917003; and A*STAR under the Central Research Fund (CRF) Award for Use-Inspired Basic Research (UIBR) and the Quantum Innovation Centre (Q.InC) Strategic Research and Translational Thrust. We thank Nikhil Bansal, Naresh Goud Boddu, Atul Singh Arora and Rahul Jain for various discussions. We also extend our thanks to the anonymous referee for pointing out the candidate construction for PRUs from Ref. [1], which is ruled out as a result of our findings.

References

[1] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. "Pseudorandom quantum states". In Annual International Cryptology Conference. Pages 126–152. Springer (2018).

[2] Joseph Emerson, Yaakov S Weinstein, Marcos Saraceno, Seth Lloyd, and David G Cory. "Pseudo-random unitary operators for quantum information processing". Science **302**, 2098–2100 (2003).

[3] Fernando G. S. L. Brandão, Aram W. Harrow, and Michał Horodecki. "Efficient quantum pseudorandomness". Phys. Rev. Lett. **116**, 170502 (2016).

[4] Fernando G S L Brandao, Aram W Harrow, and Michał Horodecki. "Local random quantum circuits are approximate polynomial-designs". Communications in Mathematical Physics **346**, 397–434 (2016).

[5] Yoshifumi Nakata, Christoph Hirche, Masato Koashi, and Andreas Winter. "Efficient quantum pseudorandomness with nearly time-independent Hamiltonian dynamics". Phys. Rev. X **7**, 021006 (2017).

[6] Valerio Scarani. "Guaranteed randomness". Nature **464**, 988–989 (2010).

[7] Yun Zhi Law, Jean-Daniel Bancal, Valerio Scarani, et al. "Quantum randomness extraction for various levels of characterization of the devices". Journal of Physics A: Mathematical and Theoretical **47**, 424028 (2014).

[8] Miguel Herrero-Collantes and Juan Carlos Garcia-Escartin. "Quantum random number generators". Reviews of Modern Physics **89**, 015004 (2017).

[9] Antonio Acín and Lluis Masanes. "Certified randomness in quantum physics". Nature **540**, 213–219 (2016).

[10] Manabendra Nath Bera, Antonio Acín, Marek Kuś, Morgan W Mitchell, and Maciej Lewenstein. "Randomness in quantum mechanics: philosophy, physics and technology". Reports on Progress in Physics **80**, 124001 (2017).

[11] Cristian S Calude and Karl Svozil. "Quantum randomness and value indefiniteness". Advanced Science Letters **1**, 165–168 (2008).

[12] Thomas Schuster, Jonas Haferkamp, and Hsin-Yuan Huang. "Random unitaries in extremely low depth". arXiv preprint arXiv:2407.07754 (2024).

[13] Fermi Ma and Hsin-Yuan Huang. "How to construct random unitaries". arXiv preprint arXiv:2410.10116 (2024).

[14] Chuhan Lu, Minglong Qin, Fang Song, Penghui Yao, and Mingnan Zhao. "Quantum pseudorandom scramblers". arXiv preprint arXiv:2309.08941 (2023).

[15] Prabhanjan Ananth, Aditya Gulati, Fatih Kaleoglu, and Yao-Ting Lin. "Pseudorandom isometries". In Annual International Conference on the Theory and Applications of Cryptographic Techniques. Pages 226–254. Springer (2024).

[16] Zvika Brakerski and Omri Shmueli. "(Pseudo) random quantum states with binary phase". In Theory of Cryptography Conference. Pages 229–250. Springer (2019).

[17] Scott Aaronson, Adam Bouland, Bill Fefferman, Soumik Ghosh, Umesh Vazirani, Chenyi Zhang, and Zixin Zhou. "Quantum Pseudoentanglement". In Venkatesan Guruswami, editor, 15th Innovations in Theoretical Computer Science Conference (ITCS 2024). Volume 287 of Leibniz International Proceedings in Informatics (LIPIcs), pages 2:1–2:21. Dagstuhl, Germany (2024). Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[18] William Kretschmer. "Quantum Pseudorandomness and Classical Complexity". In Min-Hsiu Hsieh, editor, 16th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2021). Volume 197 of Leibniz International Proceedings in Informatics (LIPIcs), pages 2:1–2:20. Dagstuhl, Germany (2021). Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[19] Prabhanjan Ananth, Luowen Qian, and Henry Yuen. "Cryptography from pseudorandom quantum states". In Advances in Cryptology–CRYPTO 2022: 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15–18, 2022, Proceedings, Part I. Pages 208–236. Springer (2022).

[20] Prabhanjan Ananth, Aditya Gulati, Luowen Qian, and Henry Yuen. "Pseudorandom (function-like) quantum state generators: New definitions and applications". In Theory of Cryptography Conference. Pages 237–265. Springer (2022).

[21] Tomoyuki Morimae and Takashi Yamakawa. "Quantum commitments and signatures without one-way functions". In Advances in Cryptology–CRYPTO 2022: 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15–18, 2022, Proceedings, Part I. Pages 269–295. Springer (2022).

[22] Prabhanjan Ananth, Yao-Ting Lin, and Henry Yuen. "Pseudorandom Strings from Pseudorandom Quantum States". In Venkatesan Guruswami, editor, 15th Innovations in Theoretical Computer Science Conference (ITCS 2024). Volume 287 of Leibniz International Proceedings in Informatics (LIPIcs), pages 6:1–6:22. Dagstuhl, Germany (2024). Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[23] Sabee Grewal, Vishnu Iyer, William Kretschmer, and Daniel Liang. "Improved stabilizer estimation via Bell difference sampling". In Proceedings of the 56th Annual ACM Symposium on Theory of Computing. Page 1352–1363. STOC 2024New York, NY, USA (2024). Association for Computing Machinery.

[24] Kang-Da Wu, Tulja Varun Kondra, Swapan Rana, Carlo Maria Scandolo, Guo-Yong Xiang, Chuan-Feng Li, Guang-Can Guo, and Alexander Streltsov. "Resource theory of imaginarity: Quantification and state conversion". Phys. Rev. A **103**, 032401 (2021).

[25] Tulja Varun Kondra, Chandan Datta, and Alexander Streltsov. "Real quantum operations and state transformations". New Journal of Physics **25**, 093043 (2023).

[26] Ming-Cheng Chen, Can Wang, Feng-Ming Liu, Jian-Wen Wang, Chong Ying, Zhong-Xia Shang, Yulin Wu, M. Gong, H. Deng, F.-T. Liang, Qiang Zhang, Cheng-Zhi Peng, Xiaobo Zhu, Adán Cabello, Chao-Yang Lu, and Jian-Wei Pan. "Ruling out real-valued standard formalism of quantum theory". Phys. Rev. Lett. **128**, 040403 (2022).

[27] Marc-Olivier Renou, David Trillo, Mirjam Weilenmann, Thinh P Le, Armin Tavakoli,

Nicolas Gisin, Antonio Acín, and Miguel Navascués. "Quantum theory based on real numbers can be experimentally falsified". Nature **600**, 625–629 (2021).

[28] Kang-Da Wu, Tulja Varun Kondra, Swapan Rana, Carlo Maria Scandolo, Guo-Yong Xiang, Chuan-Feng Li, Guang-Can Guo, and Alexander Streltsov. "Operational resource theory of imaginarity". Phys. Rev. Lett. **126**, 090401 (2021).

[29] Zheng-Da Li, Ya-Li Mao, Mirjam Weilenmann, Armin Tavakoli, Hu Chen, Lixin Feng, Sheng-Jun Yang, Marc-Olivier Renou, David Trillo, Thinh P. Le, et al. "Testing real quantum theory in an optical quantum network". Phys. Rev. Lett. **128**, 040402 (2022).

[30] T. Baumgratz, M. Cramer, and M. B. Plenio. "Quantifying coherence". Phys. Rev. Lett. **113**, 140401 (2014).

[31] Alexander Streltsov, Gerardo Adesso, and Martin B. Plenio. "Colloquium: Quantum coherence as a resource". Rev. Mod. Phys. **89**, 041003 (2017).

[32] Kaifeng Bu, Asutosh Kumar, Lin Zhang, and Junde Wu. "Cohering power of quantum operations". Physics Letters A **381**, 1670–1676 (2017).

[33] Paolo Zanardi, Georgios Styliaris, and Lorenzo Campos Venuti. "Coherence-generating power of quantum unitary maps and beyond". Phys. Rev. A **95**, 052306 (2017).

[34] Kaifeng Bu, Uttam Singh, Shao-Ming Fei, Arun Kumar Pati, and Junde Wu. "Maximum relative entropy of coherence: An operational coherence measure". Phys. Rev. Lett. **119**, 150405 (2017).

[35] Kaifeng Bu and Chunhe Xiong. "A note on cohering power and de-cohering power". Quantum Information & Computation **17**, 1206–1220 (2017).

[36] Alexander Streltsov, Uttam Singh, Himadri Shekhar Dhar, Manabendra Nath Bera, and Gerardo Adesso. "Measuring quantum coherence with entanglement". Phys. Rev. Lett. **115**, 020403 (2015).

[37] Eric Chitambar and Min-Hsiu Hsieh. "Relating the resource theories of entanglement and quantum coherence". Phys. Rev. Lett. **117**, 020402 (2016).

[38] Kaifeng Bu, Roy J Garcia, Arthur Jaffe, Dax Enshan Koh, and Lu Li. "Complexity of quantum circuits via sensitivity, magic, and coherence". Communications in Mathematical Physics **405**, 161 (2024).

[39] Mark Hillery. "Coherence as a resource in decision problems: The Deutsch-Jozsa algorithm and a variation". Phys. Rev. A **93**, 012111 (2016).

[40] J M Matera, D Egloff, N Killoran, and M B Plenio. "Coherent control of quantum systems as a resource theory". Quantum Science and Technology **1**, 01LT01 (2016).

[41] Hai-Long Shi, Si-Yuan Liu, Xiao-Hui Wang, Wen-Li Yang, Zhan-Ying Yang, and Heng Fan. "Coherence depletion in the Grover quantum search algorithm". Phys. Rev. A **95**, 032307 (2017).

[42] Guoming Wang, Dax Enshan Koh, Peter D. Johnson, and Yudong Cao. "Minimizing estimation runtime on noisy quantum computers". PRX Quantum **2**, 010346 (2021).

[43] Ronitt Rubinfeld and Madhu Sudan. "Robust characterizations of polynomials with applications to program testing". SIAM Journal on Computing **25**, 252–271 (1996).

[44] Oded Goldreich, Shari Goldwasser, and Dana Ron. "Property testing and its connection to learning and approximation". Journal of the ACM (JACM) **45**, 653–750 (1998).

[45] Harry Buhrman, Lance Fortnow, Ilan Newman, and Hein Röhrig. "Quantum property testing". SIAM Journal on Computing **37**, 1387–1400 (2008).

[46] Ashley Montanaro and Ronald de Wolf. "A survey of quantum property testing". Pages 1–81. Number 7 in Graduate Surveys. Theory of Computing Library. (2016).

[47] Aram W Harrow and Ashley Montanaro. "Testing product states, quantum Merlin-Arthur games and tensor optimization". Journal of the ACM (JACM) **60**, 1–43 (2013).

[48] David Gross, Sepehr Nezami, and Michael Walter. "Schur–Weyl duality for the Clifford group with applications: Property testing, a robust Hudson theorem, and de Finetti representations". Communications in Mathematical Physics **385**, 1325–1393 (2021).

[49] Thomas Chen, Shivam Nadimpalli, and Henry Yuen. "Testing and learning quantum juntas nearly optimally". In Proceedings of the 2023 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA). Pages 1163–1185. SIAM (2023).

[50] Adrian She and Henry Yuen. "Unitary Property Testing Lower Bounds by Polynomials". In Yael Tauman Kalai, editor, 14th Innovations in Theoretical Computer Science Conference (ITCS 2023). Volume 251 of Leibniz International Proceedings in Informatics (LIPIcs), pages 96:1–96:17. Dagstuhl, Germany (2023). Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[51] Zvika Brakerski, Devika Sharma, and Guy Weissenberg. "Unitary subgroup testing". arXiv preprint arXiv:2104.03591 (2021).

[52] Mehdi Soleimanifar and John Wright. "Testing matrix product states". In Proceedings of the 2022 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA). Pages 1679–1701. SIAM (2022).

[53] Nikhil Bansal, Wai-Keong Mok, Kishor Bharti, Dax Enshan Koh, and Tobias Haug. "Pseudorandom density matrices". PRX Quantum **6**, 020322 (2025).

[54] Chi-Fang Chen, Jordan Docter, Michelle Xu, Adam Bouland, Fernando G.S.L. Brandão, and Patrick Hayden. "Efficient unitary designs from random sums and permutations". In 2024 IEEE 65th Annual Symposium on Foundations of Computer Science (FOCS). Pages 476–484. (2024).

[55] Tony Metger, Alexander Poremba, Makrand Sinha, and Henry Yuen. "Pseudorandom unitaries with non-adaptive security". arXiv preprint arXiv:2402.14803 (2024).

[56] Zvika Brakerski and Nir Magrafta. "Real-valued somewhat-pseudorandom unitaries". arXiv preprint arXiv:2403.16704 (2024).

[57] Tony Metger, Alexander Poremba, Makrand Sinha, and Henry Yuen. "Simple constructions of linear-depth t-designs and pseudorandom unitaries". arXiv preprint arXiv:2404.12647 (2024).

[58] Eric Chitambar and Gilad Gour. "Quantum resource theories". Rev. Mod. Phys. **91**, 025001 (2019).

[59] Victor Veitch, S A Hamed Mousavian, Daniel Gottesman, and Joseph Emerson. "The resource theory of stabilizer quantum computation". New Journal of Physics **16**, 013009 (2014).

[60] Adriano Barenco, Andre Berthiaume, David Deutsch, Artur Ekert, Richard Jozsa, and Chiara Macchiavello. "Stabilization of quantum computations by symmetrization". SIAM Journal on Computing **26**, 1541–1557 (1997).

[61] Artur K. Ekert, Carolina Moura Alves, Daniel K. L. Oi, Michał Horodecki, Paweł Horodecki, and L. C. Kwek. "Direct estimations of linear and nonlinear functionals of a quantum state". Phys. Rev. Lett. **88**, 217901 (2002).

[62] Hsin-Yuan Huang, Michael Broughton, Jordan Cotler, Sitan Chen, Jerry Li, Masoud Mohseni, Hartmut Neven, Ryan Babbush, Richard Kueng, John Preskill, et al. "Quantum advantage in learning from experiments". Science **376**, 1182–1186 (2022).

[63] Michael A Nielsen and Isaac L Chuang. "Quantum computation and quantum information". Cambridge University Press. (2010).

[64] Terry Rudolph and Lov Grover. "A 2 rebit gate universal for quantum computing". arXiv preprint quant-ph/0210187 (2002).

[65] Alexander Hickey and Gilad Gour. "Quantifying the imaginarity of quantum mechanics". Journal of Physics A: Mathematical and Theoretical **51**, 414009 (2018).

[66] Tudor Giurgica-Tiron and Adam Bouland. "Pseudorandomness from subset states". arXiv preprint arXiv:2312.09206 (2023).

[67] Fernando Granha Jeronimo, Nir Magrafta, and Pei Wu. "Pseudorandom and pseudoentangled states from subset states". arXiv preprint arXiv:2312.15285 (2023).

[68] Daniel Gottesman. "The Heisenberg representation of quantum computers". Group22: Proceedings of the XXII International Colloquium on Group Theoretical Methods in PhysicsPages 32–43 (1999). url: doi.org/10.48550/arXiv.quant-ph/9807006.

[69] Dorit Aharonov, Jordan Cotler, and Xiao-Liang Qi. "Quantum algorithmic mea-

surement". Nature communications **13**, 887 (2022).

[70] Uttam Singh, Lin Zhang, and Arun Kumar Pati. "Average coherence and its typicality for random pure states". Phys. Rev. A **93**, 032125 (2016).

[71] Andi Gu, Lorenzo Leone, Soumik Ghosh, Jens Eisert, Susanne F. Yelin, and Yihui Quek. "Pseudomagic quantum states". Phys. Rev. Lett. **132**, 210602 (2024).

[72] Dax Enshan Koh, Murphy Yuezhen Niu, and Theodore J Yoder. "Quantum simulation from the bottom up: the case of rebits". Journal of Physics A: Mathematical and Theoretical **51**, 195302 (2018).

[73] Matthew McKague. "On the power quantum computation over real Hilbert spaces". International Journal of Quantum Information **11**, 1350001 (2013).

[74] Nicolas Delfosse, Philippe Allard Guerin, Jacob Bian, and Robert Raussendorf. "Wigner function negativity and contextuality in quantum computation on rebits". Phys. Rev. X **5**, 021003 (2015).

[75] Yuxiang Yang, Giulio Chiribella, and Gerardo Adesso. "Certifying quantumness: Benchmarks for the optimal processing of generalized coherent and squeezed states". Phys. Rev. A **90**, 042319 (2014).

[76] Jisho Miyazaki, Akihito Soeda, and Mio Murao. "Complex conjugation supermap of unitary quantum maps and its universal implementation protocol". Phys. Rev. Res. **1**, 013007 (2019).

[77] Jonathan Katz and Yehuda Lindell. "Introduction to modern cryptography". CRC press. (2020).

[78] Kishor Bharti, Alba Cervera-Lierta, Thi Ha Kyaw, Tobias Haug, Sumner Alperin-Lea, Abhinav Anand, Matthias Degroote, Hermanni Heimonen, Jakob S. Kottmann, Tim Menke, Wai-Keong Mok, Sukin Sim, Leong-Chuan Kwek, and Alán Aspuru-Guzik. "Noisy intermediate-scale quantum algorithms". Rev. Mod. Phys. **94**, 015004 (2022).

[79] Ryan Babbush, Jarrod R McClean, Michael Newman, Craig Gidney, Sergio Boixo, and Hartmut Neven. "Focus beyond quadratic speedups for error-corrected quantum advantage". PRX Quantum **2**, 010103 (2021).

[80] Yasunari Suzuki, Suguru Endo, Keisuke Fujii, and Yuuki Tokunaga. "Quantum error mitigation as a universal error reduction technique: applications from the NISQ to the fault-tolerant quantum computing eras". PRX Quantum **3**, 010345 (2022).

[81] Sabee Grewal, Vishnu Iyer, William Kretschmer, and Daniel Liang. "Pseudoentanglement ain't cheap". arXiv preprint arXiv:2404.00126 (2024).

[82] Ya-Dong Wu, Yan Zhu, Giulio Chiribella, and Nana Liu. "Efficient learning of continuous-variable quantum states". Phys. Rev. Res. **6**, 033280 (2024).

[83] Robbie King, Kianna Wan, and Jarrod R. McClean. "Exponential learning advantages with conjugate states and minimal quantum memory". PRX Quantum **5**, 040301 (2024).

[84] Ariel Bendersky, Juan Pablo Paz, and Marcelo Terra Cunha. "General theory of measurement with two copies of a quantum state". Physical review letters **103**, 040404 (2009).

[85] Tobias Haug and M.S. Kim. "Scalable measures of magic resource for quantum computers". PRX Quantum **4**, 010301 (2023).

[86] Mark Zhandry. "How to construct quantum random functions". Journal of the ACM (JACM) **68**, 1–43 (2021).

[87] Sandu Popescu, Anthony J Short, and Andreas Winter. "Entanglement and the foundations of statistical mechanics". Nature Physics **2**, 754–758 (2006).

[88] Joonwoo Bae and Leong-Chuan Kwek. "Quantum state discrimination and its applications". Journal of Physics A: Mathematical and Theoretical **48**, 083001 (2015).

[89] Ashley Montanaro. "Learning stabilizer states by Bell sampling". arXiv preprint arXiv:1707.04012 (2017).

[90] Otfried Gühne and Géza Tóth. "Entanglement detection". Physics Reports **474**, 1–75 (2009).

[91] Sumeet Khatri, Ryan LaRose, Alexander Poremba, Lukasz Cincio, Andrew T. Sornborger, and Patrick J. Coles. "Quantum-assisted quantum compiling". Quantum **3**, 140 (2019).

[92] Angela Sara Cacciapuoti, Marcello Caleffi, Rodney Van Meter, and Lajos Hanzo.

"When entanglement meets classical communications: Quantum teleportation for the quantum internet". IEEE Transactions on Communications **68**, 3808–3833 (2020).

[93] Junjing Xing, Tianfeng Feng, Zhaobing Fan, Haitao Ma, Kishor Bharti, Dax Enshan Koh, and Yunlong Xiao. "Fundamental limitations on communication over a quantum network". arXiv preprint arXiv:2306.04983 (2023).

[94] Artur K. Ekert. "Quantum cryptography based on Bell's theorem". Phys. Rev. Lett. **67**, 661–663 (1991).

[95] Hans J Briegel, David E Browne, Wolfgang Dür, Robert Raussendorf, and Maarten Van den Nest. "Measurement-based quantum computation". Nature Physics **5**, 19–26 (2009).

[96] Jacob D. Biamonte, Mauro E. S. Morales, and Dax Enshan Koh. "Entanglement scaling in quantum advantage benchmarks". Phys. Rev. A **101**, 012349 (2020).

[97] Richard Jozsa and Maarten Van den Nest. "Classical simulation complexity of extended Clifford circuits". Quantum Information & Computation **14**, 633–648 (2014).

[98] Dax Enshan Koh. "Further extensions of Clifford circuits and their classical simulation complexities". Quantum Information & Computation **17**, 0262–0282 (2017).

[99] Adam Bouland, Joseph F. Fitzsimons, and Dax Enshan Koh. "Complexity Classification of Conjugated Clifford Circuits". In Rocco A. Servedio, editor, 33rd Computational Complexity Conference (CCC 2018). Volume 102 of Leibniz International Proceedings in Informatics (LIPIcs), pages 21:1–21:25. Dagstuhl, Germany (2018). Schloss Dagstuhl–Leibniz-Zentrum für Informatik.

[100] Tobias Haug, Soovin Lee, and M. S. Kim. "Efficient quantum algorithms for stabilizer entropies". Phys. Rev. Lett. **132**, 240602 (2024).

[101] Sergey Bravyi, Dan Browne, Padraic Calpin, Earl Campbell, David Gosset, and Mark Howard. "Simulation of quantum circuits by low-rank stabilizer decompositions". Quantum **3**, 181 (2019).

[102] Kaifeng Bu and Dax Enshan Koh. "Efficient classical simulation of Clifford circuits with nonstabilizer input states". Phys. Rev. Lett. **123**, 170502 (2019).

[103] James R. Seddon, Bartosz Regula, Hakop Pashayan, Yingkai Ouyang, and Earl T. Campbell. "Quantifying quantum speedups: Improved classical simulation from tighter magic monotones". PRX Quantum **2**, 010345 (2021).

[104] Lorenzo Leone, Salvatore F. E. Oliviero, and Alioscia Hamma. "Stabilizer Rényi entropy". Phys. Rev. Lett. **128**, 050402 (2022).

[105] Kaifeng Bu, Dax Enshan Koh, Lu Li, Qingxian Luo, and Yaobo Zhang. "Statistical complexity of quantum circuits". Phys. Rev. A **105**, 062431 (2022).

[106] Kaifeng Bu, Weichen Gu, and Arthur Jaffe. "Stabilizer testing and magic entropy". arXiv preprint arXiv:2306.09292 (2023).

[107] Kaifeng Bu, Weichen Gu, and Arthur Jaffe. "Discrete quantum Gaussians and central limit theorem". arXiv preprint arXiv:2302.08423 (2023).

[108] Kaifeng Bu, Weichen Gu, and Arthur Jaffe. "Quantum entropy and central limit theorem". Proceedings of the National Academy of Sciences **120**, e2304589120 (2023).

[109] Richard A. Low. "Learning and testing algorithms for the Clifford group". Phys. Rev. A **80**, 052314 (2009).

[110] Guoming Wang. "Property testing of unitary operators". Phys. Rev. A **84**, 052328 (2011).

[111] Benoît Collins and Piotr Śniady. "Integration with respect to the haar measure on unitary, orthogonal and symplectic group". Communications in Mathematical Physics **264**, 773–795 (2006).

[112] Z. Puchała and J.A. Miszczak. "Symbolic integration with respect to the Haar measure on the unitary groups". Bulletin of the Polish Academy of Sciences: Technical Sciences **65**, 21–27 (2017).

Appendix

We provide proofs and additional details supporting the claims in the main text.

A Primer on PRSs, PRSSs and PRUs

We start with the basics of classical cryptography required to understand PRSs, PRSSs and PRUs. For details, refer to Ref. [77].

1 Classical cryptography basics

First, we start with the concepts of negligible and noticeable functions.

Definition S1 (Negligible Function)**.** *A function $\mu : \mathbb{N} \to \mathbb{R}$ is negligible if and only if $\forall c \in \mathbb{N}$, $\exists n_0 \in \mathbb{N}$ such that $\forall n > n_0$, $\mu(n) < n^{-c}$.*

Definition S2 (Noticeable Function)**.** *A function $\mu : \mathbb{N} \to \mathbb{R}$ is noticeable if and only if $\exists c \in \mathbb{N}$, $n_0 \in \mathbb{N}$ such that $\forall n \geq n_0$, $\mu(n) \geq n^{-c}$.*

Intuitively, a noticeable function is a function that at least scales as a polynomial n^{-c} with $c > 0$ being a constant. In contrast, a negligible function must be strictly smaller than any polynomial function. For example, since $\mu(n) = 2^{-n}$ is exponentially small, it is a negligible function. Conversely, $\mu(n) = n^{-3}$ is only polynomially small and is therefore noticeable.

Finally, a pseudorandom generator (PRG) is a deterministic algorithm that takes a short, truly random input called a seed and expands it into a longer sequence of seemingly random bits. The

generated sequence should be indistinguishable from a truly random sequence to any computationally bounded observer or algorithm.

Definition S3 (Pseudorandom Generator (PRG))**.** *Let $l(\cdot)$ be a polynomial function and let G be a deterministic polynomial-time algorithm. G takes an input s from the set $\{0,1\}^n$ and produces a string of length $l(n)$. We define G as a pseudorandom generator if it satisfies the following two conditions:*

1. Expansion: *For every n, the length of the output string, $l(n)$, is greater than n.*
2. Pseudorandomness: *For any probabilistic polynomial-time distinguisher D, there exists a negligible function* $\mathrm{negl}(n)$ *such that*

$$|\Pr[D(r)=1] - \Pr[D(G(s))=1]| \leq \mathrm{negl}(n).$$

Here, r is uniformly chosen at random from $\{0,1\}^{l(n)}$, the seed s is uniformly chosen at random from $\{0,1\}^n$, and the probabilities are computed over the random coins used by D and the choices of r and s.

The function $l(\cdot)$ is referred to as the expansion factor of the pseudorandom generator G.

Pseudorandom generators play a crucial role in cryptography, as they provide a way to generate seemingly random values from a small random seed. They are used in a variety of applications, such as key generation, encryption schemes, and secure communication protocols. PRGs are also used in other areas of computer science, including simulations, random sampling, and probabilistic algorithms. Finally, to illustrate the construction of a PRS from a PRG, we discuss the concept of pseudorandom functions (PRF):

Definition S4 (Pseudorandom Function (PRF))**.** *A keyed family of functions $\{F_k : \{0,1\}^n \to \{0,1\}^n\}_{k\in\mathcal{K}}$ is called a pseudorandom function if F_k is computable in polynomial time and for all probabilistic polynomial-time distinguishers D, there exists a negligible function* negl *such that:*

$$|\Pr[D^{F_k(\cdot)}(1^n)=1] - \Pr[D^{f(\cdot)}(1^n)=1]| \leq \mathrm{negl}(n)$$

where k is chosen uniformly at random from $\mathcal{K}=\{0,1\}^n$, and f is chosen uniformly at random from the set of all functions which map n-bit strings to n-bit strings.

Without knowing the key k, it should be computationally infeasible for an adversary to distinguish between the output of the PRF and a truly random function, even if the adversary can make adaptive queries.

PRFs and PRGs are equivalent primitives in cryptography, i.e. PRF $\iff$ PRG [77]. This extends to the case where the distinguisher has access to quantum computer, i.e. post-quantum PRF $\iff$ post-quantum PRG [86]. Furthermore, Ref. [1] proved that post-quantum PRF $\implies$ PRS.

2 Definitions of pseudorandomness

Definition S5 (Pseudorandom Unitary Operators (PRUs) [1])**.** *Consider a n-qubit Hilbert space $\mathcal{H}$ and a key space $\mathcal{K}$ with security parameter $\kappa = \mathrm{poly}(n)$. A family of unitary operators $\{U_k \in U(\mathcal{H})\}_{k\in\mathcal{K}}$ is pseudorandom if the following two conditions hold:*

1. *Efficient computation: There exists an efficient quantum algorithm Q such that for all k and any $|\psi\rangle \in \mathcal{S}(\mathcal{H})$, $Q(k,|\psi\rangle) = U_k|\psi\rangle$.*
2. *Pseudorandomness: U_k with a random key k is computationally indistinguishable from a Haar random unitary operator. More precisely, for any efficient quantum algorithm A that makes at most polynomially many queries to the oracle,*

$$\left| \Pr_{k\leftarrow\mathcal{K}}[A^{U_k}(1^\kappa)=1] - \Pr_{U\leftarrow\mu}[A^{U}(1^\kappa)=1] \right| \leq \mathrm{negl}(n).$$

In the first term, the observer uses any efficient algorithm A with access to the key size 1^κ in unary and oracle access to pseudorandom unitary U_k with random key k, while in the second term the observer is given Haar random unitaries U. This definition states that a family of unitary operators is considered pseudorandom if it is both efficiently computable and indistinguishable from Haar random unitary operators for an observer with a bounded computational power.

Definition S6 (Pseudorandom Quantum States (PRSs))**.** *Consider an n-qubit Hilbert space $\mathcal{H}$ and a key space $\mathcal{K}$ with security parameter $\kappa = \mathrm{poly}(n)$. A keyed family of quantum states $|\phi_k\rangle \in \mathcal{S}(\mathcal{H})_{k\in\mathcal{K}}$ is defined as pseudorandom if it satisfies the following conditions:*

1. *Efficient generation: There exists a polynomial-time quantum algorithm G capable of generating the state $|\phi_k\rangle$ when given the input k. In other words, for every $k \in \mathcal{K}$, $G(k) = |\phi_k\rangle$.*

2. *Pseudorandomness: When given the same random $k \in \mathcal{K}$, any polynomially bounded number of copies of $|\phi_k\rangle$ are computationally indistinguishable from the same number of copies of a Haar random state. More specifically, for any efficient quantum algorithm A and any $m \in \mathrm{poly}(n)$,*

$$\left| \Pr_{k\leftarrow\mathcal{K}}[A(|\phi_k\rangle^{\otimes m}) = 1] - \Pr_{|\psi\rangle\leftarrow\mu}[A(|\psi\rangle^{\otimes m}) = 1] \right| = \mathrm{negl}(n),$$

where μ represents the Haar measure on $\mathcal{S}(\mathcal{H})$.

In this definition, a keyed family of quantum states is considered pseudorandom if it can be generated efficiently and appears statistically indistinguishable from Haar random states to an observer with limited computational resources.

In between PRUs and PRS are pseudorandom state scramblers (PRSSs). They are an ensemble of n-qubit unitaries $\{U_i\}_i$ which applied to any (fixed) n-qubit input state $|\psi\rangle$ generate a PRS $\{U_i|\psi\rangle\}_i$ [14, 15]. Formally, we have [14]:

Definition S7 (Pseudorandom State Scrambler (PRSS))**.** *Let $\kappa = \mathrm{poly}(n)$ be a security parameter. A* pseudorandom state scrambler *(PRSS) is an ensemble of n-qubit unitary operators $\{U_k \in \mathcal{U}(\mathcal{H})\}_{k\in\mathcal{K}}$ satisfying:*

1. *Efficient computation: There exists an efficient quantum algorithm G, such that for all k and any $|\psi\rangle \in \mathcal{S}(\mathcal{H})$, $G(k, |\psi\rangle) = U_k|\psi\rangle$.*

2. *Pseudorandomness: For any $m = \mathrm{poly}(n)$, any n-qubit state $|\phi\rangle \in \mathcal{S}(\mathcal{H})$, and any efficient quantum algorithm A we have*

$$\left| \Pr_{k\leftarrow\mathcal{K}}[A((U_k|\phi\rangle)^{\otimes m}) = 1] - \Pr_{|\psi\rangle\leftarrow\mu}[A(|\psi\rangle^{\otimes m}) = 1] \right| = \mathrm{negl}(n),$$

where μ is the Haar measure on $\mathcal{S}(\mathcal{H})$.

Note that while PRSS are unitaries that generate PRS, not all unitary generators of PRS are also PRSS. In particular, there are PRS generators that produce PRS only when applied to one particular input state [1]. For example, the recently proposed construction of the binary phase state requires a product state as input, while for general input states the same generators will not produce PRS [16]. Also note that any PRU is a PRSS, while the converse is not true in general as we show in the main text. While not discussed here, note that one can define more general notion of PRSS for isometries [14, 15].

Finally, we discuss the notion of pseudoentanglement, as introduced in Ref. [17].

Definition S8 (Pseudoentangled State Ensemble (PES))**.** *A* pseudoentangled state ensemble (PES) *with gap $f(n)$ vs. $g(n)$ consists of two ensembles of n-qubit states $|\Psi_k\rangle$ and $|\Phi_k\rangle$, indexed by a secret key $k \in \mathcal{K}$ with the following properties:*

1. Efficient Preparation*: Given k, $|\Psi_k\rangle$ (or $|\Phi_k\rangle$, respectively) is efficiently preparable by a uniform, poly-sized quantum circuit.*

2. Entanglement Entropy*: With probability $\geq 1 - \frac{1}{poly(n)}$ over the choice of k, the entanglement entropy between the first $\frac{n}{2}$ and second $\frac{n}{2}$ qubits of $|\Psi_k\rangle$ (or $|\Phi_k\rangle$, respectively) is $\Theta(f(n))$ (or $\Theta(g(n))$, respectively).*

3. Indistinguishability*: No polynomial-time quantum algorithm with access to $m = \text{poly}(n)$ copies can distinguish between the two ensembles with more than negligible probability. That is, for any poly-time quantum algorithm A, we have that*

$$\left| \Pr_{k \leftarrow \mathcal{K}}[A(|\Phi_k\rangle^{\otimes m}) = 1] - \Pr_{k \leftarrow \mathcal{K}}[A(|\Psi_k\rangle^{\otimes m}) = 1] \right| = \text{negl}(n)\,.$$

We now generalize this concept to arbitrary resource theories:

Definition S9 (Pseudoresource state ensemble)**.** *With respect to resource Q, pseudoresource state ensemble with gap $f(n)$ vs. $g(n)$ (where $f(n) \geq g(n)$) consists of two ensembles with key $k \in \mathcal{K}$: A 'high-resource' ensemble $|\psi_k\rangle$ which has $Q(|\psi_k\rangle) = f(n)$ with high probablity over k, and 'low-resource' ensemble $|\phi_k\rangle$ with $Q(|\phi_k\rangle) = g(n)$. We demand following conditions for the pseudoresource state ensemble:*

- *$|\psi_k\rangle$ and $|\phi_k\rangle$ are efficiently preparable*
- *No poly-time quantum algorithm A can distinguish between the ensembles $\rho = |\psi_k\rangle^{\otimes m}\langle\psi_k|^{\otimes m}$ and $\sigma = |\phi_k\rangle^{\otimes m}\langle\phi_k|^{\otimes m}$ with $m \in \text{poly}(n)$ with more than negligible probability:*

$$\left| \Pr_{k \leftarrow \mathcal{K}}[A(|\psi_k\rangle^{\otimes m}) = 1] - \Pr_{k \leftarrow \mathcal{K}}[A(|\phi_k\rangle^{\otimes m}) = 1] \right| = \text{negl}(n)\,.$$

3 The indistinguishability experiment

It is crucial to emphasize that a pseudorandom object possesses any efficiently verifiable property that its random counterpart exhibits. To illustrate this concept, we consider a two-player experiment $\mathcal{E}(\mathcal{A}, n)$ involving a challenger $\mathcal{C}$ and a quantum polynomial time adversary $\mathcal{A}$. Let $|\phi_k\rangle \in \mathcal{S}(\mathcal{H})_{k\in\mathcal{K}}$ represent a keyed family of n-qubit quantum states and μ represent the Haar measure on $\mathcal{S}(\mathcal{H})$. Let $m = \text{poly}(n)$. The key generator algorithm $\text{Gen}(1^n)$ takes the security parameter n in unary as input, and outputs key k, which is a uniform random bitstring of size $\text{poly}(n)$. The experiment $\mathcal{E}(\mathcal{A}, n)$ proceeds as follows.

1. $\mathcal{C}$ generates a private key $k \leftarrow \mathsf{Gen}(1^n)$, where $|k| = \text{poly}(n)$.
2. $\mathcal{C}$ samples uniform random a bit $b \leftarrow \{0, 1\}$.
   (a) If b = 0, $\mathcal{C}$ prepares a state $|\psi_0\rangle := |\phi_k\rangle^{\otimes m}$.
   (b) If b = 1, $\mathcal{C}$ prepares a state $|\psi_1\rangle := |\phi_\mu\rangle^{\otimes m}$. Here, $|\phi_\mu\rangle$ is a Haar random state.
3. $\mathcal{C}$ sends $|\psi_b\rangle$ to $\mathcal{A}$.
4. $\mathcal{A}$ sends $b' \in \{0, 1\}$ to $\mathcal{C}$.
5. The output of the experiment is defined to be 1 if $b' = b$, else 0. If $\mathcal{E}(\mathcal{A}, n) = 1$, we say $\mathcal{A}$ succeeded.

If $|\phi_k\rangle \in \mathcal{S}(\mathcal{H})_{k\in\mathcal{K}}$ is PRS, then $\Pr[\mathcal{E}(\mathcal{A}, n) = 1] \leq \frac{1}{2} + \text{negl}(n)$. Here, the probability is taken over all the random coins used in the experiment. If $|\phi_k\rangle$ does not possess any efficiently verifiable property that its random counterpart exhibits, then it can be used by $\mathcal{A}$ to win the indistinguishability game $\mathcal{E}(\mathcal{A}, n)$ with a probability greater than $\frac{1}{2} + \text{negl}(n)$.

B Property Testing

Property testing.—A property tester $\mathcal{A}_Q$ has to fulfill two conditions [43–46]: The completeness condition demands that the tester accepts with high probability if the state has the property within threshold β. The soundness condition states that the tester rejects with high probability if the state exceeds a threshold value δ of the property.

Definition S10 (Property tester)**.** *An algorithm $\mathcal{A}_Q$ is a tester for property Q using $t = t(n, \delta, \beta)$ copies if, given t copies of $|\psi\rangle \in \mathbb{C}^{2^n}$, constants $\beta > 0$ and $\delta > \beta$, it acts as follows:*

- *(Completeness) If $Q(|\psi\rangle) \leq \beta$, then*

$$\Pr[\mathcal{A}_Q \text{ accepts given } |\psi\rangle^{\otimes t}] \geq \frac{2}{3}. \tag{S1}$$

- *(Soundness) If $Q(|\psi\rangle) \geq \delta$, then*

$$\Pr[\mathcal{A}_Q \text{ accepts given } |\psi\rangle^{\otimes t}] \leq \frac{1}{3}. \tag{S2}$$

C PRSs, PRUs and noise

Here, we show that PRSs and PRUs (and also PRSSs) can sustain only a negligible amount of noise. First, we restate Theorem 1 of the main text:

Theorem S1 (PRUs and PRSs are not robust to noise)**.** *Any ensemble of unitaries or states subject to a single-qubit depolarizing noise channel $\Lambda_p(X) = (1-p)X + p\mathrm{tr}(X)I_1/2$ can be PRUs and PRSs only for at most $p = \mathrm{negl}(n)$ depolarizing probability.*

Proof. The purity of a state ρ is given by

$$\gamma(\rho) = \mathrm{tr}(\rho^2) \tag{S3}$$

where $2^{-n} \leq \gamma \leq 1$, $\gamma(\rho) = 1$ for any pure state $\rho = |\psi\rangle\langle\psi|$, and for maximally mixed state $\rho_{\mathrm{m}} = I_n 2^{-n}$ we have $\gamma(\rho_{\mathrm{m}}) = 2^{-n}$. For pure Haar random states we find trivially $\mathbb{E}_{|\phi\rangle \leftarrow S(\mathcal{H})}[\gamma(|\phi\rangle)] = 1$. We can efficiently measure $\gamma(\rho)$ via the SWAP test acting on $\rho \otimes \rho$, which accepts with probability $\Pr_{\mathrm{SWAP}}(\rho) = \frac{1}{2} + \gamma(\rho)/2$ (see Fig. S1 or [60]). This follows from $\mathrm{tr}(\rho^2) = \mathrm{tr}(S\rho \otimes \rho)$, where S is the SWAP operator $S = \sum_{k\ell} |k\ell\rangle\langle\ell k|$.

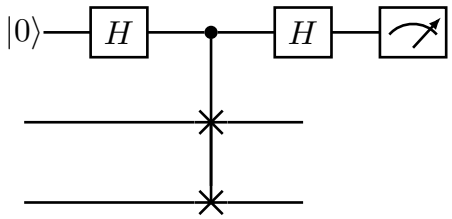

Figure S1: SWAP test.

Now, we regard the local depolarizing channel

$$\Lambda_p(\rho) = (1-p)\rho + \frac{p}{2} I_1 \otimes \mathrm{tr}_1(\rho) \tag{S4}$$

acting on the first qubit with probability p where $\mathrm{tr}_1(.)$ is the partial trace over the first qubit. For any input pure state $|\psi\rangle$ we find $\gamma(\Lambda_p(|\psi\rangle)) \leq 1 - p + p^2/2$.

Let us consider an ensemble of pure states $|\psi\rangle \in \mathcal{E}$. Now, we subject the states to noise, where we define the ensemble of corresponding noisy states $\rho \in \mathcal{E}_c$ where $\mathcal{E}_c = \{\Lambda_p(|\psi\rangle) : |\psi\rangle \in \mathcal{E}\}$ with $p = \Omega(n^{-c})$ with $c > 0$. For the noisy states we have $\mathbb{E}_{\rho\leftarrow\mathcal{E}_c}[\gamma(\rho)] = 1 - \Omega(n^{-c})$ and thus

$$\left| \mathop{\mathbb{E}}_{\rho\leftarrow\mathcal{E}_c}[\Pr_{\mathrm{SWAP}}(\rho)] - \mathop{\mathbb{E}}_{|\phi\rangle\leftarrow S(\mathcal{H})}[\Pr_{\mathrm{SWAP}}(|\phi\rangle)] \right| = \Omega(n^{-c})\,. \tag{S5}$$

We conclude that the SWAP test efficiently distinguishes Haar random states and any ensemble of states affected by $p = \Omega(n^{-c})$ depolarizing noise. Thus, PRSs can have at most $p = \mathrm{negl}(n)$ depolarizing noise.

Next, we consider the case of noisy unitaries. Consider an ensemble of unitaries $U \in \mathcal{G}$. Now, the unitaries are affected by the depolarizing channel Eq. (S4), giving us the ensemble of noisy channels $\Gamma \in \mathcal{G}_c$ with $\mathcal{G}_c = \{\Lambda_p \circ U : U \in \mathcal{G}\}$ where $p = \Omega(n^{-c})$. We now apply the noisy unitaries on a test state $|0\rangle$ and perform the SWAP test. We find

$$\left| \mathop{\mathbb{E}}_{\Gamma\leftarrow\mathcal{G}_c}[\Pr_{\mathrm{SWAP}}(\Gamma(|0\rangle))] - \mathop{\mathbb{E}}_{U\leftarrow\mathcal{U}(\mathcal{H})}[\Pr_{\mathrm{SWAP}}(U|0\rangle)] \right| = \Omega(n^{-c})\,. \tag{S6}$$

The SWAP test efficiently distinguishes Haar random unitaries and any unitaries affected by $p = \Omega(n^{-c})$ depolarizing noise. Thus, PRUs can be subject to at most $p = \mathrm{negl}(n)$ depolarizing noise. □

D Proof of inefficient testing of imaginarity for states

Here we show that imaginarity cannot be efficiently tested for states. First, we restate the Theorem 2 of the main text:

Theorem S2 (Imaginarity cannot be efficiently tested for states)**.** *Any tester $\mathcal{A}_{\mathcal{I}}$ for imaginarity according to Def. 10 for an n-qubit state $|\psi\rangle$ requires $t = \Omega(2^{n/2})$ copies of $|\psi\rangle$ for $\delta < 1 - n^2 2^{-n/2}$ and any $\beta < \delta$.*

Proof. Let us first recall Levy's lemma [87]

Lemma S1 (Levy's lemma)**.** *Given a function $f : \mathbb{S}(d) \to \mathbb{R}$ defined on the d-dimensional hypersphere $\mathbb{S}(d)$, $\epsilon > 0$ and a point $\phi \in \mathbb{S}(d)$ chosen uniformly at random,*

$$\Pr(|f(\phi) - \langle f\rangle| \geq \epsilon) \leq 2\exp\left(\frac{-2C(d+1)\epsilon^2}{\eta^2}\right) \tag{S7}$$

where η is the Lipschitz constant of f, given by $\eta = \sup|\nabla f|$, and C is a positive constant (which can be taken to be $C = (18\pi^3)^{-1}$.

Due to normalisation, pure states in a 2^n-dimensional Hilbert space can be represented by points on the surface of a $(2\cdot 2^n - 1)$-dimensional hypersphere $\mathbb{S}(2\cdot 2^n - 1)$, and hence we can apply Levy's Lemma to functions of the randomly selected quantum state $|\phi\rangle$ by setting $d = 2\cdot 2^n - 1$.

Next, we bound the Lipschitz constant η of imaginarity. For any normalized pure states $|\psi\rangle$, $|\phi\rangle$, we find

$$\eta = \max_{|\psi\rangle,|\phi\rangle} \frac{|\mathcal{I}(|\psi\rangle) - \mathcal{I}(|\phi\rangle)|}{||\psi\rangle - |\phi\rangle|} = 4, \tag{S8}$$

where $||\psi\rangle - |\phi\rangle| = \sqrt{2 - 2\Re(\langle\psi|\phi\rangle)}$ indicates the Euclidean norm. First, we have

$$\begin{aligned} |\mathcal{I}(|\psi\rangle) - \mathcal{I}(|\phi\rangle)| &= \frac{1}{4}\left| |||\psi\rangle\langle\psi| - |\psi^*\rangle\langle\psi^*|||_1^2 - |||\phi\rangle\langle\phi| - |\phi^*\rangle\langle\phi^*|||_1^2 \right| \\ &\leq |||\psi\rangle\langle\psi| - |\psi^*\rangle\langle\psi^*|||_1 - |||\phi\rangle\langle\phi| - |\phi^*\rangle\langle\phi^*|||_1| \end{aligned}$$

where we used $\|x\|^2 - \|y\|^2 = (|\|x\| - \|y\||)(\|x\| + \|y\|)$ and $\||\psi\rangle\langle\psi| + |\psi^*\rangle\langle\psi^*|\|_1 \leq 2$. Then, we have

$$\begin{aligned}|\mathcal{I}(|\psi\rangle) - \mathcal{I}(|\phi\rangle)| &\leq \||\psi\rangle\langle\psi| - |\phi\rangle\langle\phi| - (|\psi^*\rangle\langle\psi^*| - |\phi^*\rangle\langle\phi^*|)\|_1 \\ &\leq \||\psi\rangle\langle\psi| - |\phi\rangle\langle\phi|\|_1 + \||\psi^*\rangle\langle\psi^*| - |\phi^*\rangle\langle\phi^*|\|_1 \\ &= 4\sqrt{1 - |\langle\psi|\phi\rangle|^2} \leq 4||\psi\rangle - |\phi\rangle| \end{aligned} \tag{S9}$$

where in the first two steps we used the triangle inequalities $|\|x\| - \|y\|| \leq \|x - y\|$, $\|x - y\| \leq \|x\| + \|y\|$, and in the last inequality

$$\begin{aligned}1 - |\langle\psi|\phi\rangle|^2 &= 1 - \Re(\langle\psi|\phi\rangle)^2 - \Im(\langle\psi|\phi\rangle)^2 \leq 1 - \Re(\langle\psi|\phi\rangle)^2 = (1 - \Re(\langle\psi|\phi\rangle))(1 + \Re(\langle\psi|\phi\rangle)) \\ &\leq 2(1 - \Re(\langle\psi|\phi\rangle)) = ||\psi\rangle - |\phi\rangle|^2 , \end{aligned} \tag{S10}$$

which finally gives us $\eta = 4$.

From Levy's lemma and the imaginarity of Haar random states $\mathcal{I}_{\text{Haar}} = \mathbb{E}_{|\psi\rangle \leftarrow S(\mathcal{H})}[\mathcal{I}(|\psi\rangle)] = 1 - 2(2^n + 1)^{-1}$ (see Eq. (S55)), we have

$$\Pr(|\mathcal{I}(|\psi\rangle) - \mathcal{I}_{\text{Haar}}| \geq \epsilon) \leq 2\exp(-\beta_0 2^n \epsilon^2), \tag{S11}$$

where $\beta_0 = 4C/\eta^2 = (288\pi^3)^{-1}$ and $\epsilon > 0$. We now drop the absolute value $|.|$ and define $\epsilon = \mathcal{I}_{\text{Haar}} - \delta$ to get

$$\Pr(\mathcal{I}(|\psi\rangle) \leq \delta) \leq 2\exp(-\beta_0 2^n (\mathcal{I}_{\text{Haar}} - \delta)^2), \tag{S12}$$

which is valid for any $\delta < \mathcal{I}_{\text{Haar}}$.

We now choose δ such that we achieve exponential concentration, i.e. exponentially many quantum states have an imaginarity $\mathcal{I} > \delta$. We achieve this by setting

$$\delta < \mathcal{I}_{\text{Haar}}(n) - \beta_0^{-1/2} n 2^{-n/2} = 1 - \frac{2}{2^n + 1} - \sqrt{288\pi^3 \ln(2)} n 2^{-n/2} \tag{S13}$$

where we get

$$P_\delta = \Pr_{|\psi\rangle \leftarrow S(\mathcal{H})}[\mathcal{I}(|\psi\rangle) < \delta] = O(2^{-n^2}) . \tag{S14}$$

We now proceed with the choice

$$\delta < 1 - n^2 2^{-n/2} . \tag{S15}$$

which satisfies the scaling of Eq. (S14) for any $n \geq 80$.

Let us now define the ensemble $\mathcal{E}_{\mathcal{I} \geq \delta} = \{|\psi\rangle : \mathcal{I}(|\psi\rangle) \geq \delta, |\psi\rangle \in S(\mathcal{H})\}$ of states with imaginarity at least δ, and the ensemble $\mathcal{E}_{\mathcal{I} < \delta} = \{|\psi\rangle : \mathcal{I}(|\psi\rangle) < \delta, |\psi\rangle \in S(\mathcal{H})\}$ of states with imaginarity at most δ.

Given the concentration Eq. (S14) and choosing δ according to Eq. (S15), the ensemble of states with $\mathcal{I} \geq \delta$ is exponentially close to the ensemble of Haar random states $S(\mathcal{H})$ for any t

$$\text{TD}\left(\mathop{\mathbb{E}}_{|\psi\rangle \leftarrow \mathcal{E}_{\mathcal{I} \geq \delta}}[|\psi\rangle\langle\psi|^{\otimes t}], \mathop{\mathbb{E}}_{|\phi\rangle \leftarrow S(\mathcal{H})}[|\phi\rangle\langle\phi|^{\otimes t}]\right) = O(2^{-n^2}) , \tag{S16}$$

where we have the trace distance $\text{TD}(\rho, \sigma) = \frac{1}{2}\|\rho - \sigma\|_1$.

We now prove Eq. (S16) in the following:

$$\begin{aligned}&\text{TD}\left(\mathop{\mathbb{E}}_{|\psi\rangle \leftarrow \mathcal{E}_{\mathcal{I} \geq \delta}}[|\psi\rangle\langle\psi|^{\otimes t}], \mathop{\mathbb{E}}_{|\phi\rangle \leftarrow S(\mathcal{H})}[|\phi\rangle\langle\phi|^{\otimes t}]\right) \\ &= \text{TD}\Bigg((1 - P_\delta) \mathop{\mathbb{E}}_{|\psi\rangle \leftarrow \mathcal{E}_{\mathcal{I} \geq \delta}}[|\psi\rangle\langle\psi|^{\otimes t}] + P_\delta \mathop{\mathbb{E}}_{|\psi\rangle \leftarrow \mathcal{E}_{\mathcal{I} < \delta}}[|\psi\rangle\langle\psi|^{\otimes t}] \\ &\quad - P_\delta\Big(\mathop{\mathbb{E}}_{|\psi\rangle \leftarrow \mathcal{E}_{\mathcal{I} < \delta}}[|\psi\rangle\langle\psi|^{\otimes t}] - \mathop{\mathbb{E}}_{|\psi\rangle \leftarrow \mathcal{E}_{\mathcal{I} \geq \delta}}[|\psi\rangle\langle\psi|^{\otimes t}]\Big), \mathop{\mathbb{E}}_{|\phi\rangle \leftarrow S(\mathcal{H})}[|\phi\rangle\langle\phi|^{\otimes t}]\Bigg) \end{aligned} \tag{S17}$$

$$= \mathrm{TD}\left(\mathop{\mathbb{E}}_{|\phi\rangle\leftarrow S(\mathcal{H})} \left[|\phi\rangle\langle\phi|^{\otimes t}\right] - P_\delta\left(\mathop{\mathbb{E}}_{|\psi\rangle\leftarrow \mathcal{E}_{\mathcal{I}<\delta}} \left[|\psi\rangle\langle\psi|^{\otimes t}\right] - \mathop{\mathbb{E}}_{|\psi\rangle\leftarrow \mathcal{E}_{\mathcal{I}\geq\delta}} \left[|\psi\rangle\langle\psi|^{\otimes t}\right]\right), \mathop{\mathbb{E}}_{|\phi\rangle\leftarrow S(\mathcal{H})} \left[|\phi\rangle\langle\phi|^{\otimes t}\right] \right)$$

$$= P_\delta \mathrm{TD}\left(\mathop{\mathbb{E}}_{|\psi\rangle\leftarrow \mathcal{E}_{\mathcal{I}<\delta}} \left[|\psi\rangle\langle\psi|^{\otimes t}\right], \mathop{\mathbb{E}}_{|\psi\rangle\leftarrow \mathcal{E}_{\mathcal{I}\geq\delta}} \left[|\psi\rangle\langle\psi|^{\otimes t}\right] \right) = O(2^{-n^2}),$$

where in the second step we used

$$(1-P_\delta) \mathop{\mathbb{E}}_{|\psi\rangle\leftarrow \mathcal{E}_{\mathcal{I}\geq\delta}} \left[|\psi\rangle\langle\psi|^{\otimes t}\right] + P_\delta \mathop{\mathbb{E}}_{|\psi\rangle\leftarrow \mathcal{E}_{\mathcal{I}<\delta}} \left[|\psi\rangle\langle\psi|^{\otimes t}\right] = \mathop{\mathbb{E}}_{|\phi\rangle\leftarrow S(\mathcal{H})} \left[|\phi\rangle\langle\phi|^{\otimes t}\right] \tag{S18}$$

and in the last step $\mathrm{TD}(\rho,\sigma) \leq 1$ for any valid quantum states ρ, σ.

Note that Eq. (S16) is independent of the number of copies t. This is because the set of highly imaginary states and the set of Haar random states are nearly identical, differing only by some exponentially small fraction. Therefore, they remain close for any t. Note that this is in contrast to the distance between Haar random states and discrete sets of states (e.g. the K-subset phase states Eq. (4)), which due to their small size become further in distance with more copies t.

Next, we recall the K-subset phase states from Eq. (4) or Ref. [17]

$$|\psi_{S,f}\rangle = \frac{1}{\sqrt{K}} \sum_{x\in S} (-1)^{f(x)} |x\rangle, \tag{S19}$$

where S is a set of binary strings $\{0,1\}^n$ with exactly $K = |S|$ elements and $f : \{0,1\}^n \to \{0,1\}$ a binary phase function. Note that the K-subset phase state is real-valued, and thus has imaginarity $\mathcal{I}(|\psi_{S,f}\rangle) = 0$. Let us also define the set of all K-subset phase states $\mathcal{E}_{\mathrm{p}}^K = \{|\psi_{S,f}\rangle\}_{S \text{ with } |S|=K,\, f}$ which contains the states $|\psi_{S,f}\rangle$ with all binary phase functions f and all S with $K = |S|$.

The ensemble $\mathcal{E}_{\mathrm{p}}$ of phase states Eq. (S19) has been shown to be statistically close to the ensemble of Haar random states (Theorem 2.1 of Ref. [17])

$$\mathrm{TD}\left(\mathop{\mathbb{E}}_{|\psi\rangle\leftarrow \mathcal{E}_{\mathrm{p}}^K} \left[|\psi\rangle\langle\psi|^{\otimes t}\right], \mathop{\mathbb{E}}_{|\phi\rangle\leftarrow S(\mathcal{H})} \left[|\phi\rangle\langle\phi|^{\otimes t}\right] \right) = O\left(\frac{t^2}{K}\right). \tag{S20}$$

Now, as the Haar random ensemble is exponentially close to the ensemble of highly imaginary states, we can apply the inequality $\mathrm{TD}(\rho,\sigma) \leq \mathrm{TD}(\rho,\theta) + \mathrm{TD}(\theta,\sigma)$ to Eq. (S16) and Eq. (S20) to get

$$\mathrm{TD}\left(\mathop{\mathbb{E}}_{|\psi\rangle\leftarrow \mathcal{E}_{\mathrm{p}}^K} \left[|\psi\rangle\langle\psi|^{\otimes t}\right], \mathop{\mathbb{E}}_{|\phi\rangle\leftarrow \mathcal{E}_{\mathcal{I}\geq\delta}} \left[|\phi\rangle\langle\phi|^{\otimes t}\right] \right) = O\left(\frac{t^2}{K}\right). \tag{S21}$$

Eq. (S21) implies that the ensemble of phase states and the ensemble of states with imaginarity $\mathcal{I}(|\psi\rangle) \geq \delta$ (where δ given by Eq. (S15)) are exponentially close in trace-distance unless $t = \Omega(\sqrt{K})$.

Two ensembles can be distinguished only if they are sufficiently far in TD distance. In particular, for any state discrimination protocol between two ensembles ρ, σ, the maximal possible discrimination probability is given by the Helstrom bound [88]

$$P_{\mathrm{discr}}(\rho,\sigma) = \frac{1}{2} + \mathrm{TD}(\rho,\sigma). \tag{S22}$$

In particular, any algorithm trying to distinguish two ensembles with $P_{\mathrm{discr}} \geq 2/3$ requires at least $\mathrm{TD}(\rho,\sigma) \geq 1/6$.

We now consider the case $K = 2^n$, i.e. subset phase states with support on all 2^n computational basis states. To achieve $P_{\mathrm{discr}} = \Omega(1)$ between t copies of $\mathcal{E}_{\mathrm{p}}^{2^n}$ and $\mathcal{E}_{\mathcal{I}\geq\delta}$, we require $t = \Omega(2^{n/2})$ for $\delta(n) < 1 - n^2 2^{-n/2}$. Thus, testing imaginarity must also require $t = \Omega(2^{n/2})$ copies, else imaginarity testing could be used to distinguish those two ensembles. □

Note that for the proof we used the subset phase states with $\mathcal{I} = 0$ which is the extremal case (i.e. $\beta = 0$). Thus, our result holds also for property testing of imaginarity for any β with $0 \leq \beta < \delta$.

E Inefficient algorithm to measure imaginarity of states

Now, we discuss a scheme to measure imaginarity for pure states. In particular, we have

$$\mathcal{I}(|\psi\rangle) = 1 - 2^n \langle\psi|^{\otimes 2}(|\Phi\rangle\langle\Phi|)|\psi\rangle^{\otimes 2}\,, \tag{S23}$$

where $|\Phi\rangle = 2^{-n/2}\sum_{k=0}^{2^n-1}|k\rangle|k\rangle$ is the maximally entangled state. To measure imaginarity, one computes the probability of the projector $|\Phi\rangle\langle\Phi|$ for two copies of state $|\psi\rangle^{\otimes 2}$. Using the Ricochet property S32, it is easy to see for $|\psi\rangle = U|0\rangle$ with arbitrary unitary U via

$$\begin{aligned}
&\langle\psi|^{\otimes 2}|\Phi\rangle\langle\Phi||\psi\rangle^{\otimes 2} = \langle 0|^{\otimes 2}U^\dagger \otimes U^\dagger|\Phi\rangle\langle\Phi|U\otimes U|0\rangle^{\otimes 2}\\
=&\langle 0|^{\otimes 2}U^\dagger U^{\mathrm{T}^\dagger}\otimes I|\Phi\rangle\langle\Phi|U^{\mathrm{T}}U\otimes I|0\rangle^{\otimes 2}\\
=&2^{-n}\langle 0|U^\dagger U^{\mathrm{T}^\dagger}|0\rangle\langle 0|U^{\mathrm{T}}U|0\rangle = 2^{-n}|\langle\psi|\psi^*\rangle|^2,
\end{aligned}$$

where we made use of Eq. (S32) and $U^{\mathrm{T}^\dagger} = U^*$. This completes the proof of Eq. (S23).

We measure the observable $2^n|\Phi\rangle\langle\Phi|$ which has two possible outcomes with eigenvalues $\lambda_1 = 2^n$ and $\lambda_2 = 0$, occurring with probability $p = \langle\psi|^{\otimes 2}|\Phi\rangle\langle\Phi||\psi\rangle^{\otimes 2}$ and $q = 1-p$. We can see this as Bernoulli trials. The Chernoff bound for the average over M Bernoulli trials $\hat{X} = \frac{1}{M}\sum_{i=1}^{M}X_i$ with trial outcome X_i is given by

$$P(|\hat{X}-\mu| \geq \tilde{\epsilon}) \leq \exp(-\frac{M\tilde{\epsilon}^2}{3\mu})\,, \tag{S24}$$

where $\tilde{\epsilon}$ is the additive estimation error. Now we have the estimator of imaginarity $\hat{\mathcal{I}} = 1 - 2^n\hat{X}$ and the mean value $\mu = p = 2^{-n}(1-\mathcal{I})$. From this, we get

$$P(|\hat{\mathcal{I}}-\mathcal{I}| \geq \epsilon) \equiv \delta \leq \exp(-\frac{M\epsilon^2}{3(1-\mathcal{I})2^n})\,. \tag{S25}$$

and finally

$$M \leq 3\epsilon^{-2}(1-\mathcal{I})2^n\log(1/\delta) \leq 3\epsilon^{-2}2^n\log(1/\delta)\,. \tag{S26}$$

Thus, to achieve a given accuracy ϵ with failure probability δ, we require at most a number of measurements $M = O(2^n\epsilon^{-2}\log(1/\delta))$. This $O(2^n)$ scaling is exponential, but better than tomography with $O(4^n)$.

F Efficient measurement of imaginarity for stabilizer states

Claim S1 (Imaginarity of stabilizer states can be measured efficiently)**.** *Given a stabilizer state* $|\psi\rangle \in \mathrm{STAB}$*, imaginarity can be computed via*

$$\mathcal{I}_{\mathrm{STAB}}(|\psi\rangle) = 1 - 2^{-n}\sum_{\sigma\in\mathcal{P}}|\langle\psi|\sigma|\psi^*\rangle|^2|\langle\psi|\sigma|\psi\rangle|^2, \tag{S27}$$

where $\mathcal{P}$ *is the set of all Pauli strings with phase* $+1$*.* $\mathcal{I}_{\mathrm{STAB}}$ *can be efficiently measured within additive precision* δ *with a failure probability* ν *using at most* $t = O(\delta^{-2}\log(1/\nu))$ *copies.*

Proof. We denote the Pauli matrices by $\sigma_{00} = I_2$, $\sigma_{01} = \sigma^x$, $\sigma_{10} = \sigma^z$ and $\sigma_{11} = \sigma^y$. We define the set of all 4^n Pauli strings $\mathcal{P} = \{\sigma_{\boldsymbol{r}}\}_{\boldsymbol{r}}$ with $+1$ phase by N-qubit tensor products of Pauli matrices given by $\sigma_{\boldsymbol{r}} = \bigotimes_{j=1}^{n}\sigma_{\boldsymbol{r}_{2j-1}\boldsymbol{r}_{2j}}$ with $\boldsymbol{r}\in\{0,1\}^{2n}$.

A stabilizer state $|\psi_{\mathrm{STAB}}\rangle$ is defined by a commuting subgroup G of $|G| = 2^n$ Pauli strings σ. We have $\langle\psi_{\mathrm{STAB}}|\sigma|\psi_{\mathrm{STAB}}\rangle = \pm 1$ for $\sigma\in G$ and $\langle\psi_{\mathrm{STAB}}|\sigma'|\psi_{\mathrm{STAB}}\rangle = 0$ for $\sigma'\notin G$ [68].

We now propose Algorithm 1 to efficiently measure the imaginarity of stabilizer states. We recall the Bell transformation $U_{\mathrm{Bell}} = (H\otimes I_1)\mathrm{CNOT}$ (see also Fig. S2), where $H = \frac{1}{\sqrt{2}}(\sigma^x+\sigma^z)$ is the Hadamard gate, and $\mathrm{CNOT} = \exp(i\frac{\pi}{4}(I_1-\sigma^z)\otimes(I_1-\sigma^x))$. We apply the Bell transformation on two copies

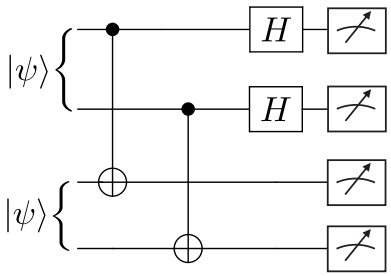

Figure S2: Bell measurement for state $|\psi\rangle$.

Algorithm 1: Imaginarity of stabilizer states

Input : $4M$ copies of $|\psi\rangle$
Output: $\mathcal{I}_{\mathrm{STAB}}$

$b = 0$
for $\ell = 1, \ldots, M$ **do**
  Prepare $|\eta\rangle = U_{\mathrm{Bell}}^{\otimes n}|\psi\rangle|\psi\rangle$
  Sample $\boldsymbol{r} \sim |\langle \boldsymbol{r}|\eta\rangle|^2$
  for $k = 1, 2$ **do**
    Prepare $|\psi\rangle$ and measure in eigenbasis of Pauli string $\sigma_{\boldsymbol{r}}$ to get eigenvalue $\lambda_k \in \{+1, -1\}$
  end
  $b = b + \lambda_1\lambda_2$
end
$\mathcal{I}_{\mathrm{STAB}} = 1 - b/M$

$|\psi\rangle \otimes |\psi\rangle$ and measure in the computational basis. The outcome $\boldsymbol{r}$ corresponding to computational basis state $|\boldsymbol{r}\rangle$ is sampled with a probability [89]

$$P(\boldsymbol{r}) = \langle\psi|\langle\psi|U_{\mathrm{Bell}}^{\otimes n\,\dagger}|\boldsymbol{r}\rangle\langle\boldsymbol{r}|U_{\mathrm{Bell}}^{\otimes n}|\psi\rangle|\psi\rangle = 2^{-n}|\langle\psi|\sigma_{\boldsymbol{r}}|\psi^*\rangle|^2\,. \tag{S28}$$

Using a combination of Bell measurements and Pauli measurements [48], we propose to measure the imaginarity of stabilizer states via

$$\mathcal{I}_{\mathrm{STAB}}(|\psi\rangle) := 1 - \mathop{\mathbb{E}}_{\boldsymbol{r}\sim P(\boldsymbol{r})}[|\langle\psi|\sigma_{\boldsymbol{r}}|\psi\rangle|^2]. \tag{S29}$$

In particular, given a stabilizer state $|\psi\rangle \in \mathrm{STAB}$ we find

$$\begin{aligned}\mathcal{I}_{\mathrm{STAB}}(|\psi\rangle) &= 1 - 2^{-n}\sum_{\sigma\in\mathcal{P}}|\langle\psi|\sigma|\psi^*\rangle|^2|\langle\psi|\sigma|\psi\rangle|^2 \\ &= 1 - 2^{-n}\sum_{\sigma\in G}|\langle\psi|\sigma|\psi^*\rangle|^2 = 1 - |\langle\psi|\psi^*\rangle|^2 \equiv \mathcal{I}(|\psi\rangle)\,,\end{aligned}$$

where in the second line we used $\sigma|\psi\rangle = \pm|\psi\rangle$ for $|\psi\rangle \in \mathrm{STAB}$ with corresponding $\sigma \in G(|\psi\rangle)$, and $\langle\psi|\sigma|\psi\rangle = 0$ for $\sigma \notin G(|\psi\rangle)$.

Note that non-real stabilizer states $|\psi_{\mathrm{STAB}}^I\rangle \notin \mathbb{R}^{2^n}$ are always maximally imaginary, i.e. $\mathcal{I}(|\psi_{\mathrm{STAB}}^I\rangle) = 1$ and $|\langle\psi_{\mathrm{STAB}}^I|{\psi_{\mathrm{STAB}}^I}^*\rangle|^2 = 0$. This can be easily seen from the fact that $|\langle\psi_{\mathrm{STAB}}|\sigma|\psi_{\mathrm{STAB}}\rangle|^2 \in \{0, 1\}$ and $|\psi_{\mathrm{STAB}}^*\rangle = \bigotimes_{k=1}^n \sigma_z^{\alpha_k}|\psi_{\mathrm{STAB}}\rangle$ with some $\alpha_k \in \{0, 1\}$ [89]. Thus, it follows $|\langle\psi_{\mathrm{STAB}}|\psi_{\mathrm{STAB}}^*\rangle|^2 = |\langle\psi_{\mathrm{STAB}}|\bigotimes_{k=1}^n \sigma_z^{\alpha_k}|\psi_{\mathrm{STAB}}\rangle|^2$. For any imaginary stabilizer, we necessarily have $|\langle\psi_{\mathrm{STAB}}^I|{\psi_{\mathrm{STAB}}^I}^*\rangle|^2 < 1$, and therefore $|\langle\psi_{\mathrm{STAB}}^I|{\psi_{\mathrm{STAB}}^I}^*\rangle|^2 = 0$.

Each repetition of the algorithm yields the outcome $\lambda_1 = -1$ or $\lambda_2 = 1$ with a range of outcomes $\Delta\lambda = 2$. We can upper bound the number of repetitions M needed to estimate $\mathcal{I}_{\mathrm{STAB}}$ using Hoeffding's inequality:

$$\Pr(|\hat{\mathcal{I}}_{\mathrm{STAB}} - \mathcal{I}_{\mathrm{STAB}}| \geq \delta) \equiv \nu \leq 2\exp\left(-\frac{2\delta^2 M}{\Delta\lambda^2}\right)\,, \tag{S30}$$

where $\hat{\mathcal{I}}_{\mathrm{STAB}}$ is the estimation of exact value $\mathcal{I}_{\mathrm{STAB}}$ from M repetitions, δ is the allowed error, $\Delta\lambda = 1$ is the range of possible measurement outcomes and ν is the failure probability of getting an error larger than δ. By inverting we find

$$M \leq \frac{\Delta\lambda^2}{2\delta^2} \log\left(\frac{2}{\nu}\right) = \frac{1}{\delta^2} \log\left(\frac{2}{\nu}\right), \tag{S31}$$

To achieve an error of at most δ with a probability of failure ν, we require at most $M = O(\delta^{-2}\log(\nu^{-1}))$ repetitions in Algorithm 1 and $4M$ copies of $|\psi\rangle$. The classical post-processing time scales as $O(n)$, which is asymptotically optimal. As real stabilizer states have $\mathcal{I} = 0$, while imaginary stabilizer states must have $\mathcal{I} = 1$, this directly implies that one can efficiently distinguish real and complex-valued stabilizer states with $t = O(1)$ copies of $|\psi\rangle$. □

We also propose Eq. (S29) as an efficient witness of non-imaginarity, which we define in analogy to entanglement witnesses [90]. When a non-imaginarity witness is zero, the state must be real. When the witness is greater than zero, then the state may be either real or imaginary. Eq. (S29) fulfills this condition as it is zero only when for real stabilizer states, and greater than zero for all other states [48].

G Efficient measurement of imaginarity for unitaries

Here, we show that measuring imaginarity $\mathcal{I}_{\mathrm{p}}(U)$ of an n-qubit unitary U is efficient. Imaginarity for unitaries can be defined via its Choi-state

$$\mathcal{I}_{\mathrm{p}}(U) \equiv \mathcal{I}(U \otimes I|\Phi\rangle) = 1 - |\langle\Phi|(U^\dagger \otimes I)(U^* \otimes I)|\Phi\rangle|^2 = 1 - 4^{-n}\left|\mathrm{tr}(U^\dagger U^*)\right|^2 .$$

Let us restate the Claim to be proven:

Claim S2 (Imaginarity of unitaries can be measured efficiently)**.** *Measuring $\mathcal{I}_p(U)$ within additive precision δ with a failure probability ν requires at most $t = O(\delta^{-2}\log(1/\nu))$ queries to U.*

Proof. First, we define the maximally entangled state $|\Phi\rangle = 2^{-n/2}\sum_{k=0}^{2^n-1}|k\rangle|k\rangle$ over $2n$ qubits. Then, we prepare the state $|\eta\rangle = U \otimes U|\Phi\rangle$. We then measure the expectation value $P_\Phi(U) = |\langle\Phi|\eta\rangle|^2$ of the projector $|\Phi\rangle\langle\Phi|$

$$\begin{aligned} P_\Phi(U) &= 4^{-n}\Big|\sum_{q,k}\langle q|\langle q|U \otimes U|k\rangle|k\rangle\Big|^2 = 4^{-n}\Big|\sum_{q,k}\langle q|\langle q|UU^T \otimes I|k\rangle|k\rangle\Big|^2 = 4^{-n}\Big|\sum_{k}\langle k|UU^T|k\rangle\Big|^2 \\ &= 4^{-n}\left|\mathrm{tr}(UU^T)\right|^2 = 4^{-n}\left|\mathrm{tr}(U^\dagger U^*)\right|^2, \end{aligned}$$

where we used the Ricochet property [91]

$$\sum_{k=0}^{2^n-1} A \otimes I_n|k\rangle|k\rangle = \sum_{k=0}^{2^n-1} I_n \otimes A^T|k\rangle|k\rangle \tag{S32}$$

for any n-qubit operator A. Thus, we can write imaginarity as

$$\mathcal{I}_{\mathrm{p}}(U) = 1 - P_\Phi(U)\,. \tag{S33}$$

$P_\Phi(U)$ can be measured efficiently by sampling in the Bell basis and measuring the probability of sampling $|\Phi\rangle$. We upper bound the required number of measurements M with Hoeffding's inequality Eq. (S31), where we have $\Delta\lambda = 1$ as the range of possible measurement outcomes. To achieve an error of at most δ with a probability of failure ν, we require at most $M = O(\delta^{-2}\log(\nu^{-1}))$ measurements and $2M$ instances of U. The classical post-processing time scales as $O(n)$, which is asymptotically optimal. □

H PRUs require imaginarity

Theorem S3. *PRUs require imaginarity* $\mathcal{I}_p = 1 - \mathrm{negl}(n)$.

Proof. We measure $P_{|\Phi\rangle} = 1 - \mathcal{I}_{\mathrm{p}}(U)$ which was introduced in the proof for Claim 2. We can interpret the measurement as a tester: We prepare $U \otimes U|\Phi\rangle$ and measure the projection onto $|\Phi\rangle\langle\Phi|$. The tester accepts when we get $|\Phi\rangle$ as outcome, else the tester rejects.

First, we consider a set of n-qubit unitaries $\mathcal{E}_c$ with imaginarity $\mathbb{E}_{U\leftarrow\mathcal{E}_c}[\mathcal{I}_{\mathrm{p}}(U)] = 1 - \Omega(n^{-c})$. For the acceptance probability of the test, we find $\mathbb{E}_{U\leftarrow\mathcal{E}_c}[P_\Phi(U)] = \Omega(n^{-c})$.

In contrast, for Haar random unitaries we find $\mathbb{E}_{U\leftarrow\mathcal{U}(\mathcal{H})}[P_\Phi(U)] = 2(2^n(2^n+1))^{-1} = O(4^{-n})$ (Appendix 2).

Thus, one can efficiently distinguish Haar random unitaries from $\mathcal{E}_c$, which places a lower bound the imaginarity of PRUs as $\mathcal{I}_{\mathrm{p}} = 1 - \mathrm{negl}(n)$. □

I Coherence testing for states

We now show the limits on coherence testing for states. First, we recall the definition of relative entropy of coherence for pure states $|\psi\rangle$

$$\mathcal{C}(|\psi\rangle) = -\sum_k |c_k|^2 \ln(|c_k|^2). \tag{S34}$$

Next, we restate the theorem of the main text:

Theorem S4 (Lower bound on coherence testing for states)**.** *Any tester $\mathcal{A}_\mathcal{C}$ for relative entropy of coherence according to Def. 10 for an n-qubit state $|\psi\rangle$ requires $t = \Omega(2^{\beta/2})$ for $\delta < n\ln(2) - 1$ and any $\beta < \delta$.*

Proof. First, we note that Haar random states concentrate around a large, but non-maximal value of coherence [70]. The coherence of n-qubit Haar random states is on average

$$\mathcal{C}_{\mathrm{Haar}} = \mathop{\mathbb{E}}_{|\phi\rangle\leftarrow S(\mathcal{H})}[\mathcal{C}(|\phi\rangle)] = \sum_{k=2}^{2^n} \frac{1}{k}\,, \tag{S35}$$

where for $n \gg 1$ we have $\mathcal{C}_{\mathrm{Haar}} = \gamma_{\mathrm{EM}} - 1 + n\ln(2) + O(2^{-n})$, where $\gamma_{\mathrm{EM}} = 0.57721$ is the Euler–Mascheroni constant. Haar random states concentrate around their average value with exponentially high probability [70]

$$\Pr(|\mathcal{C}(|\psi\rangle) - \mathcal{C}_{\mathrm{Haar}}| \geq \epsilon) \leq 2\exp\left(-\frac{2^n\epsilon^2}{36\pi^3\ln(2)(n\ln 2)^2}\right). \tag{S36}$$

Dropping the absolute value and defining $\epsilon = \mathcal{C}_{\mathrm{Haar}} - \delta$, $\delta < \mathcal{C}_{\mathrm{Haar}}$, we find that

$$\Pr(\mathcal{C}(|\psi\rangle) \leq \delta) \leq 2\exp\left(-\frac{2^n(\mathcal{C}_{\mathrm{Haar}} - \delta)^2}{36\pi^3\ln(2)(n\ln 2)^2}\right). \tag{S37}$$

When we choose $\delta < \mathcal{C}_{\mathrm{Haar}} - n^2 2^{-n/2}\sqrt{36\pi^3\ln(2)^3}$, we find exponential concentration, i.e. most states have a coherence $\mathcal{C} > \delta$

$$\Pr(\mathcal{C}(|\psi\rangle) < \delta) \leq O(2^{-n^2})\,. \tag{S38}$$

We relax this condition to $\delta < n\ln(2) - 1$, which is valid for any $n \geq 30$.

We now consider the ensemble $\mathcal{E}_{\mathcal{C}\geq\delta}$ of all states with a relative entropy of coherence greater δ. Given the concentration Eq. (S38), the ensemble $\mathcal{E}_{\mathcal{C}\geq\delta}$ is exponentially close to the ensemble $S(\mathcal{H})$ of random states for any t

$$\mathrm{TD}\left(\mathop{\mathbb{E}}_{|\psi\rangle\leftarrow\mathcal{E}_{\mathcal{C}\geq\delta}}[|\psi\rangle\langle\psi|^{\otimes t}], \mathop{\mathbb{E}}_{|\phi\rangle\leftarrow S(\mathcal{H})}[|\phi\rangle\langle\phi|^{\otimes t}]\right) = O(2^{-n^2})\,, \tag{S39}$$

where the proof follows the one for imaginarity given in Eq. (S17). Note that the distance between the states of high coherence and Haar random states is independent of the number of copies t. This is because of the concentration Eq. (S38), i.e the two sets of states are very close to each other, and the size of the sets differ by only a small fraction.

Further, we recall that Haar random states are close to K-subset phase states Eq. (S20). We recall the triangle inequality $\mathrm{TD}(\rho,\sigma) \leq \mathrm{TD}(\rho,\theta) + \mathrm{TD}(\theta,\sigma)$ and apply it on Eq. (S39) and Eq. (S20) to get for any $\delta \leq n\ln(2) - 1$

$$\mathrm{TD}\left(\mathop{\mathbb{E}}_{|\psi\rangle\leftarrow\mathcal{E}_{\mathrm{p}}^{K}}\left[|\psi\rangle\langle\psi|^{\otimes t}\right], \mathop{\mathbb{E}}_{|\phi\rangle\leftarrow\mathcal{E}_{\mathcal{C}\geq\delta}}\left[|\phi\rangle\langle\phi|^{\otimes t}\right]\right) \leq O\left(\frac{t^2}{K}\right). \tag{S40}$$

With Eq. (S40) and Helstrom bound Eq. (S22), we require $t = \Omega(\sqrt{K})$ copies to distinguish K-subset phase states from states drawn from the ensemble of states with $\mathcal{C} \geq \delta$ where $\delta > n\ln(n) - 1$.

Note that for any K-subset phase state $|\psi\rangle \in \mathcal{E}_{\mathrm{p}}^{K}$, the coherence is given by $\mathcal{C}(|\psi\rangle) = \ln(K)$.

The complexity of distinguishing K-subset phase state (which have coherence $\mathcal{C} = \log(K)$) from states with coherence $\mathcal{C} > \delta$ gives us directly a lower bound on coherence testing. In particular, to test whether an arbitrary state has coherence $\mathcal{C} = \beta$ or coherence $\mathcal{C} > \delta$ with $\beta < \delta$, one requires $t = \Omega(2^{\beta/2})$ copies.

□

Next, we show that one can efficiently measure coherence as defined by the Hilbert-Schmidt norm [30]

$$\mathcal{C}_2(|\psi\rangle) = 1 - \sum_k |c_k|^4, \tag{S41}$$

where $|\psi\rangle = \sum_k c_k|k\rangle$ with amplitudes c_k [30]. We have $0 \leq \mathcal{C}_2 \leq 1 - 2^{-n}$. Further, $\mathcal{C}_2(|\psi\rangle) = 0$ if and only if $\mathcal{C}(|\psi\rangle) = 0$.

For this measure of coherence, we have an efficient measurement protocol:

Proposition S1 (Efficient measurement of coherence)**.** *Measuring $\mathcal{C}_2(|\psi\rangle)$ within additive precision δ with a failure probability ν requires at most $t = O(\delta^{-2}\log(1/\nu))$ copies.*

Proof. $\mathcal{C}_2$ is measured efficiently with the projector $\Pi_{\mathcal{C}} = \bigotimes_{k=1}^{n}(|00\rangle\langle 00| + |11\rangle\langle 11|)$

$$\mathcal{C}_2(|\psi\rangle) = 1 - \langle\psi|^{\otimes 2}\Pi_{\mathcal{C}}|\psi\rangle^{\otimes 2}. \tag{S42}$$

The projector $\Pi_{\mathcal{C}}$ has possible eigenvalues $\lambda = 0$ or $\lambda = 1$, with eigenvalue range $\Delta\lambda = 1$. Using Hoeffding's inequality Eq. (S31), we can upper bound the number of copies $M = O(1)$ for reaching a fixed precision. □

Now, as stated in the main text, we prove that PRSs require sufficient relative entropy of coherence:

Claim S3. *PRSs require $\mathcal{C} = \omega(\log(n))$ coherence.*

Proof. We show that one can efficiently distinguish Haar random states and states with $\mathcal{C} = O(\log(n))$.

We now use the following tester: We measure the projector $\Pi_{\mathcal{C}}$ on the state $|\psi\rangle^{\otimes 2}$ from Eq. (S42). We say the tester accepts when the projector $\Pi_{\mathcal{C}}$ is successful, else we say the tester rejects the state.

Lets regard an ensemble $\mathcal{E}_c$ of states which have on average $\mathbb{E}_{|\psi\rangle\leftarrow\mathcal{E}_c}[\mathcal{C}_2(|\psi\rangle)] = 1 - \Omega(n^{-c})$. We have acceptance probability $\mathbb{E}_{|\psi\rangle\leftarrow\mathcal{E}_c}[\langle\psi|^{\otimes 2}\Pi_{\mathcal{C}}|\psi\rangle^{\otimes 2}] = \Omega(n^{-c})$.

For Haar random states, we can calculate the average coherence by standard Haar integration

$$\begin{aligned}\mathbb{E}_{|\phi\rangle\leftarrow S(\mathcal{H})}[\mathcal{C}_2(|\phi\rangle)] &= \int_U \mathcal{C}_2(U|0\rangle)\mathrm{d}U = 1 - \sum_k \int_U |\langle k|U|0\rangle|^4 \mathrm{d}U = 1 - 2^n \int_U |\langle 0|U|0\rangle|^4 \mathrm{d}U \\ &= 1 - 2^n \int_U \mathrm{tr}(U^\dagger|0\rangle\langle 0|U|0\rangle\langle 0|U^\dagger|0\rangle\langle 0|U|0\rangle\langle 0|)\mathrm{d}U = 1 - \frac{2}{2^n+1}\end{aligned}$$

where at the third equality we used the left invariance of Haar random unitaries and in the last step a standard identity for Haar random integrals. We thus find $\mathbb{E}_{|\phi\rangle\leftarrow S(\mathcal{H})}[\mathcal{C}_2(|\phi\rangle)] = 1 - O(2^{-n})$ and thus $\mathbb{E}_{|\psi\rangle\leftarrow S(\mathcal{H})}[\langle\psi|^{\otimes 2}\Pi_{\mathcal{C}}|\psi\rangle^{\otimes 2}] = O(2^{-n})$.

By repeating the testing a polynomial number of times, we can distinguish Haar random states and states drawn from $\mathcal{E}_c$ with $\Omega(1)$ probability.

As we can efficiently distinguish Haar random states and states with $\mathcal{C}_2 = 1 - \Omega(n^{-c})$, PRSs must have $\mathcal{C}_2 = 1 - 2^{-\omega(\log(n))}$. From Jensen's inequality, we have $\mathcal{C}(|\psi\rangle) \geq -\ln(1 - \mathcal{C}_2(|\psi\rangle))$. Thus, PRSs have $\mathcal{C}(|\psi\rangle) = \omega(\log(n))$.

□

J PRUs and coherence power

We now show that PRUs require a sufficient amount of coherence. First, we restate the theorem from the main text:

Theorem S5. *PRUs require $\mathcal{C}_p = \omega(\log(n))$ relative entropy of coherence power.*

Proof. Let us define the following efficient testing algorithm for coherence power of an n-qubit unitary U: We efficiently prepare the $2n$-qubit state

$$\chi(U) = (\mathcal{D}_n U \mathcal{D}_n U)^{\otimes 2}(|\Phi\rangle\langle\Phi|), \tag{S43}$$

where $\mathcal{D}_n(\rho) = \sum_{k=0}^{2^n-1} |k\rangle\langle k|\langle k|\rho|k\rangle$ is the n-qubit coherence-destroying channel. $\mathcal{D}_n$ can be efficiently implemented by measuring the state ρ in the computational basis. Next, we perform the SWAP test between the bipartition of $\chi(U)$. The SWAP test is shown in Fig. S1. We say the SWAP test accepts when the measurement returns 0 which occurs with probability $\Pr_{\text{SWAP}}(U) = (1+\text{tr}(S\chi(U)))/2$ where $S = \sum_{k\ell} = |k\ell\rangle\langle\ell k|$ is the SWAP operator. This measurement gives us the coherence power via [33]

$$\text{tr}(S\chi(U)) = 2^{-n}\sum_{k,\ell} |\langle k|U|\ell\rangle|^4 . \tag{S44}$$

Let us now consider a set of unitaries $\mathcal{E}_c$ with on average $\mathbb{E}_{U\leftarrow\mathcal{E}_c}[2^{-n}\sum_{k,\ell}|\langle k|U|\ell\rangle|^4] = \Omega(n^{-c})$ with $c > 0$. The SWAP test accepts with probability $\mathbb{E}_{U\leftarrow\mathcal{E}_c}[\Pr_{\text{SWAP}}(U)] = \frac{1}{2} + \Omega(n^{-c})$. For Haar random states, we have $\mathbb{E}_{U\leftarrow\mathcal{U}(\mathcal{H})}[2^{-n}\sum_{k,\ell}|\langle k|U|\ell\rangle|^4] = 2^{-n+1}(1+2^{-n})^{-1}$ [33] and thus $\mathbb{E}_{U\leftarrow\mathcal{U}(\mathcal{H})}[\Pr_{\text{SWAP}}(U)] = \frac{1}{2} + O(2^{-n})$. By repeating the test a polynomial number of times, we can distinguish Haar random unitaries and states drawn from $\mathcal{E}_c$ with $\Omega(1)$ probability.

Thus, an ensemble of PRUs $\mathcal{E}_{\text{PR}}$ must have $\mathbb{E}_{U\leftarrow\mathcal{E}_{\text{PR}}}[2^{-n}\sum_{k,\ell}|\langle k|U|\ell\rangle|^4] = 2^{-\omega(\log(n))}$. From Jensen's inequality, we have $\mathbb{E}_{U\leftarrow\mathcal{E}_{\text{PR}}}[-\ln(2^{-n}\sum_{k,\ell}|\langle k|U|\ell\rangle|^4)] = \omega(\log(n))$.

Now, note that we have $2^{-n}\sum_{k,\ell}|\langle k|U|\ell\rangle|^2 = 1$, where $\xi_{k\ell}(U) = 2^{-n}|\langle k|U|\ell\rangle|^2$ can be thought of as a probability distribution. From the well-known inequalities of Rényi entropies, we have

$$\ln(2^{-n}\text{card}(U)) \geq -2^{-n}\sum_{k,\ell}|\langle k|U|\ell\rangle|^2\ln(|\langle k|U|\ell\rangle|^2) \geq -\ln(2^{-n}\sum_{k,\ell}|\langle k|U|\ell\rangle|^4) . \tag{S45}$$

Finally, we use $-2^{-n}\sum_{k,\ell}|\langle k|U|\ell\rangle|^2\ln(|\langle k|U|\ell\rangle|^2) \geq -\ln(2^{-n}\sum_{k,\ell}|\langle k|U|\ell\rangle|^4)$ to get $\mathbb{E}_{U\leftarrow\mathcal{E}_{\text{PR}}}[\mathcal{C}(U)] = \omega(\log(n))$. □

K Imaginarity for rebits

While rebits are by definition real, we can define imaginarity such that it matches the definition of qubits.

We have the n-qubit qubit state

$$|\psi\rangle = \sum_{k=0}^{2^n-1}(a_k + ib_k)|k\rangle \tag{S46}$$

and the corresponding $(n+1)$-rebit state

$$|\psi_{\mathrm{R}}\rangle = \sum_{k=0}^{2^n-1} (a_k|k\rangle|R\rangle + b_k|k\rangle|I\rangle) \tag{S47}$$

with coefficients $a_k, b_k \in \mathbb{R}$. For normalization, we have

$$|\langle\psi|\psi\rangle|^2 = |\langle\psi_{\mathrm{R}}|\psi_{\mathrm{R}}\rangle|^2 = \sum_k (a_k^2 + b_k^2) = 1\,. \tag{S48}$$

First, we note

$$|\langle\psi|\psi^*\rangle|^2 = \left(\sum_k \left(a_k^2 - b_k^2\right)\right)^2 + 4\left(\sum_k a_k b_k\right)^2 = \left(\sum_k a_k^2\right)^2 + \left(\sum_k b_k^2\right)^2 - 2\sum_k a_k^2 \sum_k b_k^2 + 4\left(\sum_k a_k b_k\right)^2. \tag{S49}$$

Then, we have from normalization

$$1 = \sum_k \left(a_k^2 + b_k^2\right) = \left(\sum_k a_k^2 + \sum_k b_k^2\right)^2 = \left(\sum_k a_k^2\right)^2 + \left(\sum_k b_k^2\right)^2 + 2\sum_k a_k^2 \sum_k b_k^2. \tag{S50}$$

Next, a straightforward calculation yields

$$\mathrm{tr}_{1:n}\left(|\psi_{\mathrm{R}}\rangle\langle\psi_{\mathrm{R}}|\right) = \sum_k a_k^2 |R\rangle\langle R| + b_k^2 |I\rangle\langle I| + a_k b_k |R\rangle\langle I| + a_k b_k |I\rangle\langle R|\,, \tag{S51}$$

where $\mathrm{tr}_{1:n}(\cdot)$ is the partial trace over all rebits except the $(n+1)$-th rebit. Then, we have

$$\mathrm{tr}\left(\mathrm{tr}_{1:n}\left(|\psi_{\mathrm{R}}\rangle\langle\psi_{\mathrm{R}}|\right)^2\right) = \left(\sum_k a_k^2\right)^2 + \left(\sum_k b_k^2\right)^2 + 2\left(\sum_k a_k b_k\right)^2. \tag{S52}$$

Now, we can easily see

$$\mathrm{tr}\left(\mathrm{tr}_{1:n}\left(|\psi_{\mathrm{R}}\rangle\langle\psi_{\mathrm{R}}|\right)^2\right) = \frac{1}{2}(|\langle\psi^*|\psi\rangle|^2 + 1)\,. \tag{S53}$$

From this, we immediately conclude

$$\mathcal{I}(|\psi\rangle) \equiv 2(1 - \mathrm{tr}\left(\mathrm{tr}_{1:n}(|\psi_{\mathrm{R}}\rangle\langle\psi_{\mathrm{R}}|)^2\right)\,. \tag{S54}$$

We can measure imaginarity via the rebits efficiently by measuring the purity of the flag rebit. Purity of a single rebit can be efficiently measured, e.g. via tomography on the flag rebit which scales as $O(1)$.

L Testing for imaginarity, entanglement, magic, coherence and purity

Besides imaginarity and coherence, entanglement and magic (also known as nonstabilizerness) are important resources for quantum information processing [58]. Entanglement, characterized by nonclassical correlations between spatially separated quantum systems, has paved the way for advancements in quantum communication [92, 93], quantum cryptography [94], and quantum computation [95, 96]. On the other hand, magic, which measures the extent of deviation from states producible by Clifford circuits or from transformations effected by such circuits, can be used to perform tasks that are computationally challenging for classical computers [97–100]. Various measures of magic have been proposed in recent years [59, 85, 100–108].

Testing for the aforementioned resources is an important task for the certification of quantum information processors. We now discuss the cost of tester $\mathcal{A}_Q$ for different properties Q, where we assume $\beta = 0$ for the tester according to Def. 10. Here, we report on the scaling of the best known protocol for testing a representative measure of each property for the case of qubits. We summarize our findings in Table 1.

1. Imaginarity of states cannot be tested efficiently as we have shown in this work, specifically in Appendix D. In contrast, imaginarity of unitaries can be measured efficiently as shown in Ref. [62] or Appendix G.

2. For entanglement, one can efficiently test for bipartite entanglement of pure states [61, 84]. For unitaries, one can efficiently test whether the unitary is a product unitary [47].

3. The magic of states can be efficiently tested both for states [48, 85, 100] and unitaries [48, 109, 110].

4. For states, one can test coherence efficiently using the protocol given in Appendix I. The protocol for the coherence power of unitaries is given in [33] or Appendix J.

5. Purity of states can be tested via the SWAP test [60], where the protocol is shown in Appendix C. Analogously, for channels one can test how close the channel is to an isometry. For a channel Γ, one can efficiently test the property $g(\Gamma) = \mathrm{tr}((\Gamma \otimes I_n(|\Phi\rangle)^2)$, where one has $g = 1$ only when the channel is an isometry, and else $g < 1$. One can efficiently measure g by applying the SWAP test on the Choi state.

All mentioned properties can be efficiently measured via protocols involving Bell measurements, with the exception being the imaginarity of states.

M Imaginarity of Haar-random states and unitaries

Here, we calculate the average imaginarity of both Haar-random states and unitaries using Weingarten calculus [111].

1 Imaginarity of Haar-random states

Lemma S2. *Let $d \in \mathbb{Z}^+$ be a positive integer and let η denote the Haar measure on $U(\mathbb{C}^d)$. For $U \in U(\mathbb{C}^d)$, let $|\psi_U\rangle = U|0\rangle$ denote the state obtained by acting the unitary U on the computational basis state $|0\rangle$. Then,*

$$\int \mathrm{d}\eta(U) \left[1 - |\langle\psi_U|\psi_U^\star\rangle|^2\right] = 1 - \frac{2}{d+1}. \tag{S55}$$

Proof. By definition,

$$|\psi_U\rangle = U|0\rangle.$$

By transposing or complex-conjugating this state, we get

$$\begin{aligned} |\psi_U^\star\rangle &= U^\star|0\rangle, \\ \langle\psi_U| &= \langle 0|U^\dagger, \\ \langle\psi_U^\star| &= \langle 0|U^T. \end{aligned}$$

These expressions allow us to expand the left-hand side of Eq. (S55) as follows:

$$\begin{aligned} \int \mathrm{d}\eta(U) \left[1 - |\langle\psi_U|\psi_U^\star\rangle|^2\right] &= 1 - \int \mathrm{d}\eta(U)\ \langle\psi_U|\psi_U^\star\rangle\langle\psi_U^\star|\psi_U\rangle \\ &= 1 - \int \mathrm{d}\eta(U)\ \sum_{a=0}^{d-1} U_{0a}^\dagger U_{a0}^\star \sum_{b=0}^{d-1} U_{0b}^T U_{b0} \\ &= 1 - \sum_{a,b=0}^{d-1} \left[\int \mathrm{d}\eta(U)\ U_{b0}U_{b0}U_{a0}^\star U_{a0}^\star\right]. \end{aligned} \tag{S56}$$

The integral in Eq. (S56) is an integral taken with respect to the Haar measure of a monomial of rank 4; for such an integral, nice closed-form expressions are well-known (for example, see [112, Eq. 10] or [111]): for $d \geq 2$,

$$\int \mathrm{d}\eta(U)\ U_{i_1 j_1} U_{i_2 j_2} U^*_{i'_1 j'_1} U^*_{i'_2 j'_2} = \frac{1}{d^2-1}\left(\delta_{i_1 i'_1}\delta_{i_2 i'_2}\delta_{j_1 j'_1}\delta_{j_2 j'_2} + \delta_{i_1 i'_2}\delta_{i_2 i'_1}\delta_{j_1 j'_2}\delta_{j_2 j'_1}\right) - \frac{1}{d\,(d^2-1)}\left(\delta_{i_1 i'_1}\delta_{i_2 i'_2}\delta_{j_1 j'_2}\delta_{j_2 j'_1} + \delta_{i_1 i'_2}\delta_{i_2 i'_1}\delta_{j_1 j'_1}\delta_{j_2 j'_2}\right). \tag{S57}$$

Hence, for $d \geq 2$,

$$\begin{aligned}\int \mathrm{d}\eta(U) U_{b0} U_{b0} U^\star_{a0} U^\star_{a0} &= \frac{1}{d^2-1}\left(\delta_{ba}\delta_{ba}\delta_{00}\delta_{00} + \delta_{ba}\delta_{ba}\delta_{00}\delta_{00}\right) - \frac{1}{d\,(d^2-1)}\left(\delta_{ba}\delta_{ba}\delta_{00}\delta_{00} + \delta_{ba}\delta_{ba}\delta_{00}\delta_{00}\right)\\ &= \frac{2}{d\,(d+1)}\delta_{ab},\end{aligned}$$

and so substituting this expression into Eq. (S56) gives us

$$\int \mathrm{d}\eta(U)\left[1 - |\langle\psi_U|\psi^\star_U\rangle|^2\right] = 1 - \sum_{a,b=0}^{d-1}\frac{2}{d(d+1)}\delta_{ab} = 1 - \frac{2}{d\,(d+1)}d = 1 - \frac{2}{d+1}. \tag{S58}$$

Next, we show that this expression also holds for $d = 1$:

$$\begin{aligned}\int \mathrm{d}\eta(U)\ \left[1 - |\langle\psi_U|\psi^\star_U\rangle|^2\right] &= 1 - \int \mathrm{d}\eta(U) U_{00} U_{b0} U^\star_{a0} U^\star_{a0}\\ &= 1 - \int \mathrm{d}\eta(U)\ |U_{00}|^2 = 1 - \int \mathrm{d}\eta(U) = 1 - 1 = 0 = 1 - \frac{2}{d+1}.\end{aligned}$$

This completes the proof of Eq. (S55) for all $d \in \mathbb{Z}^+$. □

2 Imaginarity of Haar-random unitaries

Lemma S3. *Let* $\mathcal{I} : \mathcal{U}\left(\mathbb{C}^d\right) \to \mathbb{R}$, $d \in \mathbb{Z}_{\geq 2}$ *and* $\mathcal{I}(U) = 1 - \frac{1}{d^2}|\mathrm{tr}\left(U^T U\right)|^2$, *then*

$$\int \mathrm{d}\eta(U)\ \mathcal{I}(U) = 1 - \frac{2}{d\,(d+1)}.$$

Proof.

$$\begin{aligned}\int \mathrm{d}\eta(U)\ \mathcal{I}(U) &= \int \mathrm{d}\eta(U)\left(\frac{1}{d^2}\left|\mathrm{tr}\left(U^T U\right)\right|^2\right)\\ &= 1 - \frac{1}{d^2}\int \mathrm{d}\eta(U)\ \left|\mathrm{tr}\left(U^T U\right)\right|^2\\ &= 1 - \frac{1}{d^2}\int \mathrm{d}\eta(U)\ \mathrm{tr}\left(U^T U\right)\mathrm{tr}\left(U^T U\right)^*\\ &= 1 - \frac{1}{d^2}\int \mathrm{d}\eta(U)\ \mathrm{tr}\left(U^T U\right)\mathrm{tr}\left(U^\dagger U^*\right)\\ &= 1 - \frac{1}{d^2}\int \mathrm{d}\eta(U)\ \sum_{w\in\mathbb{Z}_d}\langle w|U^T U|w\rangle \sum_{y\in\mathbb{Z}_d}\langle y|U^\dagger U^*|y\rangle\\ &= 1 - \frac{1}{d^2}\sum_{w,x,y,z\in\mathbb{Z}_d}\int \mathrm{d}\eta(U)\ \langle w|U^T|x\rangle\langle x|U|w\rangle\langle y|U^\dagger|z\rangle\langle z|U^*|y\rangle\\ &= 1 - \frac{1}{d^2}\sum_{w,x,y,z\in\mathbb{Z}_d}\int \mathrm{d}\eta(U)\ U_{xw}U_{xw}U^*_{zy}U^*_{zy}\end{aligned}$$

$$= 1 - \frac{1}{d^2} \sum_{w,x,y,z \in \mathbb{Z}_d} \int \mathrm{d}\eta(U)\ U_{xw}^2 (U_{zy}^*)^2. \tag{S59}$$

The integral in Eq. (S59) is of the form Eq. (S57), and hence, by taking

$$\begin{aligned} i_1 &= i_2 = x \\ j_1 &= j_2 = w \\ i_1' &= i_2' = z \\ j_1' &= j_2' = y \end{aligned}$$

in Eq. (S57), we get

$$\begin{aligned} \int \mathrm{d}\eta(U)\ U_{xw}^2 (U_{zy}^*)^2 &= \frac{1}{d^2-1} \left(\delta_{xz}\delta_{xz}\delta_{wy}\delta_{wy} + \delta_{xz}\delta_{xz}\delta_{wy}\delta_{wy}\right) - \frac{1}{d\left(d^2-1\right)} \left(\delta_{xz}\delta_{xz}\delta_{wy}\delta_{wy} + \delta_{xz}\delta_{xz}\delta_{wy}\delta_{wy}\right) \\ &= \frac{2}{d\left(d+1\right)} \delta_{xz}\delta_{wy}. \end{aligned}$$

Thus, Eq. (S59) may be simplified as

$$\begin{aligned} \int \mathrm{d}\eta(U)\ \mathcal{I}\left(U\right) &= 1 - \frac{1}{d^2} \sum_{w,x,y,z \in \mathbb{Z}^d} \frac{2}{d\left(d+1\right)} \delta_{xz}\delta_{wy} \\ &= 1 - \frac{1}{d^2} \frac{2}{d\left(d+1\right)} d^2 \\ &= 1 - \frac{2}{d\left(d+1\right)}, \end{aligned}$$

which completes our proof. □